SAP SCM 4.1 Component Security Guide

ADDON.NDSCM_SECGUIDE

Release 410

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 4.1 Component Security Guide

Introduction

This guide does not replace the daily operations handbook, which we recommend 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 4.1 (SAP SCM 4.1). It covers the following parts of the component:

- SAP SCM 4.1 Server
  - SAP Advanced Planning and Optimization (SAP APO)
    - SAP liveCache
    - SAP APO Optimizer (optional SAP APO component)
  - SAP Event Manager (SAP EM)
  - SAP Inventory Collaboration Hub (SAP ICH)
  - Embedded SAP BW 3.5 (only used and required for the SAP APO 4.1 component within SAP SCM 4.1)
- SAP SCM - Web Communication Layer 4.1 (SAP SCM - WCL)
- SAP Forecasting and Replenishment 4.1 (F&R)
- (Third party software: map&guide mapserver for SAP SCM 4.1)

In many cases, the required information has already been provided in other security guides and in configuration and installation guides. In those 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. You can find the security guides mentioned below in the SAP Help Portal at **`help.sap.com`** → *Documentation* → *SAP NetWeaver* → *Release '04* → *English* or *German* → *SAP Library* → *SAP NetWeaver* → *Security* → *SAP NetWeaver Security Guide.* All 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	Operating System and Database 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* → *Release '04* → *English* or *German* → *SAP Library* → *SAP NetWeaver* → *Security* → *SAP NetWeaver Security Guide*
SAP NetWeaver Documentation	**help.sap.com** → *Documentation* → *SAP NetWeaver* → *Release '04* → *English* or *German* → *SAP Library* → *SAP NetWeaver*
SAP SCM Master Guide	**service.sap.com/instguides** →*mySCM* → *Using SAP SCM <your version>* → *Master Guide SCM 4.1*
SAP SCM Documentation	**help.sap.com** → *Documentation* → *mySAP Business Suite* → *SAP Supply Chain Management* → *SAP SCM 4.1* → *English* or *German* → *SAP Library* → *SAP Supply Chain Management (SAP SCM)*
SAP SCM Installation Guide	**service.sap.com/instguides** → *mySCM* → *Using SAP SCM <your version>*

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 processing time. These demands on security apply likewise to the SAP SCM 4.1 component. To assist you in securing your SAP SCM 4.1 component, we provide this SAP SCM 4.1 Component Security Guide.

We strongly recommend consulting 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. Guides of that type are only relevant for a certain phase of the software life cycle, whereas the security guides provide information that is relevant for all time frames.

Important SAP Notes

Regularly check to see which SAP Notes are available regarding 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 on Single Sign-On solutions for SAP systems
184504	Storing user data for dbmcli version 7.2.	
447543	APO: Authorizations too comprehensive/not user-specific	
386021	The system change option is ignored	
687399	SP09: Authorization problem after you jump from Alert Monitor	
727839	Authorization role for the SAP	

	SCM - SAP R/3 integration	
637052	Missing authorization object for database views	
619086	Input help in authorization maintenance of parameters	
498627	Global ATP: No logoff of user RFC_USER from APO system	
305634	RFC destination for global working on the liveCache	
616555	liveCache >= 7.4: Password change	The passwords of the standard liveCache user and the DBM user are to be changed in the liveCache environment.
25591	Changing the SAPR3, control, and SUPERDBA USER	The SAPR3 user password should be changed.
452745	New authorization concept for transaction LC10	
683528	@stake (11/2003); Security gaps in SAP DB	This note provides information on the secure operation of SAP DB/MaxDB and liveCache. This note also deals with misgivings expressed in the messages from @stake.
30724	Data protection and security in SAP systems	
128447	Trusted/Trusting Systems	Needed for the customizing of Trusted/Trusting Systems RFC connections.
821200	DBM Server must know standard user	

For more SAP Notes on security, see the SAP Service Marketplace at **`service.sap.com/security`** → *SAP Notes on mySAP Security*.

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**
Technical System Landscape & Installation	SCM Installation Guide(s)	**instguides**
Technical configuration, High availability	Technical Infrastructure Guide	**ti**
Security		**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 → User Administration and Authentication → User Management → User Management Tools*

Users

System	User	Delivered?	Type	Default Password	Detailed Description
SAP SCM Server	<sapsid>adm	Yes	SAP System Administrator	To be entered	"SAP SCM Installation Guide" → *Installation Guide – SCM Server 4.1 <Operating System/DB>* → *Installation Proces* → *Input for the Installation*.
SAP SCM Server	SAPService <sapsid>	Yes	SAP System Service Administrator	To be entered	"SAP SCM Installation Guide" → *Installation Guide – SCM Server 4.1 <Operating System/DB>* → *Installation Proces* → *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 the SAP NetWeaver Components* → *SAP Web Application Server Security Guide* →*SAP Web AS Security Guide for ABAP Technology* → *User Authentication* →*Protection Standard Users*
SAP WebAS	SAP Standard J2EE Users (Administrator, Guest, Emergency)	Yes	See SAP NetWeaver Security Guide	See SAP NetWeaver Security Guide	"*SAP NetWeaver Security Guide"* → *Security Guides for the SAP NetWeaver Components* → *SAP Web Application Server Security Guide* → *SAP Web AS Security Guide for Java Technology* → *Users and User*

					Management → Standard Users and Groups
SAP J2EE Engine	SAPJSF	Yes	Communication user	To be entered	"SAP SCM Installation Guide": *Installation Guide – SCM Server 4.1 <Operating System/DB> → Installation Process → Input for the Installation*.
SAP SCM 4.1	RFC Communication users (you will need an RFC Communication user for each RFC destination in Communication Destinations [Page 31]).	No	Communication user	The authorizations of the user will depend on the business case. For more information, see Authorizations [Page 14] in this Security Guide.	See Communication Destinations [Page 31] and Authorizations [Page 14].
SAP SCM 4.1	Business processing users (you will need a user in each component for each employee working with the system)	No	Dialog user	To be entered	See SAP SCM 4.1 documentation and Authorizations [Page 14].
SAP liveCache	<lcid>adm	Yes	Operating system user	To be changed	Installation Guide: *SAP live Cache Server → 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	Installation Guide: SAP live Cache Server → *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	Installation Guide: *SAP live Cache Server → 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	Installation Guide: SAP live Cache Server → *Post Installation Activities → Changing Passwords of Created Users* and SAP Notes 25591 and 616555.
SAP EM 4.1	SAP Event Management Users	No	Dialog user	To be entered	"*SAP SCM Documentation" → SAP Event Management (SAP 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 4.1 → Installation Preparations → Configuring the Administration User 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 SCM – WCL Specific Information → SAP SCM – WCL Configuration Parameters*.
SAP SCM - WCL	SAP SCM - WCL user	No	Dialog user	To be entered	See Authorizations [Page 14]

For more information about user types, see the “*SAP NetWeaver Security Guide” → SAP Web Application Server Security Guide → SAP WebAS Security Guide for ABAP Technology → User Authentication → User Types.*

For information about SAP NetWeaver standard users, see “*SAP NetWeaver Security Guide” → SAP Web Application Server Security Guide → SAP WebAS Security Guide for ABAP Technology → User Authentication → Protecting Standard Users .*

For information about SAP NetWeaver password rules, see the “*SAP NetWeaver Documentation” → Security → Identity Management → Users and Roles (BC-SEC-USR) → User Maintenance → Logon and Password Security in the SAP System → Password Rules.*

User Data Synchronization

To avoid unnecessary added administration, you can use user data synchronization in your system landscape. As the component SAP SCM 4.1 is based on SAP NetWeaver, all the mechanisms for user data synchronization of SAP NetWeaver are available for SAP SCM 4.1.

For information about user data synchronization, see the *SAP NetWeaver 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 4.1is 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 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 “*SAP NetWeaver Security Guide” → SAP Web Application Server Security Guide → SAP Web AS Security Guide for ABAP Technology → User Authentication.*

SAP SCM – WCL

Since SAP SCM - WCL is based on Java technology, you need the SAP Java Crypto Toolkit if you want to configure SAP logon tickets for Single Sign-On (SSO).

For more information about downloading and installing the SAP Java Crypto Toolkit for SAP SCM - WCL, see “*SAP SCM Installation Guide” → Installation/Upgrade*

SAP SCM – SAP WCL 4.1 → Post-Installation Activities → Downloading the SAP Java Crypto Toolkit.

Authorizations

The authorization concept of the component SAP SCM 4.1 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 logging on and authenticated themselves.

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

For information about the authorization concept of SAP NetWeaver, see "SAP *NetWeaver Documentation" → 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 onto 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 more information about the role maintenance and the Profile Generator, see "*SAP NetWeaver Documentation" → 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 4.1, SAP already provides a number of 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 the input help. The use of search terms helps to restrict the selection to the required standard roles (for example, the search term *APO* lists all APO-relevant SAP standard roles). The roles short text helps you find the role covering your business needs. The role documentation provides a detailed description of the role content.

Some of the components in SAP SCM 4.1 have additional authorization methods. The relevant components and the Implementation Guide (IMG) activities are shown in the following sections.

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 strongly weaken the overall security concept in your production system.

Maintaining Authorizations for SAP APO

Procedure

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 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): Configuring Planning Books

Planning books within Supply Network Planning (SNP) can only be created or modified when the system change option for the SAP_APO component is modifiable.

In a three tier system landscape, create or modify planning books in the development system and transport this to the Quality Assurance System and after testing into the production system.

 Maintaining Authorizations for SAP Event Management (SAP EM)

Use

Use this to maintain the required authorizations for SAP Event Management.

Before carrying out the steps listed below, please see the documentation for "Roles in SAP Event Management" (see the *SAP Help Portal at help.sap.com: Documentation → SAP Business Suite → SAP SCM 4.1 → SAP Event Management (SAP EM) → SAP Event Management Infrastructure → Roles in SAP Event Management)*.

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 "*SAP NetWeaver Documentation*" → *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 the "*SAP NetWeaver Documentation" → 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 Inventory Collaboration Hub

Procedure

Specifying the Person (Planner) Responsible

1. In the SAP SCM Implementation Guide (IMG), choose *Inventory Collaboration Hub* → *Specify the Person (Planner) Responsible*.
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.

Authorizations for SAP SCM - WCL / SAP Event Management (SAP EM)

The SAP SCM Web Communication Layer (WCL) offers information access and full supply chain visibility for SAP EM on the Internet. For the SAP SCM - WCL the following authorizations have to be maintained:

- Configuring the Administration User on the SAP SCM Server

  For more information about configuring the administration user on the SAP SCM server, see the *SAP SCM Installation Guide → Installation/Upgrade Guide SAP Supply Chain Management - Web Communication Layer → Installation Preparations → Configuring the Administrator User on the SAP SCM Server*.

- Configuring the Connection User Role on the SAP SCM Server

  For more information about configuring the connection user role on the SAP SCM server, see the *SAP SCM Installation Guide → Installation/Upgrade Guide SAP Supply Chain Management - Web Communication Layer → Installation Preparations → Configuring the Connection User Role on the SAP SCM Server*.

- Customizing User Profile on SAP SCM Server

  For more information about customizing the user profile on the SAP SCM server, see the *SAP SCM Installation Guide → Installation/Upgrade Guide SAP Supply Chain Management - Web Communication Layer → Installation Preparations → Customizing User Profile on SAP SCM Server*.

Maintaining Authorizations for SAP Forecasting and Replenishment

Procedure

Defining Maintainable Attributes

In this IMG activity of Forecasting and Replenishment (SAP F&R), you define maintainable fields.

1. In the IMG, choose *mySAP SCM – Implementation Guide → Forecasting and Replenishment → Master Data → Define Maintainable Attributes*.

Activities

2. 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

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.

For information about assigning planning responsibilities, see the SAP Forecasting & Replenishment – Configuration Guide at: Preconditions in SCM for F&R → *Customizing Settings in SCM for F&R → Master Data → Define Maintainable Attributes.*

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. 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.
   d. Choose *Save*.

For more information on that, see the SAP Forecasting & Replenishment – Configuration Guide at Preconditions in SCM for F&R → *Customizing Settings in SCM for F&R → Master Data → Assign Planning Responsibilities.*

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).*

For more information, see the SAP Forecasting & Replenishment – Configuration Guide, at *Preconditions in SCM for F&R → Preconditions in SCM for F&R → Master Data → Assign Replenishment Planner to Products.*

Exception Subscription

On the SAP Easy Access screen, choose *Forecasting & Replenishment → Order Proposal Management → 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 more information, see:

- *SAP Forecasting & Replenishment – Configuration Guide → Settings for the Replenishment Workbench for Stores (RWBS) → Defining User Responsibilities (Backend).*
- *SAP Scenario Forecasting & Replenishment – Configuration Guide → Settings for the Replenishment Workbench for Stores (RWBS) → SAP User Management Engine* (UME).

For information about role maintenance and the SAP Profile Generator, see the SAP Help Portal at help.sap.com → *Documentation → SAP Netweaver → 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*.

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: *Documentation → SAP NetWeaver → Release '04 → <Language> → SAP NetWeaver → Application Platform (SAP Web Application Server) → Databases → MySQL MaxDB → Installation → Installation Manual → Authorization Concept for Unix Operation Systems*.

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 the 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 → Security Aspects for Connectivity and Interoperability → 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 other SAP Components → Advanced Planning and Optimization → Basics settings for setting up the System Landscape → Assign RFC Destinations to Different Application Cases*.
3. Create for each SAP R/3 user a corresponding ATP user in the SAP SCM system.
4. Assign one or more of the following authorization roles to the user(s) in 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 Documentation → 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.

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 4.1 to achieve a secure system landscape.

You will find a detailed description of all communication channels within the component SAP SCM 4.1 on SAP Service Marketplace at **`service.sap.com/scm`** → *mySAP SCM Technology* → *Architecture.*

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

For more information about security aspects for connectivity and interoperability of SAP NetWeaver, see the "*SAP NetWeaver Security Guide*" → *Security Aspects for Connectivity and Interoperability.*

SAP APO – SAP R/3

The integration of SAP APO and SAP R/3 is technically based on SAP APO Core Interface (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 APO - SAP R/3 integration.

For more information about the integration of SAP APO and SAP R/3, see "*SAP SCM Documentation" → SAP Advanced Planning and Optimization (SAP APO) → Integration of SAP APO and SAP R/3 → Technical Integration.*

SAP Event Management (SAP EM)

As SAP 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. We recommend that you activate a secure communication protocol for all used communication channels (for example: SNC). This is **strongly** recommended if you use mobile devices for connecting to SAP EM.

For information about the infrastructure of SAP Event Management, see "S*AP SCM Documentation" → 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 XI Security Guide.

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

You can find the SAP XI security guide on the SAP Service Marketplace at **`service.sap.com/security guide`** → SAP Exchange Infrastructure (XI) Security Guide.

SAP Inventory Collaboration Hub (ICH)

Since 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 Exchange Infrastructure (XI) Security Guide.*

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

We strongly recommend that you use Secure Socket Layer (SSL), since the SAP R/3 user and its password are used to login on to the SAP SCM - WCL.

For more information about security recommendations in SAP SCM - WCL, see the "*SAP SCM Installation Guide" → Installation/Upgrade Guide - SAP WCL 4.1 → Implementation Considerations → Security Recommendations.*

Since SAP SCM - WCL is based on Java technology, you require the SAP Java Crypto Toolkit if you want to configure Secure Socket Layer (SSL).

For more information about downloading and installing the SAP Java Crypto Toolkit for SAP SCM - WCL, see the "*SAP SCM Installation Guide" → Installation/Upgrade Guide - SAP WCL 4.1 → Post-Installation Activities → Downloading the SAP Java Crypto Toolkit.*

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 of SAP NetWeaver, see the *SAP NetWeaver 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 via 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 4.1 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 Security Guide → Network and Communication Security - Using Firewall Systems for Access Control.*

Communication Destinations

Users and authorizations for connection destinations can cause serious security flaws in instances of careless use.

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 logon data for users of type “system”.
- Choose “trusted system” functionality whenever possible, instead of storing connection user logon data.

Connection Destinations

Destinations	Delivered?	Type	User, Authorizations	Description
SAPOSCOL_<DB_hostname> (SAP SCM central instance - DB instance)	Yes	RFC - TCP/IP	-	*“SAP SCM Installation Guide“ → SCM Installation Guide – SCM Server 4.1<Operating System/DB> → Post Installation Activities → Checking the RFC Destination.*
SAP APO Supply Chain Cockpit (SCC) → SAP Business Information Warehouse (BW)	No	RFC - R/3	-	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 → SAP R/3	No	RFC - R/3	Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Note: 447543 **and** 727839.	*SAP SCM IMG: Integration with SAP Components → Integration of SAP SCM and SAP R/3 → Basic Settings for Creating the Systems*

				Landscape → Set Up RFC Destination and Assign RFC Destinations to Various Application Cases.
SAP R/3 → SAP APO (ATP)	No	RFC - R/3 (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 the Integration with SAP Componen [Page 26]ts → *Maintaining Authorizations for Available-to-Promise*.
<System-ID>CLNT<Client number> (SAP liveCache)	No	RFC - R/3	<liveCache User ID>; <liveCache Authorization> (see SAP Note 305634)	"*SAP SCM Installation Guide*" → *Installation Guide – liveCache* → *liveCache Post Installation Activities* → *Setting Up Connection to the liveCache Instance* **and** SAP Note: 305634
OPTSERVER_<Optimizer>01	No	RFC - TCP/IP	-	"*SAP SCM Installation Guide*" → *Installation Guide – SAP APO Optimizer* → *SAP 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" → 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 Documentation" → SAP Event Management (SAP EM) → System Installation and Integration.*
<Logical target system> SAP ICH - SAP R/3	No	RFC-R/3	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 SCM - WCL → SAP SCM Server	Partial	RFC - TCP/ IP	The connection works with the actual front-end user. For information about the required authorization, see the "*SAP SCM Installation Guide" → Installation/Upgrade Guide – SAP Supply Chain Management – Web Communication Layer 4.1 → Installation Preparations → Configuring the Administration User on the SAP SCM Server.*	*"SAP SCM Installation Guide" → Installation/Upgrade Guide 4.1 → Installation Process → Input Parameters → Input Parameters → Input Parameters for Option: Standalone Server*
SAP SCM Server → map&guide mapserver	No	RFC-TCP/IP	-	"*SAP SCM Installation Guide" → Installation Guide - map&guide mapserver → Implementation Process → Creating an RFC Connection on the SAP SCM Server.*

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

Data Storage Security

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

For information about the data storage security of SAP NetWeaver, see "*SAP NetWeaver Security Guide" → Operation System and Database Platform Security Guides.*

Mostly all business data of the component SAP SCM 4.1 is stored in the system database. If SAP liveCache is used, some business data will also be stored there. This business data is protected by the authorization concept of SAP NetWeaver and SAP SCM 4.1.

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

SAP APO Optimizer

The SAP APO Optimizer writes log files to the gateway file system. This 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 – SAP Web Communication Level (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 Installation Guide" → Installation/Upgrade Guide - SAP WCL 4.1 → SAP SCM - WCL Specific Information → SAP SCM - WCL Configuration Parameters → Logging Manager Parameters.*

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.

map&guide mapserver

SAP SCM 4.1 comes with the optional third party software map&guide mapserver. This software requires an RFC destination on the SAP SCM 4.1 side. That RFC is described in the chapter Communication Destinations [Page 31]. For security issues regarding the map&guide mapserver software, see the third party map&guide documentation.

SAP DB

SAP SCM 4.1 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 4.1 using SAP liveCache. To learn more about the security of SAP DB, see the SAP DB Security Guide at that SAP Service Marketplace at:

http:service.sap.com/securityguide → SAP Netweaver '04 DB and OS Plaftorm Security Guides → SAP Security for MySQL Max DB.

Or, SAP Help Portal at: Documentation → SAP NetWeaver → Release '04 → <Language> → SAP NetWeaver → Application Platform (SAP Web Application Server) → Databases → MySQL MaxDB → Basic Information → SAP Security Guide: MySQL 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. This 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" → SAP Event Management (SAP EM) → SAP Event Management Infrastructure → User Interfaces*.

Other Security-Relevant Information

Web Browser as User Front End

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

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**