SAP SCM 5.0 Component Security Guide

Release SAP SCM 5.0
and SAP SCM ES 5.0

Copyright

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Typographic Conventions

Type Style	Description
Example text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

SAP SCM 5.0 Component Security Guide

Introduction

This guide does not replace the daily operations handbook that SAP recommends that customers create for their specific productive operations.

About This Guide

This Component Security Guide provides security-relevant information for the component SAP Supply Chain Management 5.0 (SAP SCM 5.0). It covers the following parts of the component:

- SAP SCM 5.0 Server
  - SAP Advanced Planning and Optimization (SAP APO)
    - SAP liveCache
    - SAP APO Optimizer (optional SAP APO component)
  - SAP Event Management (SAP EM)
  - SAP Inventory Collaboration Hub (SAP ICH)
  - Embedded SAP BW 3.5 (only used and required for the SAP APO 5.0 component within SAP SCM 5.0)
- SAP SCM Web Communication Layer 5.0 (SAP SCM WCL)
- SAP Forecasting and Replenishment 5.0 (SAP F&R)
- (Third party software: PTV eServer for SAP SCM 5.0)
- Enterprise services add-on SAP SCM ES 5.0

In many cases the required information has already been provided in other Security Guides and in Configuration and Installation Guides. In these cases, this Security Guide provides references to the relevant sections of the respective guides.

The following table provides an overview of all related Security Guides for this component. For the Security Guides mentioned below, see the SAP Help Portal at **`help.sap.com`** → *Documentation* → *SAP NetWeaver* → *SAPNetWeaver 2004s* → *English* or *German* → *SAP Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide.*

All the Security Guides are also available at **`http://service.sap.com/securityguide`**.

Related Security Guides

Product	**See**
Operating System and Database Platforms	
Operating System and Database Platforms	SAP NetWeaver 2004s DB and OS Platform Security Guides
Application Platform	

SAP Web Application Server	SAP Web AS Security Guide for ABAP Technology SAP Web AS Security Guide for J2EE Technology Internet Transaction Server Security Security Aspects in Development
SAP Content Server	SAP Content Server Security Guide
SAP Knowledge Warehouse	SAP Knowledge Warehouse Security Guide
People Integration	
SAP Enterprise Portal	SAP Enterprise Portal Security Guide
SAP Mobile Infrastructure	SAP Mobile Infrastructure Security Guide
Information Integration	
SAP Business Information Warehouse Security Guide	SAP Business Information Warehouse Security Guide
SAP Knowledge Management	SAP Knowledge Management Security Guide SAP Content Management Security Guide SAP Trex Security Guide
Process Integration	
SAP Exchange Infrastructure	SAP Exchange Infrastructure Security Guide
Solution Life-Cycle Management	
System Management	Security Aspects with System Management

This Component Security Guide often provides references to other documentation. You can find this security-relevant documentation for the SAP SCM component as follows:

Guide/Documentation	Full Path to the Guide
SAP NetWeaver Security Guide	**help.sap.com** → *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *English* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide*
SAP NetWeaver Documentation	**help.sap.com** → *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *English* or *German* → *SAP Library* → *SAP NetWeaver by Key Capability.*
SAP SCM Master Guide	**service.sap.com/instguides** → *mySAP Business Suite Solutions* → *mySCM* → *Using SAP SCM 5.0 Server* → *Master Guide SCM 5.0*
SAP SCM Documentation	**help.sap.com** → *Documentation* → *mySAP Business Suite* → *SAP Supply Chain Management* → *SAP SCM 5.0* → *English* or *German* → *SAP Supply Chain Management (SAP SCM)*
SAP SCM Installation Guide	**service.sap.com/instguides** → *mySAP Business Suite Solutions* → *mySAP SCM* → *Using SAP SCM 5.0 Server* → *Installation Document SCM 5.0*

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 of your system should not result in loss of information, or reductions in processing time. These demands on security also apply to the SAP SCM 5.0 component. To assist you in securing your SAP SCM 5.0 component, we have provided this SAP SCM 5.0 Component Security Guide.

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

Target Groups

- Technical consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Those guides are only relevant for a specific phase of the software life cycle, whereas the Security Guides provide information that is relevant for all timeframes.

Important SAP Notes

Check regularly to see which SAP Notes are available concerning the security of the application.

Important SAP Notes

SAP Note Number	Title	Comment
700659	Security Guide: mySAP Supply Chain Management	Problems discovered after publication of Security Guide and additional information concerning security issues.
138498	Single Sign-On Solutions	Information about Single Sign-On solutions for SAP systems
184504	Syntax for storing user data was changed from liveCache version 7.1 to 7.2.	
447543	APO: Authorizations too comprehensive/not user-specific	
669496	SCM 4.1 upgrade: Additional authorization objects/checks, changes and corrections	
724095	SDP Selector (Interactive SNP Planning): Authorization check for location products	
400434	Authorizations in APO	A brief explanation of the

	Demand Planning	concept behind authorizations in SAP APO for Demand Planning
687399	SP09: Authorization problem after you jump from Alert Monitor to detailed scheduling planning board	
727839	Authorizations required for the RFC user are not known for the SAP SCM – SAP R/3 DIMP Integration.	
637052	Missing authorization object for database views	
619086	Input help in authorization maintenance of parameters missing (for SAP Event Manager)	
498627	Global ATP: No logoff of user RFC_USER from APO system	
305634	Initialization of liveCache across multiple clients.	
616555	LiveCache password changes	The passwords of the standard liveCache user, the database system administrator, the DBM user, should be changed in the liveCache environment.
25591	Database user passwords.	The SAP R3 user password is to be changed.
452745	New authorization concept for transaction LC10	
683528	Security gaps in SAP DB	This note provides information about the secure operation of SAP DB/MaxDB and liveCache.
30724	Data protection and security in SAP systems (in R/3 in particular)	
128447	Setting up Trusted/Trusting System relationship between two SAP systems	Needed for Customizing of trusted/trusting system RFC connections.
389220	Certificate request reply cannot be inserted	
307356	Installation of SNC for the Internet Transaction	
110600	SAP Security Library (SAPSECULIB)	
662340	SSF Encryption Using the SAPCrytolib	The SAP Cryptographic Library has to be used for encrypting data in the SAP

		system.
506314	SAPHTTP and SSL	You want to set up a secure connection (SSL) to the Web server, with SAPHTTP.
792366	Subsequent implementation of a security level for documents	Knowledge Provider: what needs to be taken into account, application of the Knowledge Provider (KPro) decides to change the security level for documents for one or more of their PHIO classes.
629947	IisProxy: Release Notes and known issues	To be used when you have problems with the IisProxy ISAPI module for IIS
598860	Browsers supported by the HTMLB BSP Extensions	
616900	BSP FAQ – Frequently Asked Questions	
517860	Pre-connected log-on screen for BSP application screen	
510007	Setting Up SSL on the Web Application Server	
612670	SSO for local BSP calls using SAP GUI HTML control	
866317	No authorization to save/delete the selection	
821200	Standard liveCache user must be known to the DBM server	
910307	Security Note: ICH Input-Output Validation	
914920	Security Note: Input-Output Validation in APO CLP	Web servers that receive input parameters through http, and then create dynamic HTML pages, and send content to clients (Browsers), are susceptible to cross-site scripting attacks.
938252	Security Note: Information, Sensitive information	

For more SAP Notes about security, see the SAP Service Marketplace at **`service.sap.com/security`** → *SAP NetWeaver* → *SAP NetWeaver in Detail* → *Security* → *SAP Security Notes*.

Technical System Landscape

The following table lists where you can find more information about the technical system landscape:

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace (service.sap.com/)
Technical System Landscape	SCM Master Guide	**/Instguides** *(Installation & Upgrade Guides → mySAP Business Suite Solutions → mySAP SCM → Using SAP SCM 5.0 Server → Master Guide).*
Technical System Landscape & Installation	SCM Installation Guide(s)	**/Instguides** *(Installation & Upgrade Guides → mySAP Business Suite Solutions → mySAP SCM → Using SAP SCM 5.0 Server → Inst.Guide for SCM 5.0).*
Technical Configuration, High Availability	Technical Infrastructure Guide	**ti**
Security	Security Guide	**security**

User Administration and Authentication

User Management

User Management Tools

Tool	Detailed Description
User Management for the ABAP Engine (transaction SU01)	Use the user management transaction SU01 to maintain users in ABAP-based systems.
Profile Generator (transaction PFCG)	Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.
Central User Administration (CUA)	Use the CUA to centrally maintain users for multiple ABAP-based systems. Synchronization with a directory server is also supported.

User Management Engine (UME) administration console	Use the Web-based UME administration console to maintain users, roles and authorizations in Java-based systems that use the UME for the user store, for example, the SAP J2EE Engine and the Enterprise Portal. The UME also supports various persistency options, such as the ABAP Engine or a directory server.
SAP J2EE Engine user management using the Visual Administrator	Use the Visual Administrator to maintain users and roles on the SAP J2EE Engine. The SAP J2EE Engine also supports a pluggable user store concept. The UME is the default user store.

For a detailed description of the user management tools available in SAP NetWeaver, see the SAP NetWeaver Security Guide at **service.sap.com/securityguide** → *SAP NetWeaver* → *SAP NetWeaver in Detail* → *Security* → *Security in Detail* → *SAP Security Guides* → *SAP NetWeaver 2004s (Complete)* → *User Administration and Authentication* → *User Management* → *User Management Tools.*

Users

System	User	Delivered?	Type	Default Password	Detailed Description
SAP SCM 5.0 Server	<sapsid>adm	Yes	SAP System Administrator	To be entered	*SAP SCM Installation Guide → Installation Document - SCM Server 5.0 → <relevant Operating System/DB> → Installation Documentation*.
SAP SCM 5.0 Server	SAPService <sapsid>	Yes	SAP System Service Administrator	To be entered	*SAP SCM Installation Guide → Installation Document - SCM Server 5.0 <Operating System/DB> → Input for the Installation.*
SAP WebAS	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	Yes	See SAP NetWeaver Security Guide	See SAP NetWeaver Security Guide	*SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server ABAP Security Guide → User Authentication →*

					Protecting Standard Users
SAP WebAS	SAP Standard J2EE Users (Administrator, Guest, Emergency)	Yes	See SAP NetWeaver 2004s Security Guide	See SAP NetWeaver 2004s Security Guide	*SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server Java Security Guide → User Administration and Authentication → User Administration and Standard Users → Standard Users and Standard User Groups*
SAP J2EE Engine	SAPJSF	Yes	Communication user	To be entered	*SAP SCM Installation Guide → Installation Document - SCM Server 5.0 <Operating System/DB> → Installation Process → Input for the Installation.*
SAP SCM 5.0	RFC communication users (you will need an RFC communication user for each RFC destination in the chapter *Communication Destination*)	No	Communication user	The authorizations of the user will depend on the business case. For more information, see Authorizations [Page 15] in this Security Guide.	Communication Destinations [Page 33] and Authorizations [Page 15].
SAP SCM 5.0	Business processing users (you will need a user in each component, for each employee working with the system)	No	Dialog user	To be entered	SAP SCM 5.0 documentation and Authorizations [Page 15].
SAP liveCache	<lcid>adm	Yes	Operating system user	To be changed	*SAP SCM Installation Guide: Installation*

					Document - SCM Server 5.0 <Operating System/DB> → Post Installation Activities → Changing Passwords of Created Users; and SAP Notes 25591 and 616555.
SAP liveCache	SAP<SAPSID> liveCache database owner	Yes	MaxDB database user	To be changed	*SAP SCM Installation Guide: Installation Document - SCM Server 5.0 <Operating System/DB> → Post Installation Activities → Changing Passwords of Created Users,* and SAP Notes 25591 and 616555.
SAP liveCache	CONTROL liveCache database manager operator	Yes	MaxDB database user	To be changed	*SAP SCM Installation Guide: Installation Document - SCM Server 5.0 <Operating System/DB> → Post Installation Activities → Changing Passwords of Created Users,* and SAP Notes 25591 and 616555.
SAP liveCache	SUPERDBA liveCache administration user	Yes	MaxDB database user	To be changed	*SAP SCM Installation Guide: Installation Document - SCM Server 5.0 <Operating System/DB> → Post Installation Activities → Changing Passwords of Created Users* and SAP Notes 25591 and 616555.
SAP Event Manage-ment	SAP Event Management users	No	Dialog user	To be entered	*SAP SCM Documentation → SAP Event Management (SAP*

(EM)					*EM) → Supply Chain Coordination → SAP Event Management User*.
SAP SCM WCL	WCL administration user	No	Dialog user	To be entered	*SAP SCM Installation Guide: Installation/Upgrade Guide – SAP WCL → Post Installation → Configuring the Administration User on the SAP SCM Server* and *Configuring the Connection User Role on the SAP SCM Server*
SAP SCM WCL	SAP Event Management connection user	No	Communication user	To be entered	*SAP SCM Installation Guide: Installation/Upgrade Guide – SAP WCL → SAP SCM – WCL Specific Information → SAP SCM – WCL Configuration Parameters.*
SAP SCM WCL	SAP SCM WCL user	No	Dialog user	To be entered	Authorizations [Page 15]

For more information about user types, see the *SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → SAP NetWeaver Application Server ABAP Security Guide → NetWork Security for SAP Web AS ABAP.*

For more information about SAP NetWeaver standard users, see the *SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server ABAP Security Guide → User Authentication → Protecting Standard Users.*

For more information about SAP NetWeaver password rules, see the *SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → SAP NetWeaver Application Server ABAP Security Guide → User Authentication → Authentication and Single Sign-On → Logon and Password Security in the SAP System → Password Rules.*

User Data Synchronization

To avoid administrational effort, you can use user data synchronization in your system landscape. As the component SAP SCM 5.0 is based on SAP NetWeaver 2004s, all the mechanisms for user data synchronization of SAP NetWeaver 2004s are available for SAP SCM 5.0.

For information about user data synchronization, see the *SAP NetWeaver 2004s Security Guide → User Administration and Authentication → Integration of User Management in Your System Landscape*

Integration into Single Sign-On Environments

The integration into Single Sign-On environments of the component SAP SCM 5.0 is based on the integration model implemented in SAP NetWeaver.

For more information about integration into Single Sign-On environments based on SAP NetWeaver, see the SAP NetWeaver 2004s Security Guide at http://service.sap.com/security → *SAP NetWeaver in Detail → Security → Security in Detail → SAP Security Guides → SAP NetWeaver 2004s Security Guides (Complete) → SAP NetWeaver 2004s Security Guide → User Administration and Authentication → User Authentication and Single Sign-On → Integration into Single Sign-On Environments.*

For more information about authentication on the SAP Web application server ABAP, see the *SAP NetWeaver 2004s Security Guide → SAP NetWeaver Application Server ABAP Security Guide → User Authentication.*

Authorizations

The authorization concept of the component SAP SCM 5.0 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 **help.sap.com** → *Documentation → SAP NetWeaver → SAP NetWeaver 2004s → English → SAP Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → Users and Roles (BC-SEC-USR) → SAP Authorization Concept.*

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

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

For information about role maintenance and the Profile Generator, see *SAP NetWeaver by Key Capability → Security → Identity Management → Users and Roles (BC-SEC-USR) → SAP Authorization Concept → Organizing Authorization Administration → Organization if You Are Using the Profile Generator → Role Maintenance.*

With the component SAP SCM 5.0, SAP delivers SAP standard roles to cover the most-used business cases. These roles can be used as examples, or as a copy master for your own roles.

You can find the SAP standard roles in the Profile Generator (transaction code PFCG) using input help. You can use search terms to restrict the selection to the required standard roles (for example, the search term *APO* lists all APO-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.

Some of the components in SAP SCM 5.0 have additional authorization methods. The relevant components and the Implementation Guide (IMG) activities are shown in the following sections.

SAP strongly recommends 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 strongly weaken the overall security concept in your production system.

Roles in SAP SCM

For information about roles in SAP SCM, see the SAP Help Portal at **`help.sap.com`** → *mySAP Business Suite → SAP Supply Chain Management (SAP SCM) → Roles in SAP SCM.*

Authorizations for SCM-Basis

There are authorizations available for SCM Basis.

Authorization object /SCMB/PESL – Define PSM Selection

The system uses the authorization object /SCMB/PESL on the *Define Selection* screen of the Planning Service Manager. The authorization object enables the specified user to save and delete his or her selections.

Defined fields

The fields ACTVT and USER are available for the maintenance of authorization object /SCMB/PESL.

- You can choose the following activities for the ACTVT fields:
  - 06 (Delete): Delete a Selection
  - 34 (Save): Save a Selection (Create and Change)

- In the USER field you can enter the user for whose selection you want to execute the activities in the ACTVT field.

Maintaining Authorizations for SAP APO

Procedure

You use this to maintain authorizations for SAP Advanced Planning & Optimization (SAP APO).

Maintaining Master Data

1. To define iPPE user profiles, in the mySAP SCM Implementation Guide (IMG), choose *Advanced Planning and Optimization* → *Master Data* → *Integrated Product and Process Engineering (iPPE)* → *Settings for the iPPE Workbench Professional* → *Define User Profiles for the iPPE Workbench Professional*.
2. You can change the iPPE user profiles defined by SAP in this IMG activity by changing, copying, renaming, or creating new user profiles.

   The SAP standard system includes the following user profiles:

Standard User Profiles

User profile	Explanation
S_PPEALL (Total Display)	This profile includes all the settings you need to work with the iPPE Workbench.
S_ASTACT (Process Structure)	Part of the S_PPEALL profile; calls up a process structure as an application tree in the detail area of the iPPE Workbench.
S_ASTCMP (Product Structure)	Part of the S_PPEALL profile; calls up a product structure as an application tree in the detail area of the iPPE Workbench.
S_ASTFLO (Factory Layout)	Part of the S_PPEALL profile; calls up a line structure as an application tree in the detail area of the iPPE Workbench.

3. Change, copy, and rename the profiles, or create new profiles with the following options:
   - Model Definitions:

     Here you define how the model definitions between the objects are displayed in the navigation area.
   - PLM Environment:

     Here you define how objects from the Product Lifecycle Management (PLM) environment are displayed in the navigation area of the iPPE Workbench.
   - Reports

Here you define which reports will be available for this profile in the iPPE Workbench Professional. You can only choose reports that you have already defined in the activity *Define Reports for the Reporting Tree*.

4. Save your entries.

Maintaining Authorizations for Supply Chain Planning

1. To specify the person (planner) responsible, in the mySAP SCM IMG, choose *Advanced Planning and Optimization* → *Supply Chain Planning* → *Specify the Person (Planner) Responsible*.
2. To assign planning privileges to planners, you have to maintain each application for which each planner is responsible as follows:
   a. Choose *New Entries*.
   b. Enter an identifier and description for each planner.
   c. Select each area for which you want the planner to have privileges.
3. Save your entries.

Maintaining Authorizations for Supply Network Planning (SNP) and Demand Planning (DP): Configuring Planning Books

Starting with SAP SCM 4.1 (and continuing with SAP SCM 5.0), planning books within Supply Network Planning (SNP) and Demand Planning (DP) have a new authorization concept. The main advantage is that the creation of the modification of planning books can now be controlled by authorizations, and no longer by the system change option for the SAP_APO component.

For more information about the new authorization concept, see SAP Note 400434.

See also SAP Note 386021 for changes between SAP SCM 4.1 and SAP SCM 4.15 regarding the authorization concept for planning books.

Trace reads / gateway user

The optimizers of SAP APO write traces (or dumps) on the local hard disc of the optimization server. The log folder of the local RFC Gateway is used. To protect this data, the read to the traces should be restricted to the gateway user.

Passwords / RFC interface

APO no longer uses passwords. Rather, access is over RFC interfaces.

Authorizations for Service Parts Planning

Assigning Planners in SPP

In *Service Parts Planning (SPP)* you can assign users to various planners on the location product level. For more information, see the SPP documentation at **service.sap.com** → *mySAP Business Suite → SAP Supply Chain Management (SAP SCM) → SAP Advanced Planning and Optimization (SAP APO) → Service Parts Planning (SPP) → Master Data and General Functions for SPP → Assigning Planners in Service Parts Planning.*

Roles in SPP

For information about roles in SPP, see the SCM documentation at **service.sap.com** → *mySAP Business Suite → SAP Supply Chain Management (SAP SCM) → Roles in SAP SCM → Roles for Service Parts Planning (SPP)..*

Authorizations for Extended Warehouse Management

SAP Extended Warehouse Management (SAP EWM)

Standard User Roles:

- /SCWM/ADMIN (EWM: Warehouse Management Administrator)
- /SCWM/DELIVERY_FULL
- /SCWM/EXPERT (EWM: Warehouse Expert)
- /SCWM/INFORMATION (EWM: Warehouse Information)
- /SCWM/MANAGER (EWM: Warehouse Management Manager)
- /SCWM/STANDARD (EWM: Warehouse Standard Activity Role)

- /SCWM/SUPERVISOR (EWM: Warehouse Supervisor)
- /SCWM/INBD_SPECIALIST (EWM: Warehouse Specialist Inbound)
- /SCWM/OUTBD_SPECIALIST (EWM: Warehouse Specialist Outbound)
- /SCWM/YARD_SPECIALIST (EWM: Yard Specialist)
- /SCWM/WORKER (EWM: Warehouse Worker)
- /SCWM/INVENTORY_PLANNER (EWM: Physical Inventory Planner)
- /SCWM/COUNTER (EWM: Physical Inventory Counter)

Maintaining Authorizations for SAP Event Management (SAP EM)

Use

Assigning Users to Scenarios

In SAP EM, you must assign users to scenarios. By assigning users to scenarios, you specify that the system displays to the user only those parameters and conditions that are relevant to that scenario. In doing so, you limit the data displayed to that which is relevant to the scenario.

Defining Authorization Profiles

In SAP EM, you also define authorization profiles to allow:

- Information to be displayed for querying or evaluating event handler data
- Event handler to be created and changed in SAP EM

An authorization profile consists of one or more authorization profile parameter sets that the system uses to create the authorization parameters for an event handler. The authorization parameters determine how data is created, displayed, changed or evaluated.

You assign an authorization profile to an event handler type to determine which event handlers are displayed to the user and which event handlers the user may change or create. The system displays all event handlers of an event handler type to the user. These correspond to the control and information parameters of the user's authorization profile.

For example, you create an authorization profile *Vendors Europe* with a control parameter vendor with the value *Smith*. You assign the authorization profile to the event handler type *Vendors*. The vendor Smith may create, query, change or evaluate all event handler data that has event handler type *Vendor* with control parameter vendor *Smith*. Be aware that the system only checks the first forty characters of the parameter values.

Defining Filters and Assigning Filter Profiles to Users

By using filter profiles, you specify which event handler components the system displays to the user. For this purpose, you assign a filter profile to an event handler type. You can define different filter profiles for different event handler types. You can use this combination for one or more users.

You use roles to assign a user group to an existing filter profile, so that the appropriate event handler components are displayed to the user. You use the event handler type to assign the filter profile to a role.

Assigning Filter Profiles to Roles

You use roles to assign a user group to an existing filter profile, so that the appropriate event handler components are displayed to the user. You use the event handler type to assign the filter profile to a role.

Defining Event Message Senders

You define the senders who are authorized to send event messages to SAP EM.

Procedure

Assigning Users to Scenarios

1. In the mySAP SCM - Implementation Guide, choose *Event Management* → *Solutions and Scenarios* → *Assign Users to Scenarios*.
2. Select a user name.
3. Assign the user to one of the scenarios predefined by SAP or to one of your own scenarios.

   You assign a user to all available scenarios, either by entering an asterisk (*) or by **not** entering any value.

Defining Authorization Profiles

1. In the SAP SCM IMG, choose *Event Management* → *Authorizations and Filters* → *Define Authorization Profiles*.
2. Define an authorization profile parameter set with the corresponding control or info parameters. Only that data belonging to the parameters specified in this IMG activity is displayed to users when they create, change, query or evaluate event handler data.

   

   You define the control and info parameters under *Define Control and Info Parameters*.
3. Define an authorization profile and assign one or more authorization profile parameter sets.
4. Specify an authorization group number for each authorization profile parameter set.

   When checking the authorization, the system checks whether a user is authorized for all parameters of an authorization group. If an event handler belongs to several authorization groups, the user only needs authorization for one of the groups to create or change event handlers, or to have the system display them.
5. Assign the authorization profile to an event handler type.
6. Under *Role Maintenance*, assign the authorization profile to a role.

For more information about users and roles, see help.sap.com → *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *English* → *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *Users and Roles (BC-SEC-USR)*.

Defining Filters Profiles and Assigning Filter Profiles to Users

1. In the SAP SCM IMG, to:
2. Define filter profiles, choose *Event Management* → *Authorizations and Filters* → *Define Filter Profiles.*
3. Assign filter profiles to users, choose *Event Management* → *Authorizations and Filters* → *Assign Filter Profiles to Users*.
4. Select the user name.
5. Create a new entry for the corresponding event handler type and the corresponding filter profile.

   The filter profile determines the filtering of data about event handlers belonging to the selected event handler type, which the system displays.

Assigning Filter Profiles to Roles

1. In the SAP SCM IMG, choose *Event Management* → *Authorizations and Filters* → *Assign Filter Profiles to Roles*.

2. In the dialog box, specify a user role for the work area.
3. If required, to enable selection according to event handler type or filter profile, choose *Further Selection Conditions* and *Add*.
4. If required, add entry lines, change the order of the entry lines, or reset the previous entries by making a new selection.
5. Create a new entry for the corresponding event handler type and filter profile.

   The filter profile filters the data that the system displays to event handlers of the selected type.

   

   Before you can assign filter profiles to roles, you have to define them in the SAP SCM IMG. See the preceding procedure *Defining Filter Profiles and Assigning Filter Profiles to Users*.

Defining Event Message Senders

1. In the SAP SCM IMG, choose *Event Management* → *Authorizations and Filters* → *Define Event Message Senders*.
2. Define the senders who are authorized to send event messages to SAP EM.

   

   This table is not user-dependent.
3. Specify the sender code set and the sender code ID (for example, US for user as the code set, and TEST_SMITH as the code ID):

Sender Transaction	Code Set	Code ID
/SAPTRX/MI02	US	<User Name>
/SAPTRX/MI01	US	<User Name>
Web Interface	WCL	<User Name>
External Entry (for example, BAPI, IDoc)	Any	Any

4. The system checks the authorization to send an event message in the following sequence:
   a. It checks in the table whether a sender is authorized to send an event message to SAP EM.
   b. If it finds an appropriate entry, it forwards the event message to SAP EM and assigns it to the corresponding event handler.
   c. If it does not find an appropriate entry, it continues to check the authorization for the user who is logged on.
   d. It checks if the authorization to send an event message to SAP EM has been set up in the user master belonging to the user who is currently logged on.
   e. If the authorization check is successful, it forwards the event message to SAP EM and assigns it to the corresponding event handler.
   f. If the authorization check is not successful, it sends the event message and an appropriate error message back to the sender.

   For more information on creating and maintaining authorizations, see help.sap.com → *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *English* → *SAP*

Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → Users and Roles (BC-SEC-USR).

We recommend using one of the following methods to define authorized event message senders. In this IMG activity, define all users who are authorized to send an event message:

- But do not assign them an authorization to send event messages in the user master.
- With the exception of those whom you have already authorized in the user master.

This option is useful if you only want to authorize certain users to manually (online) create event messages (using transaction codes /SAPTRX/MI01 and /SAPTRX/MI02 or the Web interface), and you also want to restrict external senders who are simultaneously using automatic background programs to report events.

The table for setting up authorizations is user-dependent.

Maintaining Authorizations for SAP Forecasting and Replenishment

Procedure

Defining Maintainable Attributes

1. In this IMG activity of Forecasting and Replenishment (SAP F&R), you define maintainable fields.
2. In the IMG, choose *mySAP SCM – Implementation Guide → Forecasting and Replenishment → Master Data → Define Maintainable Attributes*.
3. **Activities**
4. Define maintenance control in SAP F&R. You can define whether fields can be changed:
   - Using interfaces only
   - From dialog boxes only
   - From processes only
   - From dialogs and processes
5. Regardless of what you select, fields can be created using interfaces. If fields are defined as being maintainable in F&R dialog boxes, they can be entered in the relevant F&R mass maintenance.
6.

Assigning Planning Responsibilities

1. In the Implementation Guide, for SCM, choose *Forecasting and Replenishment → Master Data → Assign Planning Responsibilities*.

2. To assign a replenishment planner for F&R as a purchasing planner, maintain each application for which each planner is responsible, using the following activities:
    a. 1. Choose *New Entries*.
    b. 2. Enter an identifier and description for each planner.
    c. 3. Select each area for which you want the planner to have privileges.
    d. 4. Choose *Save*.
    e.
    f.

Converting External RP Planner to Forecasting and Replenishment RP Planner

In the IMG, choose *mySAP SCM - Forecasting and Replenishment → Master Data → Convert External RP Planner to Forecasting and Replenishment RP Planner*.

Conversion between the external RP planner and the F&R RP planner is carried out automatically in the F&R inbound process, provided that the conversion specified in Customizing definitions on the client level (see F&R master data IMG activity), and the planner conversion flag is set.

Carry out the following actions:

Define the conversion of the external RP planner to the F&R RP Planner.

Assign Replenishment Planner to Products

On the SAP Easy Access screen, choose *Forecasting & Replenishment → Master Data → Product → Maintain Location Products (or: transaction /FRE/MASS_MATLOC).*

Exception Subscription

On the SAP Easy Access screen, choose *Forecasting & Replenishment → Replenishment Workbench* (transaction /FRE/RWB). Choose *Exception Subscription* and select items of unselected Business Areas. Choose *Move Left* and *Continue*.

The subscription can be done directly within the workbench by choosing *Exception Subscription*.

Authorization Concept for Replenishment Workbench for Stores (RWBS)

Authorizations for the Replenishment Workbench for Stores (RWBS) are controlled by a two-level approach:

- ABAP authorization objects and roles
- Control access lists

Creating Back-End Authorizations for Replenishment Workbench for Stores (RWBS)

To use the SAP Forecasting & Replenishment (F&R) Store User Interface (SUI), you need a user in your SAP SCM F&R system with an authorization role containing only the following authorizations (do not use any other authorizations):

- S_RFC: Authorization Check for RFC Access
- C_LIME_SI: LIME Stock Item

- C_LIME_LOC: LIME location

For information about role maintenance and the SAP Profile Generator, see the SAP Help Portal at help.sap.com → *Documentation → SAP NetWeaver → SAP NetWeaver 2004s → SAP Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → Users and Roles (BC-SEC-USR) → SAP Authorization Concept → Organizing Authorization Administration → Organization if You Are using the Profile Generator → Role Maintenance*.

Responsibility Management – Access Control Lists

The assignment of the business-related authorizations for the Replenishment Workbench for Stores (RWBS) is done by access control lists in the application. This allows decentral authorization management attendant to the business concept of RWBS.

For detailed information about the authorization concept of the Replenishment Workbench for Stores (RWBS), see the *SAP Forecasting & Replenishment- Configuration Guide at Settings for the Replenishment Workbench for Stores (RWBS) → Responsibility Management*.

Further Authorizations

For more information about this topic, see the underlying *SAP SCM Component Security Guide → Authorizations*.

1.

Maintaining Authorizations for SAP Inventory Collaboration Hub

Procedure

Specifying the Person (Planner) Responsible

1. In the SAP SCM Implementation Guide (IMG), choose *Inventory Collaboration Hub → Specify Person Responsible (Planner).*
2. To assign planning privileges to planners, maintain each application for which each planner is responsible as follows:
    a. Choose *New Entries*.
    b. Enter an identifier and description for each planner.
    c. Select each area for which you want the planner to have privileges.
3. Save your entries.

Setting User Parameters

1. In the SAP SCM IMG, choose *Inventory Collaboration Hub → Integration of SAP SCM and SAP R/3 → Basic Settings for Data Transfer → Set User Parameters*.
2. You can make user-specific entries for the following parameters:
   - Logging (configure application log on a user-specific basis)
   - Debugging (activate/deactivate debugging on a user-specific basis)
   - Recording (control event recording, that is, the publication of planning results)
3. Enter the user name as specified in the user master.
4. Use the field and input help to make the relevant settings for this user.
5. Save your entries.

Roles and Authorizations for SAP liveCache

Definition

You can use the following roles for the system administration of SAP liveCache. For more information about the authorization roles for SAP liveCache, see SAP note 452745.

For information about the authorization concept of SAP liveCache, see the SAP Help Portal: help.sap.com → *Documentation → SAP NetWeaver → SAP NetWeaver 2004s → English → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Databases → MaxDB → Installation → Installation Manual*.

Role SAP_BC_LVC_USER

Technical name: SAP_BC_LVC_USER

Tasks

This role should be given to users who are to monitor the liveCache, but who are not to change the behavior and configuration of it.

Users of this role are **not** authorized to:

- Integrate liveCaches into the system
- Start, stop, or initialize liveCaches
- Change the configuration of the liveCache

Role SAP_BC_LVC_OPERATOR

Technical name: SAP_BC_LVC_OPERATOR

Tasks

This role should be given to users who are to monitor the liveCache and carry out routine administration tasks to ensure the availability of the liveCache.

The role allows users to do the following:

- Monitor runtime behavior and critical situations
- Start and stop liveCaches

Users with this role are **not** authorized to:

- Integrate liveCaches into the system
- Initialize liveCaches
- Change the configuration of the liveCache

Role SAP_BC_LVC_ADMINISTRATOR

Technical name: SAP_BC_LVC_ADMINISTRATOR

Tasks

The role should be given to users who monitor, administer, and configure the liveCache.

The role allows users to do the following:

- Monitor the runtime behavior and critical situations
- Start and stop liveCaches
- Integrate new liveCaches
- Change integration data
- Make parameter and configuration changes
-
- Users of this role are NOT authorized to initialize liveCaches.

Role SAP_BC_LVC_SUPERUSER

Technical name: SAP_BC_LVC_SUPERUSER

Tasks

This role should be given to users who monitor, administer, configure and initialize the liveCache.

The role allows users to:

- Monitor runtime behavior and critical situations

- Start and stop liveCaches
- Initialize liveCaches
- Integrate new liveCaches
- Change integration data
- Make parameter and configuration changes

Maintaining Authorizations for Integration with SAP Components

Procedure

Maintaining Authorizations for SAP APO – SAP R/3 Integration

Using Standard Roles for SAP APO – SAP R/3 Integration

For the integration of SAP APO and SAP R/3 / SAP DIMP, use the following authorization roles for the RFC destination users, which are provided with SAP Note 727839:

- SAP_SCM_INTEGRATION_SCM.SAP

  Authorization role for the SAP SCM - SAP R/3 / SAP DIMP integration for background users in the SAP SCM System.

- SAP_SCM_INTEGRATION_R3.SAP

  Authorization role for the SAP SCM - SAP R/3 integration for background users in the SAP R/3 System.

- SAP_SCM_INTEGRATION_DIMP.SAP

  Authorization role for the SAP SCM - SAP DIMP integration for background users in the SAP DIMP System.

  

  For more information about the authorization roles for SAP APO – SAP R/3 integration, see SAP Note 727839.

Maintaining Authorizations for Available to Promise (ATP)

Regarding the integration of SAP APO and SAP R/3, available to promise (ATP) plays a special role: The ATP check needs a RFC connection with a dialog user to perform the check. As a dialog user within RFC connections is a safety flaw, it is necessary to keep this flaw as small as possible by performing the following steps.

1. Create a separate trusted system RFC connection for the ATP check.

   

   For more information about trusted system RFC connections see the SAP NetWeaver Security Guide at: help.sap.com → *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *English* → *SAP Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security* → *Security Guides for Connectivity and Interoperability Technologies* → *RFC/ICF Security Guide* → *RFC Scenarios* → *RFC*

Communication Between SAP Systems → Network Security and Communication → Using RFC Trusted System Networks.

2. To assign the RFC connection to the ATP application, in the SAP SCM IMG, choose *Integration with SAP Components → Integration via APO Core Interface (CIF) → Basic Settings for Creating the System Landscape → Assign RFC Destinations to Various Application Cases*.
3. For each SAP ERP user, create a corresponding ATP user in the SAP SCM system.
4. Assign one or more of the following authorization roles to the user(s) in the SAP SCM system:
   - SAP_APO_ATP_CO (APO: ATP Controller)
   - SAP_APO_ATP_CU(APO: ATP Customizing User)
   - SAP_APO_ATP_EU (APO: ATP Expert User)
   - SAP_APO_ATP_SU (APO: ATP Standard User)
   - SAP_APO_ATP_RSP_ALL (APO: ALL ATP Authorizations)
5. Assign the authorization S_RFCACL_ALL to the users in the SAP SCM system. This is necessary to perform RFC calls.

   For more information about the role maintenance and the SAP Profile Generator, see the *SAP NetWeaver 2004s → English → SAP NetWeaver by Key Capability → Security → Identity Management → Users and Roles (BC-SEC-USR) → SAP Authorization Concept → Organizing Authorization Administration → Organization if You Are Using the Profile Generator → Role Maintenance*.

Setting User Parameters for SAP ICH – SAP R/3 Integration

1. In the SAP SCM IMG, choose *Inventory Collaboration Hub → Integration of SAP SCM and SAP R/3 → Basic Settings for Data Transfer → Set User Parameters*.
2. You can make user-specific entries for the following parameters:
   - Logging (configure application log on a user-specific basis)
   - Debugging (activate/deactivate debugging on a user-specific basis)
   - Recording (control event recording, that is, the publication of planning results)
3. Enter the user name as specified in the user master.
4. Use the field and input help to make the relevant settings for this user.

Maintaining Authorizations for Data Transfer to the SAP Business Information Warehouse

Limiting Authorizations for Extraction

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

1. In the SAP SCM IMG, choose *Integration with SAP Components → Data Transfer to the SAP Business Information Warehouse → General Settings → Limit Authorizations for Extraction*.
2. Choose *New Entries*.

3. Choose a DataSource that you want to exclude from the extraction.
4. Choose the BW system for which you want no more data for this DataSource to be extracted.
5. In the field *Excl. Extr.*, enter whether or not you want to exclude the DataSource from the extraction.
6. Save your entries.
7. Specify a transport request.

Maintaining Authorizations for Enterprise Services

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.

The enterprise services add-on SAP SCM ES uses the standard authorization objects that are available for SAP SCM, 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 documentation at **`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *SAP NetWeaver Developer's Guide* → *Fundamentals* → *Using JavaCore Development Tasks* → *Providing and Consuming Web Services* → *Web Service Toolset* → *Web Services Security* → *Authorization*.

Network and Communication Security

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 SCM 5.0 to achieve a secure system landscape. See: **`service.sap.com/security`** → *SAP NetWeaver* → *SAP NetWeaver in Detail* → *Security* → *Security in Detail* → *SAP Security Guides* → *SAP NetWeaver 2004s Security Guides (Complete)* → *SAP NetWeaver 2004s Security Guide* → *Network and Communication Security* → *Transport Layer Security* → *Secure Network Communications.*

You will find a detailed description of all communication channels within the component SAP SCM 5.0 on SAP Service Marketplace at **`service.sap.com/scm`** → *mySAP SCM Technology* → *Architecture Overview.*

For more information about the communication security of SAP NetWeaver, see the *SAP NetWeaver 2004s Security Guide → Network and Communication Security.*

For more information about security aspects for connectivity and interoperability of SAP NetWeaver 2004s, see the *SAP Security Guides → SAP NetWeaver 2004s Connectivity Security Guides.*

SAP APO – SAP R/3

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

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

For more information about the integration of SAP APO and mySAP ERP, see the SAP SCM Documentation at help.sap.com → *Documentation → mySAP Business Suite → SAP Supply Chain Management → SAP SCM 5.0 → SAP Advanced Planning and Optimization (SAP APO) → Integration via APO Core Interface (CIF) → Technical Integration.*

SAP Event Management (SAP EM)

Since SAP Event Management (EM) comes with interfaces for connecting application systems, internal and external systems and devices, and a data warehouse system, a special focus on the communication channel security is necessary. SAP recommends activating a secure communication protocol for all communication channels used (for example, SNC). This is **strongly** recommended if you use mobile devices for connecting to SAP EM.

For more information about the infrastructure of SAP Event Management, see the SAP SCM Documentation at help.sap.com → *Documentation → mySAP Business Suite → SAP Supply Chain Management → SAP SCM 5.0 → English → SAP Event Management (SAP EM) → SAP Event Management Infrastructure → Application Integration.*

Since several interfaces of SAP EM are available for connecting to SAP Exchange Infrastructure (SAP XI), we strongly recommend that you consult the SAP Exchange Infrastructure SAP XI Security Guide.

For more information about the infrastructure of SAP EM, see *SAP SCM Documentation → SAP Event Management (SAP EM) → System Installation and Integration → SAP Exchange Infrastructure Integration.*

You can find the SAP XI security guide on the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver → SAP NetWeaver in Detail → Security → Security in Detail → SAP Security Guides → SAP Process Integration (PI) Security Guides → SAP Exchange Infrastructure (XI) Security Guide.*

SAP SCM - Web Communication Layer (SAP SCM - WCL)

SAP strongly recommends that you use Secure Socket Layer (SSL), since the ERP user and its password are used to log onto SAP SCM - WCL.

For more information about security recommendations in SAP SCM - WCL, see the SAP J2EE Engine documentation installation guide, at: *service.sap.com/instguidesnw2004s → Installation → Installation – Standalone Engines & Clients → Installation Guide – J2EE Adapter Engine for NW2004s.*

SAP Inventory Collaboration Hub (ICH)

As SAP Exchange Infrastructure (SAP XI) is a prerequisite for message-based transactions within SAP ICH, we strongly recommend that you consult the SAP XI security guide.

You can find the SAP Exchange Infrastructure Security Guide at the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver → SAP NetWeaver in Detail → Security → Security in Detail → SAP Security Guides → SAP Process Integration (PI) Security Guides → SAP Exchange Infrastructure (XI) Security Guide.*

Using customer-specific X.509 Client Certificates for SSL in SAP ICH

In order to use customer-specific X.509 client certificates for SSL, please see SAP Note 510007. The SSL key pair is stored in directory $(DIR_INSTANCE)/sec/SAPSSLS.pse, of your Web Application Server, or can be imported from the PKCS#12 certificate, using program "sapgenpse", which comes with SAPCryptolib. Enter <sapgenpse import_p12 –h> for the help. The PSE file that is created can be imported to transaction STRUST as a file and saved as: "SSL Server" PSE.

For detailed information on customer-specific X.509 client certificates for SSL, see the SAP NetWeaver Security Guide, on the SAP Service Marketplace at **`service.sap.com/security`** → *SAP NetWeaver → SAP NetWeaver in Detail → Security → Security in Detail → SAP Security Guides → SAP NetWeaver 2004s Security Guides (Complete) → SAP NetWeaver Security Guide→ User Administration and Authentication → User Authentication and Single Sign-On → Using External Authentication Mechanisms → Pluggable Authentication Services (PAS) → Pluggable Authentication Services for External Authentication → Prerequisites for Using PAS → Prerequisites for Using X.509 Client Certificates.*

Network Security

Your network infrastructure is extremely 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.

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

For information about network security for SAP NetWeaver 2004s, see the *SAP NetWeaver 2004s Security Guide → 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. (Note: external security attacks can also come from "inside", if the intruder has already taken over control of one of your systems.)

For information about the technical components of your SAP SCM 5.0 component, see the SAP Service Marketplace at **`service.sap.com/scm`** → *mySAP SCM Technology.*

For information about access control using firewalls, see the *SAP NetWeaver 2004s Security Guide → Network and Communication Security → Using Firewall Systems for Access Control.*

Network Security for Enterprise Services Add-On SAP SCM ES

For more information about network security for Web services, see the SAP NetWeaver documentation at **`help.sap.com`** → *SAP NetWeaverSAP NetWeaver 2004s → SAP NetWeaver Developer's Guide → Fundamentals → Using JavaCore Development Tasks → Providing and Consuming Web Services → Web Service Toolset → Web Services Security*.

Communication Destinations

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

Follow the "Golden Rules" for connection users and authorizations:

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

Connection Destinations

Destinations	Delivered?	Type	User, Authorizations	Description
SAPOSCOL_<DB_hostname>	Yes	RFC -	-	*SAP SCM*

(SAP SCM central instance - DB instance)		TCP/IP		*Installation Guide → SCM Installation Guide – SCM Server 5.0<Operating System/DB>→ Post-Installation Activities → Checking the RFC Destination.*
SAP APO Supply Chain Cockpit (SCC) → SAP Business Warehouse (BW)	No	RFC - ERP		SAP SCM Implementation Guide (IMG): *Advanced Planning and Optimization → Supply Chain Cockpit (SCC) → Define Default BW Destination (RFC).*
<SAP SCM name>CLNT<client> SAP APO → mySAP ERP	No	RFC - ERP	Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 **and** 727839.	SAP SCM IMG: *Integration with SAP Components → Integration via APO Core Interface (CIF) → Basic Settings for Creating the System Landscape →Assign RFC Destinations to Various Application Cases..*
mySAP ERP → SAP APO (ATP)	No	RFC - ERP (trusted system connection)	Use the Profile Generator (transaction code PFCG) and assign one or more of the following roles: SAP_APO_ATP_CO SAP_APO_ATP_CU SAP_APO_ATP_EU SAP_APO_ATP_SU SAP_APO_ATP_RSP_ALL	Maintaining Authorizations for Integration with SAP Components [External] → Maintaining Authorizations for Available-to-Promise (ATP).
<System-ID>CLNT<Client number> (SAP liveCache)	No	RFC - R/3	<liveCache User ID>; <liveCache Authorization> (see SAP Note 305634)	SAP Note: 305634.
OPTSERVER_<Optimizer>01	No	RFC -	-	*SAP SCM*

		TCP/IP		*Installation Guide → Installation Guide - SAP APO Optimizer for SAP SCM Server 5.0 → SAP APO Optimizer Installation - How To → Post-Installation Activities on the SAP Web AS Host(s) → Performing a Setup Check of RFC Gateway.*
SAP EM → Application Systems	No	RFC	Use the Profile Generator (transaction code PFCG) to define an appropriate profile.	SAP SCM IMG: *Event Management → General Settings in SAP Event Management → Define RFC Connection to Application System* **and** *SAP SCM Documentation 5.0 → SAP Event Management (SAP EM) → System Installation and Integration.*
SAP Application system → SAP EM	No	RFC	Use the Profile Generator (transaction PFCG) to define an appropriate profile.	SAP SCM IMG: *Integration with SAP Components → Event Management Interface → Define System Configuration → Define RFC Connection to SAP EM* **and** *SAP SCM 5.0 Documentation → SAP Event Management*

				(SAP EM) → System Installation and Integration.
<Logical target system> SAP ICH - mySAP ERP	No	RFC-ERP	Use the Profile Generator (transaction PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.	SAP SCM IMG: *Inventory Collaboration Hub → Integration of SAP SCM and SAP R/3 → Basic Settings for Creating the System Landscape → Set Up RFC Destination, (and) → Assign RFC Destinations to Various Application Cases* **and** *Inventory Collaboration Hub → Integration of SAP SCM and SAP R/3 → Basic Settings for Creating the System Landscape → Settings for qRFC Communication → Configure QRFC Communication.*
SAP EWM → SAP R/3 or mySAP ERP	No	RFC – ERP (qRFC)	Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.	In the SAP EWM IMG: *Extended Warehouse Management → Interfaces → ERP Integration → General Settings → Control for RFC Queue* and *SAP SCM – IMG: Integration with SAP*

				Components → Integration via APO Core Interface (CIF) → Basic Settings for Creating the System Landscape → Set Up RFC Destination.
SAP EWM → SAP APO (APO instance)	No	RFC – ERP	Use the Profile Generator (transaction PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.	In the *SAP SCM* – Implementation Guide, choose *→ Extended Warehouse Management → Goods Receipt Process → Slotting → General Settings → Change Information for APO Instances*
SAP EWM → Non-SAP Systems	No	RFC – ERP	-	In the SAP EWM IMG, choose *mySAP SCM – Implementation Guide → Extended Warehouse Management → Interfaces → Non-SAP Systems → Connect Subsystem*
SAP EWM → SAP Business Warehouse (BW)	No	RFC – ERP	-	In the SAP EWM IMG, choose *mySAP SCM – Implementation Guide → Integration with SAP Components → Data Transfer to the SAP Business Information Warehouse* AND *mySAP SCM – Implementation*

				Guide → Extended Warehouse Management → Interfaces → SAP Business Information Warehouse

For more information about communication destinations of SAP NetWeaver, see the *SAP NetWeaver Security Guide → Security Guides for Connectivity and Interoperability Technologies.*

Data Storage Security

The data storage security of SAP NetWeaver and components installed on that base is described in detail in the SAP NetWeaver 2004s Security Guide.

For information about the data storage security of SAP NetWeaver, see *SAP NetWeaver 2004s Security Guide → Security Guides for Operating System and Database Platforms.*

In general, all business data of the component SAP SCM 5.0 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 SCM 5.0.

In some special cases, business-relevant data is stored elsewhere (for example, in a file system). All those special cases are listed below:

SAP APO Optimizer

The SAP APO Optimizer writes log files to the gateway file system. The log files are located in the following directory:

<Drive:>\usr\sap\<SID>\<Gxx>\log

<SID> = Gateway-ID on the SAP APO Optimizer server

<Gxx> = Gateway number

You must protect this folder on your server against unauthorized access by a third party.

SAP SCM - WCL

Logging Manager Parameters

The Logging Manager parameters configure the SAP Logging API. The logging file and pattern is set with the following parameters:

Log File ID

Log File Pattern

You must protect the folder in which the log file is located on your server against unauthorized access by a third party.

For more information about the SAP SCM - WCL Logging Manager parameters, see the *SAP SCM 5.0 Installation Guide → Standard Installation → Additional*

Information → Configuration Parameters for SCM Web Communication Layer (WCL) → Logging Manager Parameters.

SAP Forecasting and Replenishment

SAP Forecasting and Replenishment works with the third party software Forecasting and Replenishment Processor (FRP). The data exchange between SAP F&R and the FRP is carried out using file download and upload. The directory for the file download and upload can be customized by the customer. Protect the folder in which exchange data file is located on your server against unauthorized access by a third party.

For more information about the SAP Forecasting and Replenishment data exchange using file download and upload, see the *Configuration Guide: SAP Forecasting and Replenishment.*

 Security for Additional Applications

SAP Forecasting and Replenishment

SAP Forecasting and Replenishment includes the third party software Forecasting and Replenishment Processor (FRP). To learn more about the security of this product, see the third party FRP documentation.

PTV eServer

SAP SCM 5.0 comes with the optional third party software PTV eServer. This software requires a RFC destination on the SAP SCM 5.0 side. This RFC is described in the chapter ‘Communication Destinations’. For any security issues regarding the PTV eServer software, see the third party PTV eServer documentation.

SAP DB

SAP SCM 5.0 can be used with SAP LiveCache. As LiveCache is a part of SAP DB, the SAP DB Security Guide is also relevant for SAP SCM 5.0 using SAP liveCache. To learn more about the security of SAP DB, see the SAP DB Security Guide, on the SAP Service Marketplace at:

service.sap.com*/securityguide → SAP NetWeaver 2004s → SAP NetWeaver Security Guide → Security Guides for the Operating System and Database Platforms → Database Access Protection → Max DB Security Guide.*

Or, SAP Help Portal at: Documentation → SAP NetWeaver →SAP NetWeaver 2004s → English → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Application Platform by Key Capability → Database Support → MaxDB.

 Minimal Installation

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

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

SAP APO Add-Ons

SAP APO add-ons include some Active-X-Controls. You might experience some functional restrictions in the event of a strict security policy regarding Active-X-Controls.

SAP SCM – Web Communication Layer (SAP WCL)/SAP Event Management (SAP EM)

Since the SAP SCM - WCL interface is Java-based, you might have some functional restrictions in the event of a strict security policy regarding Web services.

For information about the SAP EM web interface, see SAP SCM Documentation at help.sap.com → *Documentation* → *mySAP Business Suite* → *SAP Supply Chain Management* → *SAP SCM 5.0 (English)* → *SAP Event Management (SAP EM)* → *SAP Event Management Infrastructure* → *User Interfaces*.

Other Security-Relevant Information

User Front End

Web Browser as a User Front End

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.

RF Device as a User Front End

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

For more information about SAP Front End, see the SAP Service Marketplace at **`http://service.sap.com/instguides`** → *Installation & Upgrade Guides* → *SAP NetWeaver* → *Release 2004s* → *Installation* → *Installation* → *Standalone Engines and Clients* → *SAP Frontend 6.40 Installation Guide*.

Enterprise Services

Enterprise services for mySAP SCM are available as of SAP SCM ES 5.0. As SAP SCM ES is provided as an add-on to SAP SCM, the security guidelines applicable to SAP SCM also apply to SAP SCM ES.

For more information about special security requirements for Web services, see the SAP NetWeaver documentation at **`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *SAP NetWeaver Developer's Guide* → *Fundamentals* → *Using Java* → *Core Development Tasks* → *Providing and Consuming Web Services* → *Web Service Toolset* → *Web Services Security*.

For more information about enterprise services and security, see the *mySAP Business Suite: Service Provisioning* documentation at **`service.sap.com/swdc`** → *Download* → *Installations and Upgrades* → *Entry by Application Group* → *SAP Application Components* → *SAP SCM ES* → *SAP SCM ES 5.0* → *Installation* → *ESA SCM-SE 5.0 Add-on Documentation* → *00_mySAPServiceProvisioning.pdf* → *2.6 Security*.

For more information about the security of the exchange infrastructure, see the SAP NetWeaver security guide at **`service.sap.com/securityguide`** → *SAP Process Integration Security Guides* → *SAP NetWeaver Process Integration Security Guide*.

Auditing and Logging

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

Auditing and logging for the SCM 5.0 Component is described in detail in the SAP NetWeaver 2004s Security Guide, which you can find at: **help.sap.com** → *Documentation* → *NetWeaver 2004s* → *SAP Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide* → *Security Aspects for System 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 timestamp

The messages logged are located in the message class *VSCAN*, using the system log messages BU8 and BU9 (created in SE92). The severities are set to *High* and *Medium,* respectively. The severity of the audit class is set to *Miscellaneous*.

Audit Information System (AIS)

Information on auditing and logging for the Audit Information System (AIS) is described in detail in the *SAP NetWeaver 2004s Security Guide* → *Security Aspects for System Administration* → *Auditing and Logging* → *The Audit Information System (AIS).*

Inventory Collaboration Hub (ICH)

The information on auditing and logging for the Inventory Collaboration Hub (ICH) is described in detail at: **help.sap.com** → *Documentation* → *mySAP Business Suite* → *Supply Chain Management* → *SCM 5.0* → *SAP Inventory Collaboration Hub (ICH)* → *Cross-Application Functions* → *Audit Trail.*

Extended Warehouse Management (EWM)

Extended Warehouse Management (EWM) auditing and logging is governed by the following transactions and customizing activities (detailed below).

Auditing and logging in EWM is governed by **change documents**. Change documents have to first be activated in customizing, before they can be used.

When change documents are activated and used in the system, each field in SCM delivery documents is linked to change documents. The change documents provide information on which fields were changed, and the old and new values. When change documents are used,

the SCM system can be set to create a **log**, showing which user changed data in a delivery document, and the specific time that the change was made.

You can also run reports that retrieve archived documents. The reports are not separate transactions, 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 EWM auditing and logging (in SCM Customizing, you can set – per document type of delivery – whether a change document will be written or not for each delivery document. It can be set for all document categories in EWM, in other words, for all delivery documents in EWM, including posting changes, and internal moves).

Customizing activity:	**Customizing path (in the SAP SCM IMG):**
Activation of change documents for inbound delivery	IMG: *Extended Warehouse Management → Goods receipt process → Inbound delivery → Manual settings → Define document types for inbound delivery proces; or: Define document types for inbound delivery process using Wizard* (then set the *Change documents* indicator).
Activation of change documents for outbound delivery	*Extended Warehouse Management → Goods issue process → outbound delivery → Manual settings → Define document types for outbound delivery process (or:Define document types for outbound delivery process using Wizard),* then set the *Change documents* indicator.
Activation of change documents for posting changes	*Extended Warehouse Management → Internal warehouse processes → Delivery processing → Posting changes → Manual settings → Define document types for posting change process (or: Define document types for posting change process using Wizard).* Then set the *Change documents* indicator.
Activation of change documents for stock transfers	*Extended Warehouse Management → Internal warehouse processes → Delivery processing → stock transfers → Manual settings → Define document types for the stock transfer process (or: define document types for the stock transfer process using Wizard).* Then set the *Change documents* indicator.

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

Transaction description	**Menu path in the SCM system**
Maintain inbound delivery	*SAP Easy Access menu → Extended Warehouse Management → Delivery Processing → Inbound Delivery → Maintain Inbound Delivery.*
Maintain outbound delivery order	*SAP Easy Access menu → Extended Warehouse Management → Outbound*

	Delivery → Maintain Outbound Delivery Order.
Maintain posting change	*Extended Warehouse Management → Delivery Processing → Posting Change → Maintain Posting Change.*
Maintain internal stock transfer	*Extended Warehouse Management → Delivery Processing → Posting Change → Maintain Internal Stock Transfer.*

Forecasting and Replenishment

All changes related to order proposals are logged in the respective history tables of ODM (xxx stands for the client number):

- /1OT/FDA11HDRxxx
- /1OT/FDA12IT2xxx
- /1OT/FDA17MP2xxx
- /1OT/FDA1HREFxxx
- /1OT/FDA1IREFxxx
- /1OT/FDA1OPH1xxx
- /1OT/FDA1OPI1xxx

These data can e.g. be transferred to BW. Here, the automation of the process in terms of percentage of manually changed order proposals can be tracked in the respective reports. This logging is set to *ON* by default in the respective delivered BC sets. To check the settings for logging, use the following path in the IMG: SAP SCM – Implementation Guide → *Order Document Management → Configure Order Document Management*. In the list of the view *ODM: Order Component - Maintenance View*, choose FROP and then folder *ODM: Order Data Area, Assignment – Maintenance View*.

For the communication with the FRP modules, it is important that the data environments on the file system level are properly secured. This means that only very restricted access to this file system should be granted. See also chapter *Maintain F&R Processor Administration Settings* in the configuration guide.

Virus Check of Document Attachments

Use

SAP SCM 5.0 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 corrrectly.

For more information, see the *SAP SCM Implementation Guide (IMG) → SAP Web Application Server → System Administration → Virus Scan Interface.*

Appendix

Related Security Guides

You can find more information about the security of SAP applications on the SAP Service Marketplace, Quick Link **security**. Security guides are available using the Quick Link **securityguide.**

Related Information

For more information about topics related to security, see the links shown in the table below.

Quick Links to Related Information

Content	Quick Link on the SAP Service Marketplace (service.sap.com)
Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides	**instguides** **ibc**
Related SAP Notes	**notes**
Released platforms	**platforms**
Network security	**network** **securityguide**
Technical infrastructure	**ti**
SAP Solution Manager	**solutionmanager**
SAP Supply Chain Management	**scm**