Copyright

© Copyright 2013 SAP AG. All rights reserved.

SAP Library document classification: PUBLIC

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. National product specifications may vary.

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.

SAP 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.

# Icons in Body Text

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Caution icon" /></td>
<td>Caution</td>
</tr>
<tr>
<td><img src="image" alt="Example icon" /></td>
<td>Example</td>
</tr>
<tr>
<td><img src="image" alt="Note icon" /></td>
<td>Note</td>
</tr>
<tr>
<td><img src="image" alt="Recommendation icon" /></td>
<td>Recommendation</td>
</tr>
<tr>
<td><img src="image" alt="Syntax icon" /></td>
<td>Syntax</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example text</em></td>
<td>Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.</td>
</tr>
<tr>
<td></td>
<td>Cross-references to other documentation.</td>
</tr>
<tr>
<td><strong>Example text</strong></td>
<td>Emphasized words or phrases in body text, graphic titles, and table titles.</td>
</tr>
<tr>
<td>EXAMPLE TEXT</td>
<td>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.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example text</strong></td>
<td>Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.</td>
</tr>
<tr>
<td><code>&lt;Example text&gt;</code></td>
<td>Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.</td>
</tr>
<tr>
<td>EXAMPLE TEXT</td>
<td>Keys on the keyboard, for example, F2 or ENTER.</td>
</tr>
</tbody>
</table>
**Table of Contents**

Component Security Guide for SAP EWM 9.1 .............................................................. 9
Document History ............................................................................................................ 10
Introduction ..................................................................................................................... 11
Before You Start .............................................................................................................. 15
Technical System Landscape .......................................................................................... 20
Security Aspects of Data, Data Flow, and Processes ....................................................... 21
User Administration and Authentication ......................................................................... 23
  User Management ........................................................................................................... 24
  User Data Synchronization ............................................................................................ 29
  Integration into Single Sign-On Environments ............................................................... 30
Authorizations .................................................................................................................. 32
  Authorization Objects .................................................................................................... 36
  Maintaining Authorizations ........................................................................................ 37
  Maintaining Authorizations for Integration with SAP Components .......................... 38
  Maintaining Authorizations for Enterprise Services ................................................... 41
Session Security Protection ............................................................................................. 42
Network and Communication Security ............................................................................ 43
  Communication Channel Security ................................................................................ 45
  Network Security .......................................................................................................... 48
  Communication Destinations ......................................................................................... 49
Internet Communication Framework Security ............................................................... 52
Data Storage Security ....................................................................................................... 54
Security for Additional Applications .............................................................................. 59
Enterprise Services Security ............................................................................................ 60
Other Security-Relevant Information .............................................................................. 61
  User Frontend ............................................................................................................... 62
  Data Protection and Privacy ......................................................................................... 64
Security-Relevant Logging and Tracing .......................................................................... 65
Services for Security Lifecycle Management .................................................................... 68
Virus Check of Document Attachments .......................................................................... 70
Appendix .......................................................................................................................... 71
Document History

Before you start the implementation, make sure that you have the latest version of this document. You can find the latest version at the following location:

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>08 November 2013</td>
<td>Document created</td>
</tr>
</tbody>
</table>
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 or 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.

We strongly recommend that you also consult the SAP NetWeaver Security Guide.

About This Document

This Security Guide provides an overview of the security-relevant information that applies to the SAP EWM 9.1 component.

Applications in EWM 9.1

EWM 9.1 contains multiple applications that can be used independently of each other. For example, SAP Dock Appointment Scheduling is technically part of the EWM 9.1 installation, but it can be used independently of other EWM applications as a standalone application. If you are using SAP Dock Appointment Scheduling only, without any integration to SAP EWM, some parts of the guide are not relevant.

The following list describes the levels of relevance of this guide:
Several sections of this guide describe steps that are independent of the applications or business processes used, and you must always implement these steps. For example, securing an SAP NetWeaver system. This is true for most parts of this document. These sections are not marked.

Other sections of this guide describe topics that are relevant for both EWM in general and Dock Appointment Scheduling. These sections are not marked. Here if the term EWM is used, it means the EWM 9.1 system installation, including Dock Appointment Scheduling.

Some sections of this guide are only necessary depending on which processes or applications of EWM 9.1 you are using. These sections can be either specific to Dock Appointment Scheduling or for specific EWM processes. These sections are marked as relevant for Dock Appointment Scheduling or EWM applications. In these sections only, you can omit the steps that are specifically for EWM applications or Dock Appointment Scheduling.

This guide uses the following key to identify the applications:

- Relevant only if you are using Dock Appointment Scheduling
- Not relevant for Dock Appointment Scheduling

The guide also differentiates between standalone Dock Appointment Scheduling used as standalone and Dock Appointment Scheduling integrated with EWM.

- EWM: EWM-only processes
- All: Applies to both Dock Appointment Scheduling and EWM

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 cookies.

- 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.

- 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

<table>
<thead>
<tr>
<th>Guide/Documentation</th>
<th>Path to the Guide/Documentation</th>
</tr>
</thead>
</table>

The SAP EWM component is built on further components and 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 Installation Note | SAP Note 1501624 |

### Related Security Guides


### Related Security Guides for SAP NetWeaver Products

<table>
<thead>
<tr>
<th>Product</th>
<th>See</th>
<th>Application Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System and Database Platforms</td>
<td>Security Guides for the Operating System and Database Platforms</td>
<td>All</td>
</tr>
</tbody>
</table>
| SAP NetWeaver Application Server | Security Guides for SAP NetWeaver Functional Units > Security Guides for the Application Server:  
  o Security Aspects for AS Infrastructure Functional Units | All |
<table>
<thead>
<tr>
<th>Security Settings for the SAP Message Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>o Security Guides for Business Services</td>
</tr>
<tr>
<td>SAP Interactive Forms by Adobe Security Guide</td>
</tr>
<tr>
<td>o Security Guides for Business Services</td>
</tr>
<tr>
<td>SAP Knowledge Warehouse Security Guide</td>
</tr>
<tr>
<td>o Security Aspects for AS Infrastructure Functional Units</td>
</tr>
<tr>
<td>AS ABAP with Integrated ITS</td>
</tr>
<tr>
<td>• Security Guides for SAP NetWeaver</td>
</tr>
<tr>
<td>Functional Units</td>
</tr>
<tr>
<td>• Security Guides for Composition Environment</td>
</tr>
<tr>
<td>• Composite Application Framework Security Guide</td>
</tr>
<tr>
<td>• Security Aspects for Lifecycle Management</td>
</tr>
<tr>
<td>• Virus Protection and SAP GUI Integrity Checks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EP Core (EPC) and Enterprise Portal (EP)</th>
<th>Security Guides for SAP NetWeaver Functional Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Guides for Enterprise Portal (EP) and EP Core - Application Portal (EPC)</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAP NetWeaver Business Warehouse (SAP NetWeaver BW)</th>
<th>Security Guides for SAP NetWeaver Functional Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Guide for SAP NetWeaver BW</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAP NetWeaver Development Infrastructure (NWDI)</th>
<th>Security Aspects for Lifecycle Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security of the SAP NetWeaver Development Infrastructure</td>
<td>All</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAP NetWeaver Mobile</th>
<th>Security Guides for SAP NetWeaver Functional Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Guide for SAP NetWeaver Mobile</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAP NetWeaver Process Integration (SAP NetWeaver PI)</th>
<th>Security Guides for SAP NetWeaver Functional Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SAP NetWeaver Process Integration Security Guide</td>
</tr>
<tr>
<td></td>
<td>Relevant only if integration with SAP Transportation Management is carried out based on SAP NetWeaver PI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Guides for Standalone Engines, Clients, and Tools</th>
<th>Security Guides for SAP NetWeaver Functional Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Search and Classification (TREX) Security Guide</td>
</tr>
<tr>
<td></td>
<td>Security Guides for SAP NetWeaver Functional Units</td>
</tr>
<tr>
<td></td>
<td>Security Guides for the Application Server</td>
</tr>
<tr>
<td></td>
<td>Security Guides for Business Services</td>
</tr>
<tr>
<td></td>
<td>SAP Content Server Security Guide</td>
</tr>
<tr>
<td></td>
<td>Introduction and subsequent chapters</td>
</tr>
<tr>
<td></td>
<td>Security Guides for SAP NetWeaver Functional Units</td>
</tr>
<tr>
<td></td>
<td>Security Guides for the Application Server</td>
</tr>
<tr>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
</tbody>
</table>
Aspects for AS Infrastructure Functional Units Security Information for SAP Web Dispatcher

**Connectivity and Interoperability**

Security Guides for Connectivity and Interoperability Technologies, for example:
- RFC/ICF Security Guide
- Security Guide for Connectivity with the AS Java
- Security Aspects for Web Services

All

**Lifecycle Management**

Security Aspects for Lifecycle Management, for example:
- System Landscape Directory Security Guide
- Auditing and Logging

All

**Web Dynpro ABAP Security Guide**

This is especially important if you plan to use Dock Appointment Scheduling and the Collaborative Scenarios.


Relevant only if you are using Dock Appointment Scheduling


This guide is relevant only if you are using Labor Demand Planning.


**Important SAP Notes**

The most important SAP Notes that apply to the security of the SAP EWM component are shown in the following table:

<table>
<thead>
<tr>
<th>SAP Note</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>25591</td>
<td>Password change for DBM and DBA users</td>
<td>The SAP R/3 user password is to be changed.</td>
</tr>
<tr>
<td>30724</td>
<td>Data Protection and Security in SAP Systems</td>
<td>None</td>
</tr>
<tr>
<td>110600</td>
<td>SAP Security Library</td>
<td>None</td>
</tr>
<tr>
<td>(SAPSECULIB)</td>
<td>128447</td>
<td>Trusted/Trusting Systems</td>
</tr>
<tr>
<td>138498</td>
<td>Single Sign-On Solutions</td>
<td>Information about Single Sign-On solutions for SAP systems</td>
</tr>
<tr>
<td>389220</td>
<td>Problems with Pasting the Certificate Request Reply</td>
<td>None</td>
</tr>
<tr>
<td>447543</td>
<td>APO: Authorizations too Comprehensive/Not User-Specific</td>
<td>None</td>
</tr>
<tr>
<td>510007</td>
<td>Setting Up SSL on the Web Application Server ABAP</td>
<td>None</td>
</tr>
<tr>
<td>616555</td>
<td>LiveCache &gt;= 7.4: Password Change</td>
<td>The passwords of the standard liveCache user, the database system administrator, the DBM user, should be changed in the liveCache environment.</td>
</tr>
<tr>
<td>637052</td>
<td>Missing Authorization Object for Database Views</td>
<td>None</td>
</tr>
<tr>
<td>662340</td>
<td>SSF Encryption Using the SAPCrytolib</td>
<td>The SAP Cryptographic Library has to be used for encrypting data in the SAP system.</td>
</tr>
<tr>
<td>683528</td>
<td>Security Note: SAP MaxDB</td>
<td>This note provides information about the secure operation of SAP DB/MaxDB and liveCache.</td>
</tr>
<tr>
<td>727839</td>
<td>Authorization Role for the SAP SCM – SAP R/3 Integration</td>
<td>None</td>
</tr>
<tr>
<td>792366</td>
<td>Subsequent Implementing a Security Level for Documents</td>
<td>Knowledge Provider: what needs to be taken into account if an application of the Knowledge Provider (KPro) decides to change the security level for documents for one or more of their PHIO classes.</td>
</tr>
<tr>
<td>1501624</td>
<td>Installing or Upgrading SCMEWM 7.02 to SAP ERP 6.0</td>
<td>This note provides information on performing an add-on installation or upgrade to Enhancement Package 6 for SAP ERP 6.0</td>
</tr>
<tr>
<td>1517416</td>
<td>Collective security note for SAP EWM</td>
<td>This note contains additional security-relevant information and notes for SAP EWM.</td>
</tr>
<tr>
<td>1515223</td>
<td>SAP NetWeaver Process Integration: Release Recommendation</td>
<td>This note sets out our recommendation on which release of SAP NetWeaver PI you should use.</td>
</tr>
<tr>
<td>1536783</td>
<td>SAP Security Recommendations – Protecting Java- and ABAP Based BAS</td>
<td>This note provides information on where to find the SAP Security Recommendations Protecting Java- and ABAP-Based SAP® Applications Against Common Attacks December 2010 white paper.</td>
</tr>
<tr>
<td>900000</td>
<td>NetWeaver Business Client – FAQ</td>
<td>None</td>
</tr>
</tbody>
</table>

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

- [http://service.sap.com/securitynotes](http://service.sap.com/securitynotes)

### Additional Information

For more information about specific topics, see the addresses on SAP Service Marketplace as shown in the following table:
<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on SAP Service Marketplace or SDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Guides</td>
<td><a href="http://service.sap.com/securityguide">http://service.sap.com/securityguide</a></td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td><a href="http://service.sap.com/notes">http://service.sap.com/notes</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://service.sap.com/securitynotes">http://service.sap.com/securitynotes</a></td>
</tr>
<tr>
<td>Released Platforms</td>
<td><a href="http://service.sap.com/pam">http://service.sap.com/pam</a></td>
</tr>
<tr>
<td>Network Security</td>
<td><a href="http://service.sap.com/securityguide">http://service.sap.com/securityguide</a></td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td><a href="http://service.sap.com/solutionmanager">http://service.sap.com/solutionmanager</a></td>
</tr>
<tr>
<td>SAP NetWeaver</td>
<td><a href="http://sdn.sap.com/irj/sdn/netweaver">http://sdn.sap.com/irj/sdn/netweaver</a></td>
</tr>
</tbody>
</table>
## Technical System Landscape

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

<table>
<thead>
<tr>
<th>Topic</th>
<th>Guide/Tool</th>
<th>Quick Link to SAP Service Marketplace</th>
</tr>
</thead>
</table>
Security Aspects of Data, Data Flow, and Processes

SAP Extended Warehouse Management (SAP EWM) can be installed, distributed, and used in multiple different scenarios. For more information, see Technical System Landscape [External].

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

<table>
<thead>
<tr>
<th>Process</th>
<th>Security Measure</th>
<th>Application Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP EWM receives data from SAP ERP (such as deliveries and master data) and sends data to SAP ERP (such as confirmations and stock updates). This is typically done using standard qRFC/RFC technology.</td>
<td>Ensure appropriate user authorizations. For more information, see Communication Channel Security [External].</td>
<td>Not relevant for standalone Dock Appointment Scheduling</td>
</tr>
<tr>
<td>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.</td>
<td>For more information, see Internet Communication Framework Security [External].</td>
<td>Not relevant for standalone Dock Appointment Scheduling</td>
</tr>
<tr>
<td>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.</td>
<td>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 [External].</td>
<td>Not relevant for standalone Dock Appointment Scheduling</td>
</tr>
<tr>
<td>SAP EWM offers a collaborative scenario for Dock Appointment Scheduling. This enables appointment planners for carriers to access the system using Web Dynpro ABAP technology, for example, from outside the company network.</td>
<td>In this scenario, users outside of the company or firewall may access the system. For such scenarios, special attention must be paid to assigning authorizations to these users, and to the system setup and how the access from outside the company is granted. For more information, see Collaborative Scenario using Dock Appointment Scheduling in Network and Communication Security [Page 43].</td>
<td>Relevant only if you are using Dock Appointment Scheduling</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>SAP EWM offers a scenario for Labor Demand Planning. This enables users to access the SAP EWM system from a mobile device.</td>
<td>In this scenario, users can access the system from mobile devices using SAP Netweaver Gateway. For more information see Labor Demand Planning in Network and Communication Security [Page 43].</td>
<td>Relevant only if you are using Labor Demand Planning from a mobile device</td>
</tr>
<tr>
<td>SAP EWM offers a scenario for direct integration to SAP Transportation Management (SAP TM).</td>
<td>In this scenario, SAP EWM receives inbound messages from SAP TM and can send outbound messages to SAP TM. The communication is performed using enterprise services.</td>
<td>Relevant only if you are using a direct integration to SAP TM</td>
</tr>
</tbody>
</table>
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 also apply to the SAP EWM component. For more information, see the SAP NetWeaver Security Guide under Security Guides for SAP NetWeaver Functional Units Security Guides for the Application Server Security Guides for AS ABAP SAP NetWeaver Application Server ABAP Security Guide.

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 24]
  
  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 29]
  
  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 30]
  
  This topic describes how the SAP EWM component supports Single Sign-On mechanisms.
User Management

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 SAP NetWeaver documentation under SAP NetWeaver Library: Function-Oriented View > Security > Identity Management.

User Administration Tools

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

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management for the ABAP Engine (transaction SU01)</td>
<td>Use the user management transaction SU01 to maintain users in ABAP-based systems.</td>
</tr>
<tr>
<td>Profile Generator (transaction PFCG)</td>
<td>Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.</td>
</tr>
<tr>
<td>Central User Administration (CUA)</td>
<td>Use the CUA to maintain users for multiple ABAP-based systems centrally. Synchronization with a directory server is also supported.</td>
</tr>
<tr>
<td>User Management Engine (UME) administration console</td>
<td>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.</td>
</tr>
<tr>
<td>SAP NetWeaver Application Server Java user management using the Visual Administrator</td>
<td>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.</td>
</tr>
</tbody>
</table>

For a detailed description of the user management tools available in SAP NetWeaver, see the SAP NetWeaver Security Guide under 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.

The user types required for SAP EWM include the following:

- **Individual users**
  - Dialog users are used for business users who are assigned to roles that allow them to work individually on their dedicated tasks in your SAP EWM 9.1 system.
  - Internet users are used for external users who are allowed to access your SAP EWM 9.1 system from the Internet. If your scenario contains the collaborative scenario for appointment planners for carrier, employees of the carrier can log on via the Internet.

- **Technical users**
  - Service users are used for technical purposes, such as service administrators, and are usually available to a larger, anonymous group of users.
  - Communication users are used for dialog-free communication for external RFC calls, for example, for the communication between your SAP EWM 9.1 system and an SAP ERP system.

- **Background users** are used for running background jobs and executing reports.

For more information about these user types, see the SAP NetWeaver Security Guide under Security Guides for SAP NetWeaver Functional Units Security Guides for the Application Server Security Guides for AS ABAP SAP NetWeaver Application Server ABAP Security Guide User Administration and Authentication User Management User Types.

The user types required for SAP EWM include the following:

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
<th>Application Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP EWM 9.1</td>
<td>&lt;sapsid&gt;adm</td>
<td>Yes</td>
<td>SAP System Administrator</td>
<td>To be entered</td>
<td>SAP EWM System Administrator</td>
<td>All</td>
</tr>
<tr>
<td>SAP EWM 9.1</td>
<td>SAPServicem&lt;sapsid&gt;</td>
<td>Yes</td>
<td>SAP System Service Administrator</td>
<td>To be entered</td>
<td>SAP EWM System Service Administrator</td>
<td>All</td>
</tr>
<tr>
<td>SAP SCM 7.0 Server including SAP enhancement package 3</td>
<td>&lt;sapsid&gt;adm</td>
<td>Yes</td>
<td>SAP System Administrator</td>
<td>To be entered</td>
<td><a href="http://service.sap.com/instguides">http://service.sap.com/instguides</a></td>
<td><a href="http://service.sap.com/instguides">SAP Business Suite Applications SAP SCM SAP SCM Server Using SAP enhancement package 3 for SAP SCM Server 7.0</a></td>
</tr>
<tr>
<td><strong>SAP SCM 7.0 Server including SAP enhancement package 3</strong></td>
<td>SAPService &lt;sapsid&gt;</td>
<td>Yes</td>
<td>SAP System Service Administrator Service User</td>
<td>To be entered</td>
<td>All, if EWM is installed on top of an SCM Server system</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>----------------------</td>
<td>-----</td>
<td>-----------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>SAP NetWeaver AS Java</td>
<td>SAPJSF</td>
<td>Yes</td>
<td>Communication user</td>
<td>To be entered</td>
<td>SAP Business Suite Applications &gt; SAP SCM &gt; SAP SCM Server &gt; Using SAP enhancement package 3 for SAP SCM Server 7.0 &gt; Installation Guides &gt; Installation Guides for SAP EHP3 for SAP SCM 7.0 &gt; Generic Installation Guides</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>-----</td>
<td>---------------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>SAP EWM 9.1</td>
<td>RFC communication users (you need an RFC communication user for each RFC destination described in section Communication Destinations [External])</td>
<td>No</td>
<td>Communication user</td>
<td>The authorizations of the user depend on the business case. For more information, see Authorizations [External] in this Security Guide.</td>
<td>Documentation for SAP EWM 9.1 under Communication Destinations [External] and Authorizations [External]</td>
<td></td>
</tr>
<tr>
<td>SAP EWM 9.1</td>
<td>Business processing users (you need a user in each component for each employee working with the system)</td>
<td>No</td>
<td>Dialog user</td>
<td>To be entered</td>
<td>Documentation for SAP EWM 9.1 under Authorizations [External]</td>
<td></td>
</tr>
<tr>
<td>SAP EWM 9.1</td>
<td>Users for employees of a carrier who takes part in the collaborative scenario for Dock Appointment</td>
<td>No</td>
<td>Internet user</td>
<td>To be entered</td>
<td>Documentation for SAP EWM 9.1 under Authorizations [Page 32]</td>
<td>Relevant only if you are using Dock Appointment Scheduling</td>
</tr>
<tr>
<td>SAP EWM 9.1</td>
<td>User for Labor Demand Planning used from a mobile device</td>
<td>No</td>
<td>Communication user</td>
<td>To be entered</td>
<td>Used for access from a mobile device in Labor Demand Planning. The user is used for the connection from SAP Netweaver Gateway to SAP EWM.</td>
<td>Relevant only if you are using mobile devices in Labor Demand Planning</td>
</tr>
</tbody>
</table>


For more information about SAP NetWeaver password rules, see SAP Library for SAP NetWeaver under SAP NetWeaver Library: Function-Oriented View Security Identity Management User and Role Administration of Application Server ABAP Configuration of User and Role Administration First Installation Procedure Logon and Password Security in the ABAP System Password Rules.
**User Data Synchronization**

To save administrative effort, you can synchronize user data in your system landscape. Since the SAP Extended Warehouse Management (SAP EWM) component is based on SAP NetWeaver 7.4, all the mechanisms for user data synchronization of SAP NetWeaver 7.4 are available for SAP EWM.

For information about user data synchronization in SAP NetWeaver, see the SAP NetWeaver documentation under SAP NetWeaver Library: Function-Oriented View Security Identity Management Identity Management for System Landscapes.
Integration into Single Sign-On Environments

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 under User Administration and Authentication > User Authentication and Single Sign-On in the section Integration.


The following mechanisms are supported:

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 under 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 under 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 under User Administration and Authentication > User Authentication and Single Sign-On in the section Client Certificates.

If you use any of the following, we recommend that you use client certificates instead of authentication with user name and password:

- The collaborative scenario for Dock Appointment Scheduling, with carriers and users who have access to your system from the Internet
- The mobile application for Labor Demand Planning

This prevents Internet users from trying to log on with another user’s user name.
### Authorizations

The authorization concept of the SAP Extended Warehouse Management (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 the SAP NetWeaver documentation under [SAP NetWeaver Library: Function-Oriented View Security > Identity Management > User and Role Administration of Application Server ABAP > AS ABAP Authorization Concept](https://www.sap.com) and [User Management of the Application Server Java > Authorization Concept of the AS Java](https://www.sap.com).

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 maintain your own new roles or those provided by SAP centrally, 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.

To avoid authorizations being misused, we recommend that users are assigned only the minimal authorizations that they require for their work. Never assign full authorizations.

It is very important that RFC users are assigned only minimal authorizations.

For an overview of the role administration and more information about how a delivered standard role can be used and adjusted to your own needs, see the SAP NetWeaver documentation under SAP NetWeaver Library: Function-Oriented View > Security > Identity Management > User and Role Administration of Application Server ABAP > Configuration of User and Role Administration > Role Administration. See Role Administration Functions and, for example, Changing Standard Roles or Creating Derived Roles and Copying Authorizations.

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.

You can find the application-relevant roles using the following search terms:

- 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.

- The search term */SCWM/*/DAS* lists all roles that are relevant for Dock Appointment Scheduling.

Alternatively, you can 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.

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

This is not relevant for standalone Dock Appointment Scheduling.
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 the SAP EWM documentation under *Roles for Extended Warehouse Management (EWM)*.

For information about users and roles in SAP NetWeaver, see the SAP NetWeaver documentation under *SAP NetWeaver Library: Function-Oriented View Security Identity Management User and Role Administration of Application Server ABAP* and *User Management of the Application Server Java*.

**Critical Roles and Authorization Combinations**

**Expert Role**

SAP EWM provides the expert role *EWM: Warehouse Expert (/SCWM/EXPERT)*. This role contains almost all transactions and authorizations for SAP EWM and the corresponding customizing. Therefore, we recommend that you assign this role very carefully and only to very specific users, and that you do not assign this role to normal users or users who work in specific SAP EWM areas only.

**Appointment Planner for Carrier**

This role is relevant only if you are using Dock Appointment Scheduling.

SAP Dock Appointment Scheduling offers a collaboration scenario where appointment planners for carriers can log on to the SAP Dock Appointment Scheduling system, and view and maintain appointments for their carrier.

Since this potentially means that employees of a different company access SAP Dock Appointment Scheduling from outside the company network, you must put a special focus on authorizations.

This kind of user should have very limited authorizations. As well as this, they should be able to access data of their own carrier only, and not be able to access other carriers’ data. They should not be able to see internal data, like overall capacities of loading points. Therefore you must be very careful and restrictive when assigning roles and authorizations to this kind of user.

SAP Dock Appointment Scheduling delivers a special role for this: Appointment Planner for Carrier in Dock Appointment Scheduling (/SCWM/DAS_EXT_CARR_PLANNER).

This role contains only one Web Dynpro screen in the menu, *Maintain Appointments – Textual (/SCWM/DSAPP_LIST)*. This screen allows the appointment planners for carriers to view and create appointments. The Web Dynpro application *Direct Access to Appointment – Textual (/SCWM/DSAPP_MAINT)* is also available, but it is not visible in the user menu, as it is started indirectly from the *Maintain Appointments – Textual screen*.

The role also contains very limited number of authorization objects.
We highly recommend that you define, in the roles, the loading points for which a user may view or create appointments. You can do this in the authorization field **Loading Point** (/SCWM/DSLP) in the authorization objects **Loading Appointment** (/SCWM/DSAP) and **Slot** (/SCWM/DSSL).

In addition, the authorization field **User Process Scope for Dock Appointment Scheduling** (/SCWM/DSPS) is very important. It is available on the authorization objects **Loading Appointment** and **Slot**. For appointment planners for carriers, set this field to **Scope for an Appointment Planner for Carrier**. This ensures that this user can create and view appointments only for the carrier that is assigned to him or her. Otherwise such a user could create appointments for any carrier.

For more information, see the SAP Dock Appointment Scheduling documentation at [http://help.sap.com/ewm](http://help.sap.com/ewm) ➔ SAP EWM 9.1 ➔ Application Help ➔ SAP Library ➔ In SAP Library, choose ➔ SAP Extended Warehouse Management (SAP EWM) ➔ SAP Dock Appointment Scheduling ➔ Collaboration with Carriers

**Warehouse Management Monitor: Authorization to Display Batch Execution Data**

In the warehouse management monitor (/SCWM/MON), you can execute selections using batch jobs. You can view the results in the warehouse management monitor. During the selection, the system performs the normal authorization checks and selects and stores only data for which the user has authorization in the data containers for the warehouse management monitor. But if these data containers are then displayed by other users, the system does not perform these authorization checks. Therefore, you should only grant the authorization to display batch execution data for monitor nodes or users where these checks are not critical.

The authorization object used for the authorization to display batch execution data in the warehouse management monitor is /SCWM/DATC. For more information about this authorization object, see the documentation of authorization object /SCWM/DATC and the documentation of the warehouse management monitor in SAP Library for SAP EWM under ➔ SAP Extended Warehouse Management (SAP EWM) ➔ Monitoring ➔ Warehouse Management Monitor.
Authorization Objects

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 the SAP NetWeaver documentation under SAP NetWeaver Library: Function-Oriented View Security Identity Management User and Role Administration of Application Server ABAP AS ABAP Authorization Concept.

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.

If you are using SAP Dock Appointment Scheduling, ensure that you have read the information regarding the authorization objects for SAP Dock Appointment Scheduling, and especially the authorization field User Process Scope for Dock Appointment Scheduling (/SCWM/DSPS). See Critical Roles and Authorization Combinations in Network and Communication Security [Page 43].
Maintaining Authorizations

Using the SAP Extended Warehouse Management (SAP EWM) component, you can assign users to various standard user roles. For more information, see the SAP EWM documentation under 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 the SAP EWM documentation under General Functions Authorizations.

If you are using SAP Dock Appointment Scheduling, ensure that you have read the information regarding roles for SAP Dock Appointment Scheduling. See Critical Roles and Authorization Combinations in Network and Communication Security [Page 43].
Maintaining Authorizations for Integration with SAP Components

Procedure

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

This is not relevant for standalone Dock Appointment Scheduling.

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 the SAP EWM documentation under Roles for Extended Warehouse Management (EWM).

For the integration from an ERP to an EWM system, for example, the role /SCWM/ERP_EWM_INTEGRATION exists.

For the integration from EWM to an ERP system, the corresponding RFC users also require the proper authorizations. For more information, see Note 727839.

In some cases, for example, for migration functions like transaction /SCWM/MIG_PRODUCT, the RFC enabled function module RFC_READ_TABLE is called on ERP side from EWM. For such scenarios, the corresponding RFC user requires this authorization. To avoid misuse, you should restrict the tables to be accessed to a minimum. You can therefore use the authorization objects S_TABU_NAM or S_TABU_DIS. For more information about which applications require which table accesses, see Note 1539105.

If you grant the usage of RFC function RFC_READ_TABLE to an RFC user, it is very important that you restrict the tables that can be accessed to a minimum to avoid misuse.

Maintaining Authorizations for Data Transfer to SAP NetWeaver Business Warehouse

This is not relevant for standalone Dock Appointment Scheduling.
Limiting Authorizations for Extraction

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

1. In Customizing for SAP EWM, choose ⇒ Integration with Other SAP Components ⇒ Data Transfer to Business 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 BW system for which you want no more data for this DataSource to be extracted.
5. In the Ex. 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 Data Transfer between SAP EWM Shipping and Receiving (S&R) and SAP Dock Appointment Scheduling

This is not relevant for standalone Dock Appointment Scheduling.

SAP Dock Appointment Scheduling and S&R are two independent components. But it is also possible to integrate the components, for example, so that the system communicates appointment status changes in SAP Dock Appointment Scheduling to S&R and appointment status changes in S&R to SAP Dock Appointment Scheduling. For more information, see the SAP EWM documentation under ⇒ SAP Dock Appointment Scheduling ⇒ Integration with SAP EWM.

For integration between SAP Dock Appointment Scheduling and S&R, the system uses queued Remote Function Call (qRFC) technology.

Using Standard Roles for SAP Dock Appointment Scheduling to SAP EWM Integration

For the integration from SAP Dock Appointment Scheduling to S&R, the technical role /SCWM/DAS_TO_EWM_INTEGRATION is available. It contains the necessary authorizations to update the relevant S&R objects. The role does not contain any menu entries or transactions, as it is only a technical role for Remote Function Call (RFC) communication. You must assign this role to the SAP Dock Appointment Scheduling user or RFC user, depending on if you use RFC communication, with which the integration is done.
Using Standard Roles for SAP EWM to SAP Dock Appointment Scheduling Integration

For the integration from S&R to SAP Dock Appointment Scheduling, the technical role /SCWM/EWM_TO_DAS_INTEGRATION is available. It contains the necessary authorizations to update the relevant Dock Appointment Scheduling objects. The role does not contain any menu entries or transactions as it is only a technical role for RFC communication. This role must be assigned to the SAP Dock Appointment Scheduling user or RFC user, depending on if you use RFC communication, with which the integration is done.

Maintaining RFC Authorizations for Internal Communication in SAP EWM

For RFC communication, users usually require the authorizations for authorization object S_RFC. As RFCs are potential security risks, you should be very restrictive in granting them.

In certain cases, SAP EWM also uses RFCs for internal purposes, for example for parallel processing or for asynchronous communication. For these purposes, no RFC authorizations have to be granted as these calls are within the SAP EWM system.

SAP EWM also uses specific RFC-enabled function modules, which are used to extract content from queued RFCs (qRFC). For example, these function modules are used to extract the warehouse number or delivery number from qRFCs.

These function modules do not perform data changes in SAP EWM and also do not return data to a caller. They are required for delivery processing and for displaying of message queue entries in the warehouse management monitor.

The function modules are in the following special function groups:

- /SCWM/CORE_MQ_REPLAY Message Queue Mon: Replay Functions
- /SCWM/CORE_RF_MQ_REPLAY Replay Function Modules for RF
- /SCWM/DELIVERY_MQ_REPLAY Replay Function Modules for Deliveries
- /SCWM/ERP_MQ_REPLAY Replay Function Modules - ERP Interface
- /SCWM/SR_MQ_REPLAY Replay Function Modules - S&R
- /SCWM/VAS_MQ_REPLAY Replay Function Modules for VAS
- /SCWM/WC_SERVICE_MQ_REPLAY Replay Function Modules for Workcenter
- /SCWM/WAVE_MGMT_MQ_REPLAY Replay Function Modules for Wave

If you use the message queue monitor node in the warehouse management monitor, you must add these function groups to authorization S_RFC. Use the activity Execute (16) and the Function Group (FUGR) type of RFC object.

For delivery and warehouse task processing, for example, confirming and creation of warehouse tasks, you must add the following function group to authorization S_RFC:

- /SCWM/DELIVERY_MQ_REPLAY Replay Function Modules for Deliveries

These authorizations are already in the standard roles in SAP EWM, so they are only relevant if you create your own roles.
Maintaining Authorizations for Enterprise Services

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 Management (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 the SAP NetWeaver Security Guide under Security Guides for Connectivity and Interoperability Technologies » Security Aspects for Web Services » Authorizations.
Session Security Protection

To increase security and prevent access to the SAP logon ticket and security session cookies, 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 clients using the transaction SICF_SESSIONS.

For more information, a list of the relevant profile parameters, and detailed instructions, see the SAP NetWeaver documentation under SAP NetWeaver Library: Function-Oriented View ➔ Security ➔ User Authentication and Single Sign-On ➔ Authentication Infrastructure ➔ AS ABAP Authentication Infrastructure ➔ Activating HTTP Security Session Management on AS ABAP ➔.
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 [Page 45]
  This topic describes the communication paths and protocols used by the SAP EWM component.

- Network Security [Page 48]
  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 49]
  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 SAP NetWeaver Security Guide under the following sections:

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

Collaborative Scenario using SAP Dock Appointment Scheduling

This is relevant only if you are using Dock Appointment Scheduling.

In a collaborative scenario, users from other companies, such as carriers, can access data from SAP Dock Appointment Scheduling. For example, carriers can create or view loading appointments. For this, such users require access the Dock Appointment Scheduling system from outside the company’s network.
If you use such a scenario, you must pay special attention to the network setup and zones or topology, for example, if firewalls, demilitarized zones, ports, should be used, and which ones.

For this collaboration, SAP Dock Appointment Scheduling uses Web Dynpro ABAP technology. For more information, see the following guides:

- Communication Channel Security [Page 45]
- Network Security [Page 48]
- Communication Destinations [Page 49]


**Mobile Access to Labor Demand Planning**

Labor Demand Planning offers the possibility to access data from a mobile device. The proposed usage is that these mobile applications are used within the company's firewall.

SAP Note 1894045 contains additional information about how these applications can be set up.

The application is built using a HTML5 UI. The system uses OData as the communication channel between the backend and the SAP UI5 frontend. The corresponding OData service is /SCWM/LM_LABOR_DEMAND_PLANNING.


If you are using the application outside of the company's firewall, which is not the proposed usage, you should ensure that minimal authorizations are used for accessing the SAP Netweaver Gateway and the SAP EWM system. Also, in such a case, you should consider the technical system landscape and setup proposals in the SAP Netweaver Gateway Security Guide.
**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 the SAP NetWeaver Security Guide under [Network and Communication Security ➤ Transport Layer Security ➤ Secure Network Communications (SNC)](http://service.sap.com/scm#SAP SCM in Detail ➤ Technology ➤ Architecture Overview).

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 in Detail ➤ Technology ➤ Architecture Overview](http://service.sap.com/scm#SAP SCM in Detail ➤ Technology ➤ Architecture Overview).

For more information about the communication security of SAP NetWeaver, see the SAP NetWeaver Security Guide under [Network and Communication Security](http://service.sap.com/scm#SAP SCM in Detail ➤ Technology ➤ Architecture Overview).

For more information about security aspects for connectivity and interoperability of SAP NetWeaver, see the SAP NetWeaver Security Guide under [Security Guides for Connectivity and Interoperability Technologies](http://service.sap.com/scm#SAP SCM in Detail ➤ Technology ➤ Architecture Overview).

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

<table>
<thead>
<tr>
<th>Communication Channel</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Application Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front-end client that uses SAP GUI for Windows for the application server</td>
<td>DIAG</td>
<td>All application and customizing data</td>
<td>All</td>
</tr>
<tr>
<td>SAP ERP</td>
<td>RFC and IDOC</td>
<td>Master data and transaction data</td>
<td>Not relevant for standalone Dock Appointment Scheduling</td>
</tr>
<tr>
<td>SAP SCM</td>
<td>RFC</td>
<td>ATP data</td>
<td>Not relevant for standalone Dock Appointment Scheduling</td>
</tr>
<tr>
<td>SAP SCM</td>
<td>RFC</td>
<td>Master data</td>
<td>Not relevant for standalone Dock Appointment Scheduling</td>
</tr>
<tr>
<td>SAP GTS</td>
<td>RFC</td>
<td>GTS-relevant data</td>
<td>Not relevant for standalone Dock Appointment</td>
</tr>
</tbody>
</table>
Scheduling

<table>
<thead>
<tr>
<th>Component</th>
<th>Data Sources</th>
<th>Required for Dock Appointment Scheduling</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver BW</td>
<td>RFC</td>
<td>Not relevant</td>
</tr>
<tr>
<td>SAP CRM</td>
<td>RFC and IDOC</td>
<td>Not relevant</td>
</tr>
<tr>
<td>Warehouse Control Units or PLCS</td>
<td>RFC, IDOC (depending on whether or not SAP plant connectivity is used)</td>
<td>Not relevant</td>
</tr>
<tr>
<td>Legacy systems</td>
<td>RFC, IDOC, HTTP, File</td>
<td>Depends on legacy scenario</td>
</tr>
<tr>
<td>SAP Plant Connectivity</td>
<td>RFC</td>
<td>Not relevant</td>
</tr>
<tr>
<td>Frontend client using a</td>
<td>HTTP/HTTPS</td>
<td>All</td>
</tr>
<tr>
<td>SAP NetWeaver Business Client</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>SAP Transportation Management</td>
<td>WebService / RFC</td>
<td>Not relevant</td>
</tr>
</tbody>
</table>

DIA 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 the SAP NetWeaver Security Guide under Network and Communication Security Transport Layer Security.

Note that many of the entries depend on the configuration and how SAP EWM is used. For example, usage of SAP GTS, SAP NetWeaver BW, 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 from SAP EWM, see the appendix of the EWM Application Operations Guide at http://service.sap.com/instguides SAP Business Suite Applications SAP SCM SAP EWM Using SAP EWM 9.1 Application Operations Guide for SAP EWM 9.1

Core Interface (CIF) – SAP ERP

This is not relevant for Dock Appointment Scheduling.
The integration of SAP EWM and SAP ERP is technically based on CIF. Since 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.

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 the SAP NetWeaver Security Guide under Network and Communication Security.

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 SCM in Detail Technology.

For more information about access control using firewalls, see the SAP NetWeaver Security Guide under Network and Communication Security Using Firewall Systems for Access Control.

Ports


For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see also the document TCP/IP Ports Used by SAP Applications, which can be found using the Search field on SAP Developer Network at http://sdn.sap.com/irj/sdn/security.
Communication Destinations

⚠️ 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 logon data for users of type system.
- Choose trusted system functionality whenever possible, rather than storing connection user logon data.

This is not relevant for standalone Dock Appointment Scheduling.

This is not relevant if the system does not use communication to external systems.

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

### Connection Destinations

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;EWM name&gt;CLNT&lt;client&gt;</td>
<td>No</td>
<td>RFC – ERP</td>
<td>Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.</td>
<td>For more information, see Customizing for SCM Basis under Integration &gt; Basic Settings for Creating the System Landscape &gt; Assign RFC Destinations to Various Application Cases</td>
</tr>
<tr>
<td>EWM to SAP ERP</td>
<td>No</td>
<td>qRFC</td>
<td>Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.</td>
<td>For more information, see Customizing for Extended Warehouse Management under Interfaces &gt; ERP Integration &gt; General Settings &gt; Control for RFC Queue and Customizing for SCM Basis</td>
</tr>
<tr>
<td>Integration</td>
<td>Basic Settings for Creating the System Landscape</td>
<td>Assign RFC Destinations to Various Application Cases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EWM to SAP APO (APO instance)</td>
<td>No</td>
<td>RFC – ERP</td>
<td>Use the Profile Generator (transaction PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839. For more information, see Customizing for Extended Warehouse Management under Goods Receipt Process Slotting General Settings Change Information for APO Instances.</td>
<td></td>
</tr>
<tr>
<td>EWM to Third party geocoding application</td>
<td>No</td>
<td>RFC</td>
<td>None</td>
<td>For more information, see Customizing for SAP NetWeaver under General Settings Set Geocoding or SAP Help Portal at <a href="http://help.sap.com/ewm">http://help.sap.com/ewm</a> SAP EWM 9.1 Application Help English SAP Library for SAP Extended Warehouse Management (EWM) SCM Basis SCM Basis Master Data Location.</td>
</tr>
<tr>
<td>EWM to Non-SAP Systems</td>
<td>No</td>
<td>RFC – ERP</td>
<td>None</td>
<td>For more information, see Customizing for Extended Warehouse Management under Interfaces Non-SAP Systems Connect Subsystem.</td>
</tr>
<tr>
<td>EWM to SAP GTS</td>
<td>No</td>
<td>RFC –</td>
<td>None</td>
<td>For more information, see Customizing for Extended Warehouse Management under Interfaces GTS Integration Basic Settings of GTS Integration.</td>
</tr>
<tr>
<td>EWM to SAP NetWeaver Business Warehouse (SAP NetWeaver BW)</td>
<td>No</td>
<td>RFC – ERP</td>
<td>None</td>
<td>For more information, see Customizing for SAP ERP under Integration with Other SAP Components Data Transfer to Business Warehouse and Customizing for Extended Warehouse Management under Interfaces SAP Business Information Warehouse.</td>
</tr>
<tr>
<td>EWM to SAP Plant Connectivity</td>
<td>No</td>
<td>RFC</td>
<td>None</td>
<td>This function is only available if you implement the sample implementation.</td>
</tr>
</tbody>
</table>
For more information, see Customizing for Extended Warehouse Management under Business Add-Ins (BAdIs) for Extended Warehouse Management > Master Data > Work Center > Adjust User Interface for Work Center > BAdI: Determination of HU Weight Using Scale.

<table>
<thead>
<tr>
<th>SAP EWM to SAP TM</th>
<th>Yes</th>
<th>WebService</th>
<th>None</th>
</tr>
</thead>
</table>

For more information about communication destinations of SAP NetWeaver, see the SAP NetWeaver Security Guide under 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 services are available:

- **RFUI**
  
  This is not relevant for standalone Dock Appointment Scheduling.

  - **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 the SAP EWM documentation under `Radio Frequency Framework > Work Processing Using Radio Frequency > Resource Management Using Radio Frequency`.

- **SAP Dock Appointment Scheduling Applications**

  **Path:** `/default_host/sap/bc/webdynpro/scwm/`

  The services are as follows:

  - **DSAPP_APPT:** Process Appointments – Textual
  - **DSAPP_APPT_VISUAL:** Monitor Appointments
  - **DSAPP_LIST:** Maintain Appointments in Textual View
  - **DSAPP_LIST_VISUAL:** Maintain Appointments in Graphical View
  - **DSAPP_MAINT:** Direct Access to Appointment – Textual
  - **DSAPP_MAINT_VISUAL:** Direct Access to Appointment – Graphical
  - **DSDL_MAINT:** Docking Location Maintenance
  - **DSSL_MAINT:** Loading Point Maintenance
  - **DSSL_DEL_ACC:** Delete Time Slots
  - **DSSL_GEN:** Create Time Slots in Graphical View
  - **DSSL_GEN_ACC:** Create Time Slots in Textual View
  - **DSSL_MAINT:** Change Time Slots in Graphical View
  - **DSSL_MAINT_ACC:** Change Time Slots in Textual View
  - **DSS_SETUP:** Simple Setup
  - **DS_CARR_PLAN_ASGN:** Maintain Planners for Carrier
  - **WDCC_DS_REPORTING:** DAS Reporting: Show Appointment Data

- **Applications used in an integrated scenario for Dock Appointment Scheduling and Shipping and Receiving**

  **Path:** `/default_host/sap/bc/webdynpro/scwm/`

  The services are as follows:

  - **SHP_ASSIGN_DOOR_LP:** Assign Doors to Loading Point
  - **SHP_ASSIGN_TU_DOOR:** Assign Transportation Unit to Door

- **Applications used for the collaborative Dock Appointment Scheduling scenario**
The services are as follows:

- **DSAPP_LIST**: Maintain Appointments in Textual View
- **DSAPP_MAINT**: Direct Access to Appointment – Textual

Note that these services can be used for internal access as well as for collaborative scenarios involving access from outside the company’s network. Therefore you must pay special attention when activating these services for external access.

### Applications used in Shipping and Receiving

Path: /default_host/sap/bc/webdynpro/scwm/

The services are as follows:

- **SCO**: Shipping Cockpit
- **SCO_EXEC**: Shipping Cockpit Execution

### Applications used in tool-based ERP integration

Path: /default_host/sap/bc/webdynpro/scwm/

The services are as follows:

- **WD_IT_GUIDE_ERP_1**: EWM: Implementation Tool for ERP System Connection
- **WD_IT_GUIDE_ERP_3**: EWM: Implementation Tool ERP Integration: Warehouse Integration

### Applications used for mobile access to Labor Demand Planning

Path: /default_host/sap/bc/ui5_ui5/scwu/

The services are as follows:

- **LM_LDP**: Labor Demand Planning

Use the transaction SICF to activate this service.

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

For more information, see the SAP NetWeaver Documentation under SAP NetWeaver Library: Function-Oriented View > Application Server > Application Server Infrastructure > Connectivity > Components of SAP Communication Technology > Communication Between ABAP and Non-ABAP Technologies > Internet Communication Framework > Development > Server-Side Development > Creating and Configuring ICF Services > Activating and Deactivating ICF Services.

For more information about ICF security, see the SAP NetWeaver Security Guide under Security Guides for Connectivity and Interoperability Technologies > RFC/IFC Security Guide.
Data Storage Security

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

For more information about the data storage security of SAP NetWeaver, see the SAP NetWeaver Security Guide under Security Guides for the 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

This is not relevant for standalone Dock Appointment Scheduling.

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 explicitly to 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

To enable the validation of physical filenames, the following logical filenames have been created:

- 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 path 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

Transactions/programs using this logical filename:

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

Parameters and format used in this context:

- \(<\text{PARAM}_1\>=\text{Warehouse number} \ (\text{CHAR}4)\)

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.

- EWM_PRODUCT_UPLOAD

Transactions/programs using this logical filename:

- /SCWM/MIG_PRODUCT
- Program /SCWM/R_MIG_PRODUCT

Logical file path used:

- EWM_PRODUCT_UPLOAD_PATH

- EWM_PACKSPEC_UPLOAD

Transactions/programs using this logical filename:

- Transaction /SCWM/MIG_PRODUCT and /SCWM/IPU
- Program /SCWM/R_MIG_PRODUCT and /SCWM/R_PS_DATA_LOAD

Logical file path used in this context:

- EWM_PACKSPEC_UPLOAD_PATH

- EWM_PI_COMPL_UPLOAD

Transactions/programs using this logical filename:

- /SCWM/MIG_PI_COMPL
- Program /SCWM/R_MIG_PI_COMPL

Logical file path used:

- EWM_PI_COMPL_UPLOAD_PATH

**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 the following:

- The SAP NetWeaver documentation under SAP NetWeaver Library: Function-Oriented View > Application Server > Application Server ABAP > Other Services > Services for Application Developers > Logical File Names
Security for Additional Applications

Geocoding

This is not relevant for standalone Dock Appointment Scheduling.

The SAP Extended Warehouse Management (SAP EWM) component can, in some cases, make use of third party geocoding applications, for example, PTV eServer. The software could be used, for example, to calculate geographical information for the locations or distances for transportation lanes. To connect to the third party software, this software may require an RFC destination on the SAP EWM side. This RFC is described in the Communication Destinations [External] chapter.

For more information on geocoding, see SAP Help Portal at http://help.sap.com/ewm SAP Extended Warehouse Management 9.1 Application Help SAP Library. In SAP Library, choose SCM Basis SCM Basis Master Data Location. For any security issues regarding the third party application, for example, PTV eServer software, see the third party documentation.

Plant Connectivity for Scale Integration

This is not relevant for standalone Dock Appointment Scheduling.

The SAP Extended Warehouse Management (SAP EWM) component can, in some cases, integrate an external scale. The software could be used, for example, to calculate the weight of a handling unit. In BAdi: Determination of HU Weight Using Scale (/SCWM/EX_WRKC_UI_GET_WEIGHT), a sample implementation exists for this. In this example, the system uses SAP Plant Connectivity to integrate an external scale. This software may require an RFC destination on the SAP EWM side to connect to the SAP Plant Connectivity. For more information, see Communication Destinations [Page 49].

Enterprise Services Security

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

- User Administration and Authentication
- Network and Communication Security
- SAP NetWeaver Process Integration Security Guide
- Security Guide Web Services
- Security Aspects for Web Services
- Security Guides for the Operating System and Database Platforms
- Security Aspects for Lifecycle Management
- Security Guides for the AS ABAP
- Security Guides for the AS Java

For more information about special security requirements for web services, see the SAP NetWeaver Security Guide under Security Guides for Connectivity and Interoperability Technologies ➔ Security Aspects for Web Services ➔.
Other Security-Relevant Information

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

- User Frontend [Page 62]
- Data Protection and Privacy [Page 64]
User Frontend

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.

SAP NetWeaver Business Client

SAP Netweaver Business Client is the proposed UI for using Web Dypro applications, for example, from SAP Dock Appointment Scheduling or Shipping Cockpit in SAP EWM.

For more information about SAP Netweaver Business Client, see SAP Note 900000.


Making Browser Settings for Easy Graphics Framework (EGF)

This is not relevant for standalone Dock Appointment Scheduling.

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 the SAP EWM documentation under Monitoring Easy Graphics Framework.

RF Device as a User Frontend

This is not relevant for standalone Dock Appointment Scheduling.

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.


SAP Dock Appointment Scheduling
This is relevant only if you are using Dock Appointment Scheduling.

If you use the applications *Create Time Slots in Graphical View*, *Change Time Slots in Graphical View*, or *Maintain Appointments — Graphical*, you must install Microsoft® Silverlight® version 5 or later.

**Access from Mobile Device using OData and Gateway**

Labor Demand Planning offers the possibility to access data from a mobile device. The UI uses SAP NetWeaver Gateway to access SAP EWM data. For more information, see *Network and Communication Security* [Page 43].
Data Protection and Privacy

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 various 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 the SAP NetWeaver Security Guide under Security Aspects for Lifecycle Management Auditing and Logging.

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 time stamp

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 NetWeaver under 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 the SAP NetWeaver Security Guide under Security Aspects for Lifecycle Management Auditing and Logging Audit Information System (AIS).

SAP EWM

This is not relevant for standalone Dock Appointment Scheduling.

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).

<table>
<thead>
<tr>
<th>Customizing Activity</th>
<th>Path in Customizing for SAP EWM</th>
</tr>
</thead>
</table>

The following transactions are relevant for SAP EWM auditing and logging (in each of these transactions, you can use the Open Advanced Search pushbutton on the screen for that transaction, to retrieve and display archived report data):
<table>
<thead>
<tr>
<th>Transaction Description</th>
<th>Menu Path in the SAP EWM System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain Inbound Delivery</td>
<td>On the SAP Easy Access screen, choose <strong>Extended Warehouse Management</strong> ➔ <strong>Delivery Processing</strong> ➔ <strong>Inbound Delivery</strong> ➔ <strong>Maintain Inbound Delivery</strong>.</td>
</tr>
<tr>
<td>Maintain Expected Goods Receipt</td>
<td>On the SAP Easy Access screen, choose <strong>Extended Warehouse Management</strong> ➔ <strong>Delivery Processing</strong> ➔ <strong>Inbound Delivery</strong> ➔ <strong>Expected Goods Receipt</strong> ➔ <strong>Maintain Expected Goods Receipt</strong>.</td>
</tr>
<tr>
<td>Maintain Outbound Delivery Order</td>
<td>On the SAP Easy Access screen, choose <strong>Extended Warehouse Management</strong> ➔ <strong>Delivery Processing</strong> ➔ <strong>Outbound Delivery</strong> ➔ <strong>Maintain Outbound Delivery Order</strong>.</td>
</tr>
<tr>
<td>Maintain Posting Change</td>
<td>On the SAP Easy Access screen, choose <strong>Extended Warehouse Management</strong> ➔ <strong>Delivery Processing</strong> ➔ <strong>Posting Change</strong> ➔ <strong>Maintain Posting Change</strong>.</td>
</tr>
<tr>
<td>Maintain Internal Stock Transfer</td>
<td>On the SAP Easy Access screen, choose <strong>Extended Warehouse Management</strong> ➔ <strong>Delivery Processing</strong> ➔ <strong>Maintain Internal Stock Transfer</strong>.</td>
</tr>
</tbody>
</table>
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 that 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 monitor a system landscape for compliance with predefined settings continuously, 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 nontrivial Gateway configuration or making sure that standard users do not have default passwords.

Security in the Run SAP 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
- Comprehensive list of Security Notes: http://service.sap.com/securitynotes
- Configuration Validation: http://service.sap.com/changecontrol
- Run SAP Roadmap, including the Security and the Secure Operations Standard: http://service.sap.com/runsap (See the Run SAP chapters 2.6.3, 3.6.3 and 5.6.3)
Virus Check of Document Attachments

This is not relevant for standalone Dock Appointment Scheduling.

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 NetWeaver under Application Server > System Administration > Virus Scan Interface.
Appendix

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 following table:

**Quick Links to Related Information**

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on SAP Service Marketplace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides</td>
<td><a href="http://service.sap.com/instguides">http://service.sap.com/instguides</a></td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td><a href="http://service.sap.com/notes">http://service.sap.com/notes</a></td>
</tr>
<tr>
<td>Released platforms</td>
<td><a href="http://service.sap.com/platforms">http://service.sap.com/platforms</a></td>
</tr>
<tr>
<td>Network security</td>
<td><a href="http://service.sap.com/securityguide">http://service.sap.com/securityguide</a></td>
</tr>
<tr>
<td>Technical infrastructure</td>
<td><a href="http://service.sap.com/installnw74">http://service.sap.com/installnw74</a></td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td><a href="http://service.sap.com/solutionmanager">http://service.sap.com/solutionmanager</a></td>
</tr>
<tr>
<td>SAP Supply Chain Management</td>
<td><a href="http://service.sap.com/scm">http://service.sap.com/scm</a></td>
</tr>
</tbody>
</table>