



Security Guide

SAP Supply Network Collaboration: Security Guide

Release 7.0 Including Enhancement Package 2

Target Audience

- Technical Consultants
- Security Consultants
- System Administrators

CUSTOMER

Document version: 1.1 – 2012-10-03

© Copyright 2012 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, System i, System i5, System p, System p5, System x, System z, System z9, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, POWER5+, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

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

Oracle is a registered trademark of Oracle Corporation.

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

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

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

Java is a registered trademark of Sun Microsystems, Inc.

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

SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Typographic Conventions

Example	Description
<>	Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your <User Name>”.
► → ◄	Arrows separating the parts of a navigation path, for example, menu options
Example	Emphasized words or expressions
Example	Words or characters that you enter in the system exactly as they appear in the documentation
<u>Example</u>	Textual cross-references to an internet address, for example, http://www.sap.com
/example	Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web
<u>123456</u>	Hyperlink to an SAP Note, for example, SAP Note 123456
<i>Example</i>	<ul style="list-style-type: none"> Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options. Cross-references to other documentation or published works
Example	<ul style="list-style-type: none"> Output on the screen following a user action, for example, messages Source code or syntax quoted directly from a program File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE
EXAMPLE	Keys on the keyboard

Document History

**CAUTION**

Before you start the implementation, make sure you have the latest version of this document.

You can find the latest version at the following location: <http://service.sap.com/securityguide>.

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

Version	Date	Description
1.1	2012-10-03	Chapter 2 and chapter 12 updated: new virus scan profiles added
1.0	2011-11-08	First version

Table of Contents

Chapter 1	Introduction	<u>7</u>
Chapter 2	Before You Start	<u>9</u>
Chapter 3	Information About the Technical System Landscape	<u>15</u>
Chapter 4	Security Aspects of Data, Data Flow and Processes	<u>17</u>
Chapter 5	User Administration and Authentication	<u>21</u>
5.1	User Management	<u>21</u>
5.2	User Data Synchronization	<u>24</u>
5.3	Integration Into Single Sign-On Environments	<u>24</u>
Chapter 6	Authorizations	<u>27</u>
6.1	Maintaining Authorizations for SAP Supply Network Collaboration	<u>33</u>
6.2	Maintaining Authorizations for Integration with SAP Components	<u>33</u>
Chapter 7	Session Security Protection	<u>35</u>
Chapter 8	Network and Communication Security	<u>37</u>
8.1	Communication Channel Security	<u>37</u>
8.2	Network Security	<u>39</u>
8.3	Communication Destinations	<u>40</u>
8.4	Internet Communication Framework Security	<u>46</u>

Chapter 9	Data Storage Security	<u>47</u>
Chapter 10	Security for Additional Applications	<u>49</u>
Chapter 11	Enterprise Services Security	<u>51</u>
Chapter 12	Other Security-Relevant Information	<u>53</u>
Chapter 13	Trace and Log Files	<u>55</u>
Chapter 14	Services for Security Lifecycle Management	<u>57</u>
Chapter A	Reference	<u>59</u>
A.1	The Main SAP Documentation Types	<u>59</u>

1 Introduction



CAUTION

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

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

Why is Security Necessary

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



RECOMMENDATION

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

About This Document

The Security Guide provides an overview of the security-relevant information that applies to SAP SNC.

Overview of the Main Sections

The SAP SNC Security Guide comprises the following main sections:

- **Before You Start**

This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

- **Technical System Landscape**

This section provides an overview of the technical components and communication paths that are used by SAP SNC.

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

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

- **User Administration and Authentication**

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

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

■ **Authorizations**

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

■ **Session Security Protection**

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

■ **Network and Communication Security**

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

■ **Internet Communication Framework Security**

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

■ **Data Storage Security**

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

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

This section provides security information that applies to third-party or additional applications that are used with SAP SNC.

■ **Enterprise Services Security**

This section provides security information about enterprise services.

■ **Other Security-Relevant Information**

This section contains information about:

- Virus checks
- Security Settings in File Transfer
- Validation of SOAP Message Header in Inbound XML Messages

■ **Trace and Log Files**

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

■ **Services for Security Lifecycle Management**

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

■ **Appendix**

This section provides references to further information.

2 Before You Start

Fundamental Security Guides

This guide also covers security-related information about the following business scenarios that run on SAP Supply Network Collaboration (SAP SNC):

- Automotive business scenarios:
 - Supplier Managed Inventory (SMI)
 - Release Processing (RP)
 - Web-Based Supplier Kanban (Pull)
 - Web-Based Supplier Kanban with MRP (Pull)
- High Tech business scenarios:
 - Supply Network Inventory
 - Contract Manufacturing Procurement
 - Work Order Collaboration
- Consumer Products business scenarios:
 - Responsive Replenishment

The business scenarios run on the following SAP application components:

- SAP Supply Network Collaboration (SAP SNC)
- SAP Supply Chain Management (SAP SCM) (Responsive Replenishment)
- SAP NetWeaver Process Integration (SAP NetWeaver PI)
- SAP NetWeaver BI
- SAP R/3 4.6C or higher
- SAP DIMP 4.71 or higher (Web-Based Supplier Kanban with MRP (Pull) only)
- SAP Event Management
- SAP Project and Portfolio Management
- SAP NetWeaver Identity Management

Therefore, the corresponding component security guides also apply to SAP SNC business scenarios. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

Fundamental Security Guides

Scenario, Application, or Component Security Guide	Most-Relevant Sections or Specific Restrictions
SAP SCM Component Security Guide	

Scenario, Application, or Component Security Guide	Most-Relevant Sections or Specific Restrictions
SAP NetWeaver Security Guide	In the SAP NetWeaver Security Guide, choose ► <i>Security Guides for SAP NetWeaver According to Usage Types</i> → <i>Security Guide for Usage Type PI</i> → <i>SAP NetWeaver Process Integration Security Guide</i> ◀ In the SAP NetWeaver Security Guide, choose ► <i>Security Guides for the Operating System and Database Platform</i> ◀
SAP Basis / Web AS Security Guide	
SAP ERP Security Guide	
SAP Project and Portfolio Management Security Guide	Collaboration Folders
SAP Event Management Security Guide	
SAP NetWeaver Identity Management Security Guide	

For a complete list of the available SAP Security Guides, see the Quick Link [/securityguide](#) on the SAP Service Marketplace.



NOTE

For more information about the required components and releases for the business scenarios, see the Master Guides for SAP for Automotive, SAP for Consumer Products, and SAP for High Tech on the SAP Service Marketplace at <http://service.sap.com/instguides>.

Important SAP Notes

The most important SAP Notes that apply to the security of SAP SNC are shown in the table below.

Important SAP Notes

Title	SAP Note Number	Comment
Collective Security Note	1394093	This note cover release-independent information concerning security-related issues for SAP systems.
Security Guide: SAP Supply Chain Management	700659	The note covers all problems discovered after the publication of the security guide and contains additional information about security issues.
Single Sign-On Solutions	138498	Information about Single Sign-On solutions for SAP systems
Trusting/Trusted Systems	128447	Discusses the issues relevant to setting up a trusted/trusting system

Title	SAP Note Number	Comment
		relationship between two SAP systems.
Installation/Upgrade SCMSNC 701 auf NW 7.0 EHP2	1501625	Provides instructions on how to install SAP SNC 7.0 on SAP NetWeaver 7.0 including enhancement package 2
Adobe Acrobat Reader Creates Temporary Files	853497	Provides instructions on how to delete PDF files that are stored in the Temporary Internet Files folder. If you open PDF files while using Web-based applications, these files are not necessarily deleted when you close the applications. This could be a security issue if the PDF file contains confidential information.
Business Partners in SAP SNC	1122502	The note enhances the Display Partner, User, Location Assignments transaction (/SCA/USRPRTLLOC). With the enhanced transaction, you can display all users without business partner assignment (see also <i>User Management</i> [page 21]).
Consulting Note—How to switch off authorization check in selection modes	1113695	Provides instructions on how to switch off authorization checks in selection mode configuration.
Configuration of e-mail, fax, paging or SMS using SMTP	455140	Provides instructions on how to configure e-mail, fax, paging or SMS in the SAP Web Application Server using SMTP. It also explains, which prerequisites and settings are required outside the SAP system.
Secure E-mail: Encryption, digital signature	149926	Provides instructions on how to encrypt or assign a digital signature to an e-mail when you send them from SAP systems.
Integrating a virus scan into SAP applications	817623	Provides instructions on how to integrate a virus scan.
Virus scan profile update	1695265	Provides instructions on how to set up separate virus scan profiles for the Work Order component, and for the microblog building block for the quick view.
Antivirus protection within SAP applications	639486	Provides information about antivirus protection.

Title	SAP Note Number	Comment
Data protection and security in SAP Systems	30724	Questions on the topic of data protection in SAP systems and in R/3 in particular.
Super user feature in SNC	1430757	For certain UIs in SAP SNC, SAP SNC offers a super user functionality. This means: if a business partner is not assigned to a user, he or she can see all data for which he or she has authorization according to the user role. Due to security concerns this functionality will not be supported by default anymore.
Setting up SSL on Web Application Server ABAP	510007	Provides a brief description of the steps required to set up SSL on the Web Application Server ABAP.
New start authorization check for Web Dynpro ABAP	1413011	Provides details about the new start authorization check for Web Dynpro ABAP applications. This note is relevant for the business-process roles we deliver.

Additional Information

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

Quick Links to Additional Information

Content	Quick Link on the SAP Service Marketplace or SDN
Security	► https://service.sap.com/security ◀
Related SAP Notes	► https://service.sap.com/notes ◀
Security related SAP Notes	► http://service.sap.com/securitynotes ◀
SAP Solution Manager	► https://service.sap.com/solutionmanager ◀
SAP NetWeaver Security Guide	► https://service.sap.com/securityguide ◀
SAP NetWeaver documentation	► https://help.sap.com/nw703 → SAP NetWeaver ◀
Master Guide for SAP SCM 7.0 including enhancement package 2	► https://service.sap.com/instguides → SAP Business Suite Applications → SAP SCM → SAP SCM Server → Using SAP SCM 7.0 Server → Using SAP enhancement package 2 for SAP SCM 7.0 Server ◀
SAP SCM documentation	► https://help.sap.com/scm702 → SAP Supply Chain Management ◀
SAP SCM 7.0 Installation Guide including enhancement package 2	► https://service.sap.com/instguides → SAP Business Suite Applications → SAP SCM → SAP SCM Server → Using SAP SCM 7.0 Server → Using SAP enhancement package 2 for SAP SCM 7.0 Server ◀
SAP SCM Component Security Guide	► https://service.sap.com/securityguide → SAP Supply Chain Management ◀
Master Guide for SAP SNC 7.0 including enhancement package 2	► https://service.sap.com/instguides → SAP Business Suite Applications → SAP SCM → SAP SNC → Using

Content	Quick Link on the SAP Service Marketplace or SDN
	<i>SAPSNC 7.0 → Using SAP enhancement package 2 for SAPSNC 7.0</i> ↩
SAP SNC documentation	▶ https://help.sap.com/snc702 → <i>SAP Supply Network Collaboration</i> ↩
SAP Event Management Security Guide	▶ https://service.sap.com/securityguide → <i>SAP Event Management</i> ↩
SAP Project and Portfolio Management Security Guide	▶ https://service.sap.com/securityguide → <i>SAP cProject Suite Security Guides</i> → <i>SAP Project and Portfolio Management Security Guide</i> ↩
SAP SNC Business Scenarios: Configuration Documentation	The configuration documentation is part of SAP Solution Manager.
SAP WebAS Security Guide	▶ https://service.sap.com/securityguide → <i>SAP Basis/Web AS Security Guides</i> ↩
SAP NetWeaver Identity Management 7.1 Security Guide	▶ http://help.sap.com/nwidm71/ → <i>SAP NetWeaver Identity Management 7.1 → Installation and Implementation</i> → <i>Security Guide</i> ↩
SAP NetWeaver Installation Guide	▶ https://service.sap.com/instguides → <i>SAP NetWeaver</i> → <i>SAP NetWeaver 7.0 (2004s)</i> → <i>Installation</i> ↩
SAP NetWeaver usage type Process Integration (PI): Configuration	The configuration documentation is part of SAP Solution Manager.
BI Content documentation	▶ http://help.sap.com/nw703/ → <i>SAP NetWeaver by Key Capability</i> → <i>BI Content</i> ↩

For more information about security, see SAP Service Marketplace at ▶ <http://service.sap.com/security> → *SAP NetWeaver* → *SAP NetWeaver in Detail* → *Security* → *SAP Security Notes* ↩.

**This page is left blank for documents
that are printed on both sides.**

3 Information About the Technical System Landscape

The following table provides links to additional information about the technical system landscape:

More Information About the Technical System Landscape

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace or SDN
Technical system landscape for SAP Supply Network Collaboration (SAP SNC)	SAP SNC Master Guide and Industry Master Guides for Automotive, Consumer Products, and High Tech	https://service.sap.com/instguides
Technical system landscape and installation procedure for SAP Supply Chain Management (SAP SCM) and SAP ERP	SAP SCM Installation Guide SAP ERP Installation Guide	https://service.sap.com/instguides
Installation of SAP SNC	SAP Note 1501625	
Security		https://service.sap.com/security

Deployment Options

SAP SNC can run with the following deployment options:

- As an add-on with SCM Basis in SAP NetWeaver
- As part of the SAP SCM Server

For more information about the security of the SAP SCM Server, see the SAP SCM Security Guide.

Optional Components

SAP Event Management and Collaboration Folders (cFolders) are optional components that can run with SAP SNC. The SAP SNC Security Guide also contains SAP SNC relevant security information about cFolders. For more information about SAP SNC relevant security information for SAP Event Management and cFolders, see the SAP Event Management Security Guide on SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP Event Management* ◀ or the SAP Project and Portfolio Management Security Guide on SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP Project and Portfolio Management* ◀.

For more information about the system landscape, see the SAP SNC Master Guide on SAP Service Marketplace at ► <http://service.sap.com/instguides> → *SAP Business Suite Applications* → *SAP SCM* → *SAP SNC* → *Using SAP enhancement package 2 for SAP SNC 7.0* ◀.

**This page is left blank for documents
that are printed on both sides.**

4 Security Aspects of Data, Data Flow and Processes

The figures below show an overview of the data flow for two features of the file transfer function in SAP Supply Network Collaboration (SAP SNC). For these two features, you must set up the e-mail infrastructure of the system to check or generate digital signatures for inbound or outbound e-mails or to encrypt the content of the e-mails.

Data Flow of a File Download and Delivery by E-Mail

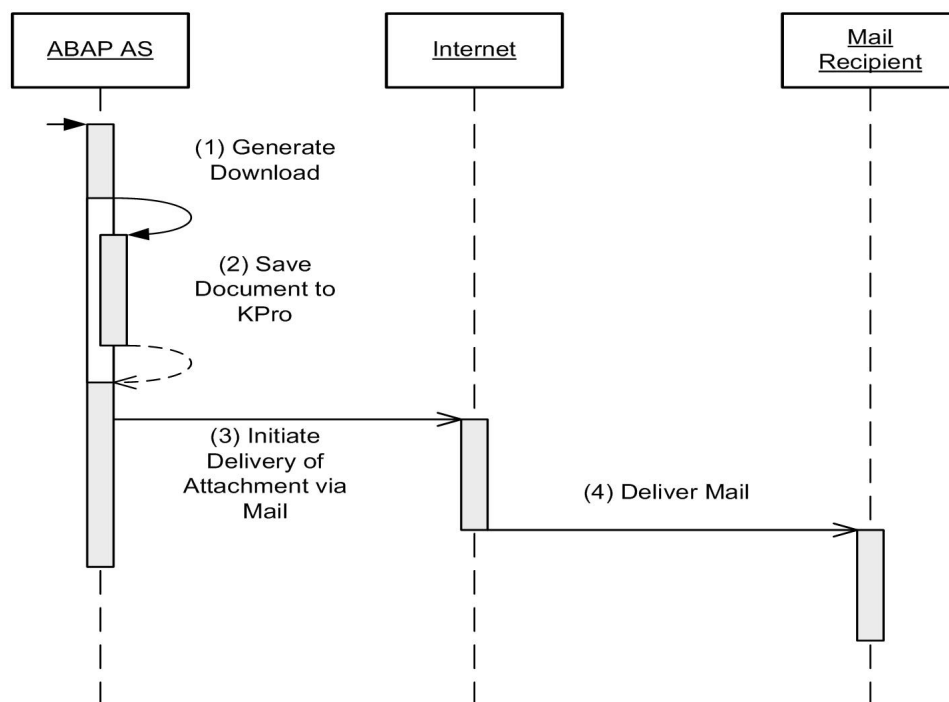


Figure 1: Data Flow for Download

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

Step	Description	Security Measure
1	Generate Download	The download job runs in the name of the user who is the download profile owner. The system bases the visibility of master data and transactional data on the authorization rights given to the user who is the download profile owner.
2	Save Download to KPro	Not available

Step	Description	Security Measure
3	Initiate Delivery of Mail with Attachment	If the system sends the e-mail through a network that is unknown or not trusted, you must protect the content of the e-mail against any third parties who may attempt to view or change any master data or transactional data.
4	Deliver Mail	Not available

Data Flow of a File Upload from an Inbound E-Mail

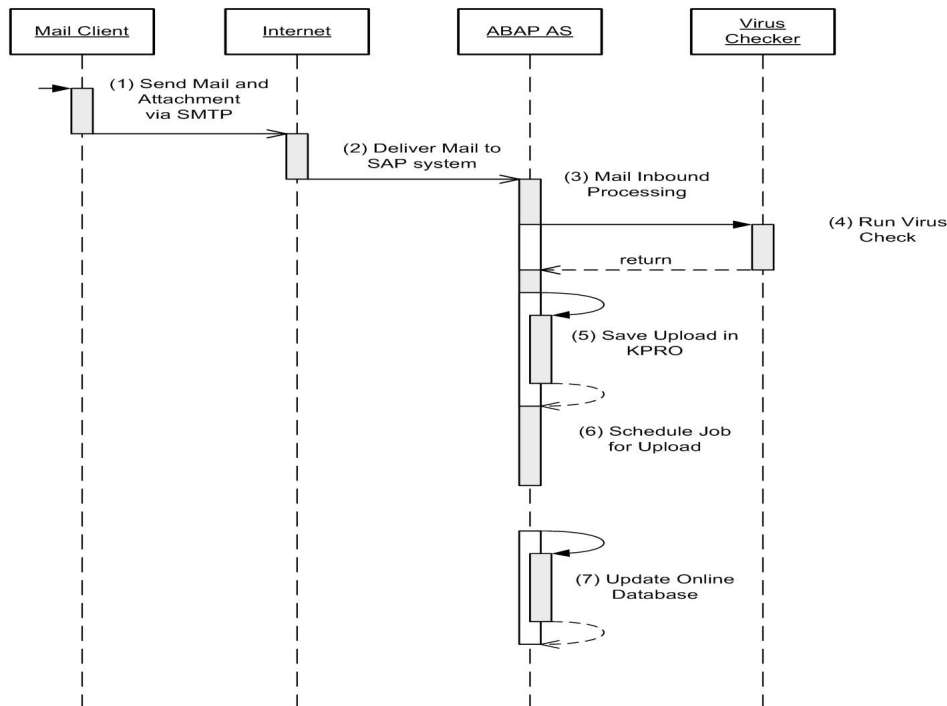


Figure 2: Data Flow for File Upload

Step	Description	Security Measure
1	Send Mail (via SMTP)	If the system sends the e-mail through a network that is unknown or not trusted, you must protect the content of the e-mail against any third parties who may attempt to view or change any master data, transactional data, or accompanying meta information such as the sender's e-mail address.
2	Deliver Mail to SAP System	Not available
3	Mail Inbound Processing	A technical user processes the inbound e-mail. You must enter the sender's e-mail address as an accepted e-mail address for file uploads in Customizing for <i>Supply Network Collaboration</i> under ► <i>Tools</i> → <i>File Transfer</i> → <i>Determine Accepted E-Mail Addresses for File Upload</i> ⚙.
4	Run Virus Check	You must check the uploaded file for viruses. The virus scanner can be located on another system, therefore take into consideration that master data or transactional data can pass through an unsecured network.
5	Save Upload in KPro	Not available
6	Schedule Job for Upload	Not available

Step	Description	Security Measure
7	Scheduled Job Updates Data in Database	The upload job runs in the name of the user who is the download profile owner. The system bases the visibility of master data and transactional data on the authorization rights given to the user who is the upload profile owner.

**This page is left blank for documents
that are printed on both sides.**

5 User Administration and Authentication

SAP Supply Network Collaboration (SAP SNC) uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide also apply to SAP SNC.

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

- *User Management* [\[page 21\]](#)

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

- *User Data Synchronization* [\[page 24\]](#)

This topic describes how the user data is synchronized with other sources.

- *Integration Into Single Sign-On Environments* [\[page 24\]](#)

This topic describes how SAP SNC supports Single Sign-On mechanisms.

5.1 User Management

User management for SAP Supply Network Collaboration (SAP SNC) uses the mechanisms provided by the SAP NetWeaver Application Server (ABAP), for example, tools, user types, and password policies. For an overview of how these mechanisms apply for SAP SNC, see the sections below. In addition, we provide a list of the standard users required for operating SAP SNC.

User Administration Tools

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

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.
User Administration on the SAP SNC Web user interface using the <i>User Administration</i> Web screen.	Use the <i>User Administration</i> Web screen to maintain users for the leading business partner in a supplier collaboration, as well as for its business partners.
User Administration in the SAP NetWeaver Identity Management system.	Use Identity Management to maintain users centrally in a dedicated SAP NetWeaver Identity Management system. For

5.1 User Management

Tool	Detailed Description
	more information, see <i>Documentation Center – SAP NetWeaver Identity Management 7.0 / 7.1</i> at ► http://service.sap.com/instguides → <i>SAP NetWeaver</i> → <i>SAP NetWeaver Identity Management 7.0</i> ◀.
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.
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.

User Types

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

The user types that are required for SAP SNC include:

- Individual users:
 - Dialog users are used for individual, interactive system access.
- Technical users:
 - Service users are dialog users that are available to a larger, anonymous group of users.
 - Communication users are used for dialog-free communication for external RFC calls.

For more information about these user types, see the SAP NetWeaver AS ABAP Security Guide on SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *User Administration and Authentication* → *User Management* ◀.

Standard Users

The table below shows the standard users that are necessary for operating SAP SNC.

Standard Users

System	User	Delivered?	Type	Password	Description
SAP NetWeaver	Communication users for the connection between SAP SNC and SAP NetWeaver	No	Dialog User	To be entered	For more information, see the SAP NetWeaver Installation Guide under <i>Ensuring User Security</i> .

System	User	Delivered?	Type	Password	Description
SAP SNC	Business partner users	No	Dialog User	To be entered	For more information, see the references below.

Remark About Business Partner Users in SAP SNC

For each business partner (supplier, customer, third-party logistics provider), you must create an SAP SNC business partner of type Organization. For each user at a business partner (supplier, customer, third-party logistics provider), you must create an SAP SNC business partner of type Person, and an SAP SNC user. When you create users, make sure you assign them to business partners. In addition, when you synchronize users in SAP SNC and in other SAP NetWeaver based systems, make also sure you assign these users to business partners.



CAUTION

In customer collaboration, users that are not assigned to any business partner can access all data in SAP SNC, regardless to which business partner the data belongs. Depending on the users' authorizations, they can also edit the data. You can check the business partner assignment of your users using the *Display Partner, User, Location Assignments* (transaction code /SCA/USRPRTLOC) transaction. To call up the *Display Partner, User, Location Assignments* transaction, on the *SAP Easy Access* screen, choose ► *Supply Network Collaboration* → *Master Data* → *Visibility* → *Display Partner, User, Location Assignments* ⚡.

Further Information

For more information, see the following:

- Creating business partners for *Supplier Managed Inventory* and *Release Processing*

For more information, see the configuration documentation ► *Solutions/Applications* → *SAP for Automotive* → *Scenarios* → *Supplier Managed Inventory or Release Processing* ⚡.

Choose the following topics:

- Creating an SCM User (for the Customer)
 - Creating Business Partner of Type Person (for the Customer)
 - Creating an SCM User (for the Supplier)
 - Creating Business Partner of Type Person (for the Supplier)
 - Creating business partners for *Web-Based Supplier Kanban* (all scenario variants)
- For more information, in SAP Solution Manager, choose ► *Solutions/Applications* → *SAP for Automotive* → *Scenarios* → *Web-Based Supplier Kanban (with MRP) (Pull)* ⚡.
- Creating business partners for *Supply Network Inventory*, *Work Order Collaboration*, and *Contract Manufacturing Procurement*

5.2 User Data Synchronization

For more information, in SAP Solution Manager, choose ► *Solutions/Applications* → *SAP for High Tech* → *Scenarios* → *Supply Network Inventory* ⚡, ► *Work Order Collaboration*, ⚡ or ► *Contract Manufacturing Procurement* ⚡.

■ Standard users

For more information, see the SAP NetWeaver Security Guide at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *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 NetWeaver Password Rules

For more information, see the SAP NetWeaver documentation on SAP Help Portal at <http://help.sap.com/nw703>. In SAP Library, choose ► *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *Identity Management of the Application Server ABAP* → *Configuration of Identity Management* → *First Installation Procedure* → *Logon and Password Security in the ABAP System* → *Password Rules* ⚡.

5.2 User Data Synchronization

By using user data synchronization in your system landscape, you can avoid administration effort. Since SAP Supply Network Collaboration (SAP SNC) including enhancement package 2 is based on SAP enhancement package 3 for SAP NetWeaver 7.0, all the mechanisms for user data synchronization of SAP NetWeaver 7.0 EHP3 are available for SAP SNC.

For more information about user data synchronization, see the Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guide (Online Version)* → *User Administration and Authentication* → *Integration of User Management in Your System Landscape* ⚡.

Integration of SAP SNC with SAP NetWeaver Identity Management

With SAP NetWeaver Identity Management, you can trigger automatic generation of users and business partners for SAP SNC. For more information, see the SAP Help Portal at <http://help.sap.com/snc702>. In SAP Library, choose under ► *Processes and Tools for Enterprise Applications (CA-EPT)* → *User Management and Distribution with SAP NetWeaver Identity Management* → *Identity Management for SAP Supply Network Collaboration* ⚡.

5.3 Integration Into Single Sign-On Environments

SAP Supply Network Collaboration (SAP SNC) supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Security Guide* also apply to SAP SNC.

**NOTE**

For more information about integration into SSO environments based on SAP NetWeaver, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → SAP NetWeaver 7.0 Security Guides (Complete) → SAP NetWeaver 7.0 EhP3 Security Guides (Online Version) → 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 Service Marketplace at ► <http://service.sap.com/securityguide> → SAP NetWeaver 7.0 Security Guides (Complete) → SAP NetWeaver 7.0 EhP3 Security Guides (Online Version) → Security Guides for SAP NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server ABAP Security Guide → User Authentication ◀.

The most widely-used supported mechanisms are listed below.

- Secure Network Communications (SNC)

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

For more information, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → SAP NetWeaver 7.0 Security Guides (Complete) → SAP NetWeaver 7.0 EhP3 Security Guides (Online Version) → Network and Communication Security → Transport Layer Security → Secure Network Communications (SNC) ◀.

- SAP Logon Tickets

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

For more information, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → SAP NetWeaver 7.0 Security Guides (Complete) → SAP NetWeaver 7.0 EhP3 Security Guides (Online Version) → Network User Administration and Authentication → User Authentication and Single Sign-On ◀.

- Client certificates

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

For more information, go to the SAP Service Marketplace at ► <http://service.sap.com/securityguide> → SAP NetWeaver 7.0 Security Guides (Complete) → SAP NetWeaver 7.0 EhP3 Security Guides (Online Version) → User Administration and Authentication → User Authentication and Single Sign-On ◀.

**This page is left blank for documents
that are printed on both sides.**

6 Authorizations

SAP Supply Network Collaboration (SAP SNC) uses the authorization provided by the SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver AS Security Guide ABAP* also apply to SAP SNC.

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



NOTE

For more information about how to create roles, see the SAP NetWeaver documentation at <http://help.sap.com/nw703>. In SAP Library, choose ► *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *Identity Management of the Application Server ABAP* → *Administering Users and Roles* ◀.

Standard Roles

In SAP SNC, we deliver standard technical roles and standard business-process roles.

Standard Technical Roles for SAP SNC

Role	Description
SAP_SCM_ICH_DISPLAY	SAP SNC: Display User
SAP_SMI_SUPERUSER	SAP SNC: Superuser
SAP_SMI_MD	SAP SNC: Master Data Maintenance
SAP_SMI_EXT_MD_SUPERUSER	SAP SNC: Master Data Superuser
SAP_SMI_SELASSN	SAP SNC: Selection Assignments
SAP_SMI_SELECTIONS	SAP SNC: Selection Maintenance
SAP_SCM_ICH_ALRT_TYP	SAP SNC: Alert Display
SAP_SCM_ICH_AMON	SAP SNC: Alert Monitor Maintenance

Standard Business-Process Roles as of SAP SNC 7.02

Role	Description
SAP_SMI_ASNDISPLAY	Supplier Collaboration: ASN Display
SAP_SMI_ASNSUPERUSER_2	Supplier Collaboration: ASN Superuser
SAP_LIME_USER_2	General Basis Authorizations
SAP_SCM_ICH_IV_SUP_2	Invoice Maintenance (Supplier)
SAP_SCM_ICH_ASN_SUP_2	ASN Maintenance (Supplier)
SAP_SCM_ICH_RK_SUP_2	Release and Kanban Processing (Supplier)
SAP_SCM_ICH_DR_SUP_2	Dynamic Replenishment (Supplier)

Role	Description
SAP_SCM_ICH_FCS_CUS_2	Forecast Collaboration (Customer)
SAP_SCM_ICH_FCS_SUP_2	Forecast Collaboration (Supplier)
SAP_SCM_ICH_OMO_CUS_2	Outsourced Manufacturing: Order Processing (Customer)
SAP_SCM_ICH_OMO_SUP_2	Outsourced Manufacturing: Order Processing (Supplier)
SAP_SCM_ICH_OMP_CUS_2	Outsourced Manufacturing: Planning (Customer)
SAP_SCM_ICH_PO_SUP_2	Purchase Order Processing (Supplier)
SAP_SCM_ICH_QN_SUP_2	Quality Collaboration (Supplier)
SAP_SCM_ICH_RP_SUP_2	Replenishment Processing (Supplier)
SAP_ICH_PLANNER_2	Responsive Replenishment: Planner (Supplier)
SAP_SCM_ICH_SU_CUS_2	Supplier Collaboration: Superuser (Customer)
SAP_SCM_ICH_SU_SUP_2	Supplier Collaboration: Superuser and Administrator (Supplier)
SAP_SCM_ICH_ADM_CUS_2	Supplier Collaboration: Administrator (Customer)
SAP_SCM_ICH_DPA_SUP	Supplier Performance Management (Supplier)
SAP_SCM_ICH_DPA_CUS	Supplier Performance Management (Customer)

**CAUTION**

As of SAP SNC including enhancement package 2, the standard roles in the *Obsolete Standard Roles as of SAP SNC 7.02* table are obsolete. For more information, see the documentation for roles SAP Help Portal at <http://help.sap.com/snc702>. In SAP Library, choose ► *Cross-Application Functions* → *Partner and User Management* → *Roles for SAP Supply Network Collaboration (SAP SNC)* ◀ and SAP Note [1413011](#).

Obsolete Standard Roles as of SAP SNC 7.02

Role	Description
SAP_SMI_ASNDISPLAY	Supplier Collaboration: ASN Display
SAP_SMI_ASNSUPERUSER	Supplier Collaboration: ASN Superuser
SAP_LIME_USER	General Basis Authorizations
SAP_SCM_ICH_IV_SUP	Invoice Maintenance (Supplier)
SAP_SCM_ICH_ASN_SUP	ASN Maintenance (Supplier)
SAP_SCM_ICH_RK_SUP	Release and Kanban Processing (Supplier)
SAP_SCM_ICH_DR_SUP	Dynamic Replenishment (Supplier)
SAP_SCM_ICH_FCS_CUS	Forecast Collaboration (Customer)
SAP_SCM_ICH_FCS_SUP	Forecast Collaboration (Supplier)
SAP_SCM_ICH_OMO_CUS	Outsourced Manufacturing: Order Processing (Customer)
SAP_SCM_ICH_OMO_SUP	Outsourced Manufacturing: Order Processing (Supplier)
SAP_SCM_ICH_OMP_CUS	Outsourced Manufacturing: Planning (Customer)
SAP_SCM_ICH_PO_SUP	Purchase Order Processing (Supplier)
SAP_SCM_ICH_QN_SUP	Quality Collaboration (Supplier)
SAP_SCM_ICH_RP_SUP	Replenishment Processing (Supplier)
SAP_ICH_PLANNER	Responsive Replenishment: Planner (Supplier)

Role	Description
SAP_SCM_ICH_SU_CUS	Supplier Collaboration: Superuser (Customer)
SAP_SCM_ICH_SU_SUP	Supplier Collaboration: Superuser and Administrator (Supplier)
SAP_SCM_ICH_ADM_CUS	Supplier Collaboration: Administrator (Customer)

Roles for SAP SNC

With SAP SNC, you get a number of predefined user roles with which you can assign the correct authorizations and user menus. You can use these roles as they are defined, or you can adapt them to your specific needs. In addition, you can use the authorization objects for these roles to create your own roles.

For more information about predefined user roles in SAP SNC, see SAP Help Portal at <http://help.sap.com/snc702>. In SAP Library, choose ► *Cross-Application Functions* → *Partner and User Management* → *Roles for SAP Supply Network Collaboration (SAP SNC)* ◀.

For more information about assigning roles for the Supplier Managed Inventory and Release Processing business scenarios, see the configuration documentation in SAP Solution Manager under ► *Solutions/Applications* → *SAP for Automotive* → *Scenarios* → *Supplier Managed Inventory or Release Processing* → *Configuration* → *Business Customizing in SAP SCM* → *Users and Authorizations* → *Generating and Assigning Roles* ◀.

Roles for SAP NetWeaver Usage Type Process Integration

In SAP NetWeaver, you get a number of predefined user roles. There are user roles for SAP NetWeaver configuration and user roles for the necessary service users for Process Integration (PI).

For more information about user roles for PI in SAP NetWeaver, see the configuration documentation in SAP Solution Manager under ► *Solutions/Applications* → *Basic Configuration* → *Configuration Structures* → *SAP NetWeaver 2004s* → *Usage Type PI* → *Communication and Security* → *User Management and User Roles* ◀.

Other Roles and Authorizations

Collaboration Folders Integration

You can integrate Collaboration Folders (cFolders) with SAP SNC by installing cFolders on the same server that SAP SNC has been installed on or on a different server. SAP SNC can call cFolders using remote function calls (RFCs). We therefore recommend that you always use a RFC destination for the connection between cFolders and SAP SNC.

For RFC communication between cFolders and SAP SNC, you need to have created two users, a user in SAP SNC that also exists in cFolders (in the following called SNCUSER1) and a technical user in the cFolders system (in the following called CFOLDERUSER).



RECOMMENDATION

We recommend you set up the RFC destination in SAP SNC with the technical user CFOLDERUSER and a saved password.

The following table lists the roles and authorization objects that you must assign to the users:

User	System	Role	Authorization Object
SNCUSER1	cFolders	CFX_USER	Not relevant
SNCUSER1	SAP SNC	Not relevant	C_SNC_CF
CFOLDERUSER	cFolders	SAP_CFX_ADMINISTRATOR and SAP_CFX_USER	Not relevant

The table below shows the security-relevant authorization objects that are used by SAP SNC for the Collaboration Folders (cFolders) integration:

Standard Authorization Objects

Authorization Object	Field	Value	Description
CFX_OBJ	CFX_OBJ	COL	Authorization for collaborations in the collaborative scenario
CFX_OBJ	ACTVT	01	Adding or creating objects
CFX_USER	USER_TYPE	USER	The user needs this field value to use cFolders.
ACO_SUPER			This is the authorization for reading, writing, or managing specified object types. Possible values for cFolders are: <ul style="list-style-type: none"> ■ <i>area</i>: Authorization for all existing collaborations ■ <i>stat_prof</i>: Authorization for all status profiles ■ <i>usrgrp</i>: Authorization for all user groups

If you do not want to install cFolders on the same system as SAP SNC, you can install it on a separate server. In this case, SAP SNC calls the cFolders system on another server, using remote function calls (RFCs). Therefore you need the S_RFC authorization object, as indicated below:

Standard Authorization Objects for Calling cFolders on Another Server

Authorization Object	Field	Value	Description
S_RFC	ACTVT	16	Execute
S_RFC	RFC_NAME	From CFX_ACO to CFX_ACO* From CFX_API to CFX_API* CFX_MA_UI CFX_UI_API CFX_UI_BADI CPRO_API RFC1 SDIFRUNTIME SYST SYSU UWLCONN	
S_RFC	RFC_TYPE	FUGR	Type of RFC object to be protected: function group
S_RFACL	RFC_SYSID	System ID of cFolders system	

Authorization Object	Field	Value	Description
S_RFCACL	RFC_CLIENT	Client of cFolders system	
S_RFCACL	RFC_EQUSER	Y	
S_RFCACL	RFC_TCODE	se37	
S_RFCACL	ACTVT	16	

Web-Based Supplier Kanban


For more information about other roles and authorizations in SAP SCM, see the SAP SCM Component Security Guide under *Authorizations*.

For the business scenario variants of *Web-Based Supplier Kanban*, you need to ensure that users have the authorizations for kanban processing in the ERP system.

File Transfer

File transfer can receive files by means of inbound e-mails that contain the files in the form of attachments. To process the e-mails, file transfer uses the SAPconnect service. You must create a user for the SAPconnect service that you are using. The user assigned to the SAPconnect service processes the attachments in batch jobs. The batch jobs run under the name of the SAPconnect service user. To ensure that the SAPconnect user can run batch jobs for the web users who use file transfer, you must add the following authorizations to the SAPconnect service user:

Standard Authorization Objects for Batch Jobs in File Transfer

Authorization Object	Field	Value
S_BTCH_NAM	BTCUNAME	<div>  NOTE By listing users maintained in transaction SU01 or user administration for SAP SNC here, you ensure that the user assigned to the SAPconnect service can only run batch jobs for those users. </div>
S_BTCH_JOB	JOBACTION	RELE
S_BTCH_JOB	JOBGROUP	*
S_BTCH_ADM	BTCADMIN	Y



NOTE

The user that you assign to the SAPconnect service is a general user. We recommend that you restrict access to the transaction *Exit Rules for Inbound Processing* (S050). By doing this you avoid that the user assigned to the SAPconnect service adds any harmful exit names.

Roles for the Integration of SAP NetWeaver Identity Management with SAP SNC

You have created a user in SAP SNC that a system administrator can use for calling up SAP SNC from the SAP NetWeaver Identity Management system in the background. You have assigned the technical roles SAP_CA_BP_IDM_INTEGRATION and SAP_BC_SEC_IDM_COMMUNICATION to this user in SAP SNC.

If you are triggering the creation of users and business partners for SAP NetWeaver Identity Management with User Administration on the SAP SNC Web user interface, you need to assign authorization objects to your users.

The following table displays the authorization objects required:

Authorization Object	Field	Value	Description
S_RFC	ACTVT	16	Execute
S_RFC	RFC_NAME	SPML_CLIENT	
S_RFC	RFC_TYPE	FUGR	Type of RFC object to be protected: function group

Two-Level Authorization Concept in SAP SNC

To control which SAP SNC Web screens are visible to a user and which transactional or master data he or she can maintain, SAP SNC uses the following authorization concepts:

- Roles

The role assigns the correct authorizations and user menus to SAP SNC users. For more information, see the SAP Help Portal at <http://help.sap.com/snc702>. In SAP Library, choose ► *Cross-Application Functions* → *Partner and User Management* → *Roles for SAP Supply Network Collaboration (SAP SNC)* ↩.

- User-partner-based or profile-based and parameter-based visibility concept

These visibility concepts restrict the visibility of a user of a business partner in an SAP SNC application to the master data and transaction data that is relevant and allowed for the business partner based on his or her role in the supply chain. This authorization is determined using selection modes. For more information, see the SAP Help Portal at <http://help.sap.com/snc702>. In SAP Library, choose ► *Cross-Application Functions* → *Partner and User Management* → *Visible Master and Transaction Data* ↩.

- Authorization objects per location and product

A system administrator can assign an authorization object to a location, a product, or a specific location-product combination. SAP SNC restricts the results of selections that a user enters on an application Web screen to restrict the visibility of locations and products.

Once SAP SNC determines the user menus that are visible to the user using roles, SAP SNC uses a two-level authorization concept to determine which transactional data is visible to the user. The first level of authorization depends on the selection mode that the Web screen has been assigned. The second level of authorization is based on authorization objects that the system administrator can assign on location-product level per user.



EXAMPLE

A system administrator creates the supplier user SUPPLIER1 and assigns him or her to the supplier business partner SNC_SUP. The system administrator further assigns the purchase order processing role to SUPPLIER1, which authorizes him or her to use all purchase order (PO) relevant screens. The PO relevant Web screens use the selection mode ODM_PO, which means that in the

6.1 Maintaining Authorizations for SAP Supply Network Collaboration

supplier view in which business partner SNC_SUP is automatically set as the supplier, SUPPLIER1 can view all POs in which SNC_SUP is maintained as the supplier. To further restrict the location products that are visible to SUPPLIER1, a system administrator can assign authorization objects to specific location products. If SUPPLIER1 creates a selection with location products that are restricted by the authorization object, the system automatically restricts SUPPLIER1's visibility of these location products.

6.1 Maintaining Authorizations for SAP Supply Network Collaboration

This procedure allows you to maintain authorizations for SAP Supply Network Collaboration (SAP SNC).

Procedure

Specifying the Responsible Planner

1. In Customizing for *SCM Basis*, choose ► *Master Data* → *Specify Person Responsible (Planner)* ◀.
2. To assign planning privileges to planners, maintain the applications for which a planner is responsible:
 1. Choose *New Entries*.
 2. In *Planner*, enter a value.
 3. Select the relevant application area.
 4. Enter information in the following fields:
 - *Name*
 - *Full Name*
 - *DL Name*
3. Save your entries.

6.2 Maintaining Authorizations for Integration with SAP Components

This procedure allows you to maintain authorizations to integrate with SAP components. In particular, with the appropriate authorization settings, you can exclude DataSources from being extracted to SAP NetWeaver Business Intelligence (SAP NetWeaver BI). Data that is stored in the extraction structure of this DataSource cannot be transferred to SAP NetWeaver BI.

Procedure

Setting User Parameters for SAP SNC – SAP ERP Integration

1. In Customizing for *Supply Network Collaboration*, choose ► *SCM Basis* → *Integration* → *Basic Settings for Data Transfer* → *Set User Parameters* ◀.

6.2 Maintaining Authorizations for Integration with SAP Components

2. Under the *User* column, enter the user name as specified in the user master.
3. Using the pull-down list, select your entries for the following parameters:
 - *Logging*
This option allows you to configure application log on a user-specific basis.
 - *Debugging*
This option allows you to activate/deactivate debugging on a user-specific basis.
 - *Recording*
This option allows you to control event recording (the publication of planning results).
4. Save your entries.

Maintaining Authorizations for Data Transfer to the SAP Business Information Warehouse

1. In Customizing for *Integration with SAP Components*, choose ► *Data Transfer to the SAP Business Information Warehouse* → *General Settings* → *Limit Authorizations for Extraction* ◄.
2. Follow the instructions of the Customizing documentation.

7 Session Security Protection

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management. We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

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

For more information and detailed instructions, see *Activating HTTP Security Session Management* on AS ABAP in the AS ABAP security documentation.

**This page is left blank for documents
that are printed on both sides.**

8 Network and Communication Security

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

The network topology for SAP Supply Network Collaboration (SAP SNC) is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to SAP SNC. Details that specifically apply to SAP SNC are described in the following topics:

- *Communication Channel Security* [page 37]

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

- *Network Security* [page 39]

This topic describes the recommended network topology for SAP SNC. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate SAP SNC.

- *Communication Destinations* [page 40]

This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* ◀ under the following sections:

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

8.1 Communication Channel Security

The table below shows the communication paths used by SAP Supply Network Collaboration (SAP SNC), the protocol used for the connection, and the type of data transferred.

8.1 Communication Channel Security

Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a Webbrowser to application server	HTTP	Application data	Passwords
Application server to application server	RFC	Application data	Passwords

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

**NOTE**

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

Communication channels transfer all kinds of your business data, so you should protect them from unauthorized access. SAP offers general recommendations and technologies, based on SAP NetWeaver, to protect your system landscape.

Secure Network Communication**CAUTION**

To ensure a secure system landscape, you must activate the SNC for all the communication channels in SAP SNC. For more information, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *Network and Communication Security* → *Transport Layer Security* → *Secure Network Communications (SNC)* ◀.

Communication Channels and Connectivity

For more information about the communication channels in SAP SNC, see SAP Service Marketplace at ► <http://service.sap.com/scm> → *Technology* → *Architecture overview* ◀.

For more information about the communication security for SAP NetWeaver, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *Network and Communication Security* ◀.

For more information about security aspects for connectivity and interoperability of SAP enhancement package 3 for SAP NetWeaver 7.0, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Connectivity Security Guides* ◀.

Security for Message-Based Transactions

SAP NetWeaver Process Integration (SAP NetWeaver PI) is a prerequisite for message-based transactions in SAP SNC. For more information about SAP NetWeaver PI security, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP Process Integration (PI) Security Guides* ◀.

Using Customer-Specific X.509 Client Certificates for SSL in SAP SNC

To use customer-specific X.509 client certificates for SSL, see SAP Note [510007](#).

The SSL key pair is stored in the \$(DIR_INSTANCE) / sec / SAPSSLS . pse directory of your Web Application Server. It can also be imported from the PKCS#12 certificate using program *sapgenpse*, which comes with SAPCryptolib.

Enter **sapgenpse import_p12 -h** for the online help documentation. The PSE file that is created can be imported to transaction STRUST as a file and saved as *SSL Server PSE*.

**NOTE**

For more information about customer-specific X.509 client certificates for SSL, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *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* ◀.

For more information about communication channel security, especially for the integration SAP Advanced Planning & Optimization (SAP APO) and ERP systems, see the SAP SCM Security Guide under ► *Communication Channel Security* ◀.

8.2 Network Security

Your network infrastructure is important in protecting your system. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. SAP offers general recommendations to protect your system landscape, based on SAP NetWeaver.

**NOTE**

For information about network security for SAP enhancement package 3 for SAP NetWeaver 7.0, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *Network and Communication Security* ◀.

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

**NOTE**

For information about access control using firewalls, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0*

EhP3 Security Guides (Online Version) → Network and Communication Security → Using Firewall Systems for Access Control .

8.3 Communication Destinations



CAUTION







If used carelessly, users and authorizations for connection destinations can cause major security flaws.

Follow these rules for connection users and authorizations:













- Choose user type *System*.
- Assign only the minimum required authorizations.
- Choose a secure and secret password.
- Store only connection user logon data for users of the *System* type.
- Choose *Trusted System* functionality whenever possible instead of storing connection user logon data.

The table below shows an overview of the communication destinations used by SAP Supply Network Collaboration (SAP SNC).

Connection Destinations

Destination	Delivered	Type	User, Authorizations	Description
► SAP SNC → SAP NetWeaver <LCRSAPRFC> 	No	RFC – TCP/IP		For more information, see the configuration documentation in SAP Solution Manager under ► <i>Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment</i>  and ► <i>Creating RFC Destinations in the ABAP and Java Environments</i>  and ► <i>Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine</i>  .
► SAP SNC → SAP NetWeaver <SAPSLDAP> 	No	RFC – TCP/IP		For more information, see the configuration documentation in SAP Solution Manager under ► <i>Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment</i>  and ► <i>Creating RFC</i>

8.3 Communication Destinations

Destination	Delivered	Type	User, Authorizations	Description
				<i>Destinations in the ABAP and Java Environments</i>  and <i>▮ Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine</i>  .
<i>▮ ERP system → SAP NetWeaver <LCRSAPRFC></i> 	No	RFC – TCP/IP		For more information, see the configuration documentation in SAP Solution Manager under <i>▮ Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment</i>  and <i>▮ Creating RFC Destinations in the ABAP and Java Environments</i>  and <i>▮ Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine → Set up Connection to Integration Server</i>  .
<i>▮ ERP system → SAP NetWeaver <SAPSLDAP></i> 	No	RFC – TCP/IP		For more information, see the configuration documentation in SAP Solution Manager under <i>▮ Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment</i>  and <i>▮ Creating RFC Destinations in the ABAP and Java Environments</i>  and <i>▮ Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine → Creating Connection to SLD.</i> 
<i>▮ SAP NetWeaver → SAP NetWeaver <LCRSAPRFC></i> 	No	RFC – TCP/IP		For more information, see the configuration documentation in SAP Solution Manager under <i>▮ Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP and Java Environments</i>  .

8.3 Communication Destinations

Destination	Delivered	Type	User, Authorizations	Description
► SAP NetWeaver → SAP NetWeaver <SAPSLDAP> ↩	No	RFC – TCP/IP		For more information, see the configuration documentation in SAP Solution Manager under ► Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP and Java Environments ↩.
► SAP NetWeaver Usage Type PI → SAP SNC ↩	No	RFC – HTTP Connections to ABAP System		For more information, see the configuration documentation in SAP Solution Manager under ► Solutions/ Applications → SAP SCM → Configuration Structures → SAP SCM 5.1 → Basic Settings for SAP Supply Network Collaboration → System Connections ↩.
► SAP SNC → SAP NetWeaver Usage Type PI ↩	No	RFC – HTTP Connections to ABAP System	User role: SAP_XI_APPL_SERV_USER	For more information, see the configuration documentation in SAP Solution Manager under ► Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment ↩ and ► Creating RFC Destinations in the ABAP and Java Environments ↩ and ► Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine ↩.
► ERP system → SAP NetWeaver Usage Type PI ↩	No	RFC – HTTP Connections to ABAP System		For more information, see the configuration documentation in SAP Solution Manager under ► Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment ↩ and ► Creating RFC Destinations in the ABAP and Java Environments ↩ and ► Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine ↩.
► SAP NetWeaver Usage Type PI → ERP system ↩	No	RFC – HTTP Connections		For more information, see the configuration documentation in SAP Solution Manager under ► Solutions/

8.3 Communication Destinations

Destination	Delivered	Type	User, Authorizations	Description
		to ABAP System		<p><i>Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment</i>  and <i>Creating RFC Destinations in the ABAP and Java Environments</i> </p> <p>and</p> <p><i>Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine</i> .</p>
<i>► SAP NetWeaver Usage Type PI → ERP system</i> 	No	RFC – ABAP Connections		For more information, see the configuration documentation in SAP Solution Manager under <i>► Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Integration of Business Systems → Integration Using the IDoc Adapter → Settings on Integration Server System</i>  .
<i>► ERP system → SAP NetWeaver Usage Type PI</i> 	No	RFC – ABAP Connections	User role: SAP_XI_APPL_SERV_USER	For more information, see the configuration documentation in SAP Solution Manager under <i>► Solutions/Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Integration of Business Systems → Integration Using the IDoc Adapter → Settings on IDoc Sending System</i>  .
<i>► ERP system → SAP SNC</i> 	No			You need to set up a RFC connection for master data integration using Core Interface.
<i>► SAP SNC → Collaboration Folders</i> 	No	RFC – ABAP Connections		We recommend you set up a RFC connection to the Collaboration Folders system. For more information, see <i>Authorizations</i> .
<i>► SAP SNC → SAP Event Management</i> 	No	RFC – ABAP Connections	Service user and password, RFC authorization	<p>You need to set up a RFC connection to SAP EM, if you are running the following visibility processes in SAP SNC:</p> <ul style="list-style-type: none"> ■ SNC Visibility Process for Inbound Message ■ SNC Visibility Process for Purchase Order ■ SNC Visibility Process for Replenishment Order
<i>► SAP Event Management → SAP SNC</i> 	No	RFC – ABAP Connections		You need to set up a RFC connection to SAP SNC, if you are running the following visibility processes in SAP SNC:

8.3 Communication Destinations

Destination	Delivered	Type	User, Authorizations	Description
				<ul style="list-style-type: none"> ■ SNC Visibility Process for Inbound Message ■ SNC Visibility Process for Purchase Order ■ SNC Visibility Process for Replenishment Order
► SAP SCM → SAP NetWeaver Usage Type PI ◀	No	RFC – HTTP Connections to ABAP System		<p>You need to set up this RFC connection to ensure the integration of XML services if you are using Planning and Collaboration as part of the Supplier Managed Inventory with Replenishment Orders business process and the Dynamic Replenishment business process.</p> <p>For more information, see the configuration documentation in SAP Solution Manager under ► <i>Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment</i> ◀ and ► <i>Creating RFC Destinations in the ABAP and Java Environments</i> ◀ and</p> <p>► <i>Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Configuration of Business Systems with Integration Engine</i> ◀.</p>
► SAP NetWeaver Usage Type PI → SAP SCM ◀	No	RFC – ABAP Connections		<p>You need to set up this RFC connection to ensure integration using the IDoc adapter if you are using Planning and Collaboration as part of the Supplier Managed Inventory with Replenishment Orders business process and the Dynamic Replenishment business process.</p> <p>For more information, see the configuration documentation in SAP Solution Manager under ► <i>Solutions/ Applications → Basic Configuration → Configuration Structures → SAP NetWeaver 2004s → Usage Type PI → Integration of Business Systems → Integration Using the IDoc Adapter → Settings on IDoc Sending System</i> ◀.</p>
► SAP NetWeaver Identity Management → SAP SNC ◀	No	RFC – ABAP Connections		<p>You need to set up a background RFC connection to SAP SNC from SAP NetWeaver Identity Management, if you are using the <i>Creation of users and business partners for employees use case</i> for the</p>

8.3 Communication Destinations

Destination	Delivered	Type	User, Authorizations	Description
				integration of SAP NetWeaver Identity Management with SAP SNC. For more information, see SAP Library for SAP Enhancement Package 2 for SAP Supply Network Collaboration 7.0 on SAP Help Portal at http://help.sap.com/snc702 . In SAP Library, choose ► <i>Processes and Tools for Enterprise Applications (CA-EPT)</i> → <i>User Management and Distribution with SAP NetWeaver Identity Management</i> → <i>Identity Management for SAP Supply Network Collaboration</i> ⏮.
► SAP SNC → SAP NetWeaver Identity Management ⏮	No	RFC - ABAP Connections		You need to set up a background RFC connection to SAP NetWeaver Identity Management from SAP SNC, if you are using the <i>Distribution of local users</i> use case for the integration of SAP NetWeaver Identity Management with SAP SNC. For more information, see SAP Library for SAP Enhancement Package 2 for SAP Supply Network Collaboration 7.0 on SAP Help Portal at http://help.sap.com/snc702 . In SAP Library, choose ► <i>Processes and Tools for Enterprise Applications (CA-EPT)</i> → <i>User Management and Distribution with SAP NetWeaver Identity Management</i> → <i>Identity Management for SAP Supply Network Collaboration</i> ⏮.

Central Activation Switch for Remote Communication**SAP SNC**

1. To designate at least one logical system name as SAP Event Management, in Customizing for *Integration with SAP Components*, choose ► *Event Management Interface* → *Define Application Interface* → *Define SAP EM* ⏮.
2. Enter the defined SAP Event Management name in Customizing entries under *Define Application Interface*.
3. To view the Customizing activities necessary to define the RFC connection and the logical system name, in Customizing for *Integration with SAP Components*, choose ► *Event Management Interface* → *Define System Configuration* ⏮.

SAP EM

To designate the logical system name for SAP SNC as an application system in Customizing, choose ► *Event Management* → *General Settings in SAP Event Management* → *Define Application System* ⏮.

This application system name can then be used in additional customizing settings.

8.4 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For SAP Supply Network Collaboration (SAP SNC) the following services are needed:

- default_host/sap/public/bc/icons
- default_host/sap/public/bc/icons_rtl
- default_host/sap/public/bc/webdynpro
- default_host/sap/public/myssocntl
- default_host/sap/public/bc/webicons
- default_host/sap/public/bc/pictogram
- default_host/sap/xi/engine
- default_host /sap/public/bc/UR
- default_host/sap/bc/webdynpro/scf/snc
- default_host/sap/bc/webdynpro/scf/snc_c
- default_host/sap/bc/webdynpro/scf/snc_s
- default_host/sap/bc/webdynpro/scf/snc_g
- default_host/sap/bc/webdynpro/scf/snc_rr
- default_host/sap/bc/webdynpro/scf/snc_returns_c
- default_host/sap/bc/webdynpro/scf/snc_returns_s
- default_host/sap/bc/webdynpro/scf/snc_returns_g
- default_host/sap/bc/webdynpro/scf/snc_rr/SPM_OVP

Use the transaction SICF to activate these services. If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly. Only activate services for SAP SNC if they are available in the value help of the *Service Path* field.

For information about RFC/ICF security, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *RFC/ICF Security Guide* ◀.

For information about activating and deactivating ICF services, see SAP Library at <https://help.sap.com/nw703>. In SAP Library, choose ► *SAP NetWeaver* → *SAP NetWeaver by Key Capability* → *Application Platform by Key Capability* → *Platform-Wide Services* → *Connectivity* → *Components of SAP Communication Technology* → *Communication Between ABAP and Non-ABAP Technologies* → *Internet Communication Framework* → *Internet Communication Framework* → *Server-Side Development* → *Creating and Configuring an ICF Service* → *Activating and Deactivating ICF Services* ◀.

9 Data Storage Security

SAP Supply Network Collaboration (SAP SNC) including enhancement package 2 is based on SAP NetWeaver 7.0 including enhancement package 3. The data storage security of SAP NetWeaver and the components that are installed on that base is described in detail in the *SAP NetWeaver 7.0 EhP3 Security Guide*.



NOTE

For more information about the data storage security of SAP NetWeaver, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *Security Guides for Operating System and Database Platforms* ◀.

The SAP SNC business data is stored in the system database.

**This page is left blank for documents
that are printed on both sides.**

10 Security for Additional Applications

Internet Graphics Service

SAP Supply Network Collaboration (SAP SNC) uses the Internet Graphics Service (IGS) to display graphics in the Web UI. For more information about IGS security, see SAP Help Portal at <http://help.sap.com/nw703>. In SAP Library, choose ► *SAP NetWeaver by Key Capability* → *Application Platform by Key Capability* → *ABAP Technology* → *UI Technologies in ABAP* → *SAP Graphics (BC-FES-GRA)* → *Internet Graphics Service* → *Internet Graphics Service Security* ◀.

Web Dynpro

SAP SNC uses Web Dynpro technology for Web UIs. For more information about Web Dynpro security issues, see SAP Service Marketplace at ► <http://service.sap.com/securityguide> → *SAP NetWeaver Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Aspects for Usage Type DI and Other Development Technologies* → *Security Issues in Web Dynpro for ABAP* ◀.

**This page is left blank for documents
that are printed on both sides.**

11 Enterprise Services Security

The following sections in the SAP NetWeaver Security Guide are relevant for all enterprise services delivered with SAP Supply Network Collaboration:

► <http://service.sap.com/securityguide> → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 EhP3 Security Guides (Online Version)* ◀

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

For more information about special security requirements for Web services, see the SAP NetWeaver Documentation on SAP Help Portal at <http://help.sap.com/nw703>. In SAP Library, choose ► *SAP NetWeaver Developer's Guide* → *Fundamentals* → *Using Java* → *Core Development Tasks* → *Providing and Consuming Web Services* → *Web Service Toolset* → *Web Services Security* ◀.

**This page is left blank for documents
that are printed on both sides.**

12 Other Security-Relevant Information

Security Settings for E-Mail Communication in File Transfer

You use the file transfer application to send outbound e-mails with files attached that contain data, which the user can process offline. After processing the data, the user can send an e-mail back to SAP SNC with the processed file attached. SAP SNC receives and processes the e-mail and the attached file. By making the following security settings, you ensure secure e-mail communication for the file transfer:

- SAP SNC uses the security checks of the mail servers that are connected to the SAP Web Application Server. For this, SAP SNC uses the standard BCS interface. The SAP Web Application Server communicates directly with a mail server using SMTP protocol. The SAP system can receive inbound mails from any number of mail servers. You can reach each client using separate, configurable port numbers. For more information, see SAP Note [455140](#).



NOTE

Ensure that the mail server that is connected to SAP Web Application Server is secure.

If you want to use secure e-mails (encryption and digital signatures), see SAP Note [149926](#).

- To ensure that SAP SNC only accepts e-mails from known business partners, you can determine the e-mail address patterns that file transfer accepts. If the sender is known, the system accepts the file upload request. If the sender is not known, the system writes an entry into the log and rejects the file upload request. In the standard system, file uploads by e-mail are not possible. To make file uploads by e-mail possible, you must make the necessary settings in Customizing. You make these settings in Customizing for *Supply Network Collaboration* under ► *Tools* → *File Transfer* → *Determine Accepted E-Mail Addresses for File Upload* ⚡.

Virus Check of Document Attachments

SAP Supply Network Collaboration (SAP SNC) provides functionality to check documents using a virus scanner before they are uploaded to SAP SNC. Ensure that you have a virus scanner correctly installed and configured.

For more information, in Customizing for *SAP NetWeaver*, choose the activities under ► *Application Server* → *System Administration* → *Virus Scan Interface* ⚡.

SAP SNC-Specific Virus Scan Profiles

SAP delivers virus scan profiles specifically for certain functions of SAP SNC:

- For the file transfer application, the *FTR Virus Scan Profile* (*/SCA/DM_FTR/UPLOAD_FILE*) virus scan profile is available to protect the system from viruses when uploading files by e-mail or by means of the *Upload Center* Web screen. If you activate the profile, file transfer records any events in the

application log. If an error occurs during processing, the upload is terminated. For more information, see SAP Notes [817623](#) and [639486](#).

- For the microblog building block in the quick view, the *Profile for Scanning Attachment Uploads to Quick View Microblog in SCM SNC (/SCA/DM_MYS/UPLOAD_FILE)* virus scan profile is available.

The SAP Supply Network Collaboration (SAP SNC) microblog allows customer users and supplier users to communicate with each other by posting short messages on the quick view. When you create a microblog message, you can attach a file to it. By implementing this virus scan profile, you prevent users from uploading virus-infected attachments to the microblog.

- For the Work Order component, the *Profile for Scanning Attachment Uploads to Work Orders in SCM SNC (/SCA/DM_MFGC/UPLOAD_FILE)* virus scan profile is available.

In *Work Order Details*, both customers and suppliers can upload documents as a way of distributing instructions. By implementing this virus scan profile, you prevent users from uploading virus-infected attachments to the Work Order component.

Validation of SOAP Message Header in Inbound XML Messages

When SAP SNC receives an inbound XML message, the system validates the sender party and receiver party by means of the payload message header of the XML message. However, there is no validation check of the sender and receiver information in the SOAP message header when the XML message is passed from the SAP enhancement package 1 for SAP NetWeaver Process Integration 7.0 to SAP SNC. With this lack of validation, the SOAP message header might contain different sender and receiver information as the content of the authenticated payload message header. The lack of validation could induce a security breach. To avoid this security breach, you can activate the SAP SNC Business Add-In (BAI) *Validation of the Message Header (Inbound)/SCA/BIF_MI_MSGHDR* to retrieve the sender and receiver business content from the SOAP message header. For more information, see *Customizing for Supply Network Collaboration* under ► *Business Add-Ins (BAIs) for SAP SNC* → *Basic Settings* → *Processing Inbound and Outbound Messages* → *BAI: Validation of the Message Header (Inbound)* ◀.

13 Trace and Log Files

SAP systems maintain logs for the following reasons:

- System administration
- Monitoring
- Problem solving
- Auditing

Audits and logs are important because they monitor your system's security and track events.

For more information about auditing and logging, see SAP Help Portal at <http://help.sap.com/nw703>. In SAP Library, choose ► *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide* → *Security Aspects for System Management* → *Auditing and Logging* ↩.

For more information about auditing and logging for SAP Supply Network Collaboration, see SAP Help Portal at <http://help.sap.com/snc702>. In SAP Library, choose ► *Cross-Application Functions* → *Audit Trail* ↩.

For more information about auditing and logging in SAP Supply Chain Management, see also the *SAP SCM Component Security Guide*.

**This page is left blank for documents
that are printed on both sides.**

14 Services for Security Lifecycle Management

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

Security Chapter in the EarlyWatch Alert (EWA) Report

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

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

Security Optimization Service (SOS)

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

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

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

Security Configuration Validation

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

Security in the RunSAP Methodology / Secure Operations Standard

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

More Information

For more details on these services see:

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

A Reference

A.1 The Main SAP Documentation Types

The following is an overview of the **most important** documentation types that you need in the various phases in the life cycle of SAP software.



Figure 3: Documentation Types in the Software Life Cycle

Cross-Phase Documentation

SAPterm is SAP's terminology database. It contains SAP-specific vocabulary in over 30 languages, as well as many glossary entries in English and German.

- Target group:
 - Relevant for all target groups
- Current version:
 - On SAP Help Portal at ► <http://help.sap.com> → *Additional Information* → *Glossary* ◀ (direct access) or *Terminology* (as terminology CD)
 - In the SAP system in transaction **STERM**

SAP Library is a collection of documentation for SAP software covering functions and processes.

- Target group:
 - Consultants
 - System administrators
 - Project teams for implementations or upgrades
- Current version:
 - On SAP Help Portal at <http://help.sap.com> (also available as documentation DVD)

The **security guide** describes the settings for a medium security level and offers suggestions for raising security levels. A collective security guide is available for SAP NetWeaver. This document contains general guidelines and suggestions. SAP applications have a security guide of their own.

- Target group:
 - System administrators
 - Technology consultants
 - Solution consultants
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/securityguide>

Implementation

The **master guide** is the starting point for implementing an SAP solution. It lists the required installable units for each business or IT scenario. It provides scenario-specific descriptions of preparation, execution, and follow-up of an implementation. It also provides references to other documents, such as installation guides, the technical infrastructure guide and SAP Notes.

- Target group:
 - Technology consultants
 - Project teams for implementations
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/instguides>

The **installation guide** describes the technical implementation of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
 - Technology consultants
 - Project teams for implementations
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/instguides>

Configuration Documentation in SAP Solution Manager—SAP Solution Manager is a life-cycle platform. One of its main functions is the configuration of business and IT scenarios. It contains IMG activities, transactions, and so on, as well as documentation.

- Target group:
 - Technology consultants
 - Solution consultants
 - Project teams for implementations
- Current version:
 - In SAP Solution Manager

The **Implementation Guide (IMG)** is a tool for configuring a single SAP system. The IMG activities and their documentation are structured from a functional perspective. (In order to configure a whole system landscape from a process-oriented perspective, SAP Solution Manager, which refers to the relevant IMG activities in the individual SAP systems, is used.)

- Target group:
 - Solution consultants
 - Project teams for implementations or upgrades
- Current version:
 - In the SAP menu of the SAP system under ► *Tools* → *Customizing* → *IMG* ◀

Production Operation

The **technical operations manual** is the starting point for operating a system that runs on SAP NetWeaver, and precedes the solution operations guide. The manual refers users to the tools and documentation that are needed to carry out various tasks, such as monitoring, backup/restore, master data maintenance, transports, and tests.

- Target group:
 - System administrators
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/instguides>

The **solution operations guide** is used for operating an SAP application once all tasks in the technical operations manual have been completed. It refers users to the tools and documentation that are needed to carry out the various operations-related tasks.

- Target group:
 - System administrators
 - Technology consultants
 - Solution consultants
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/instguides>

Upgrade

The **upgrade master guide** is the starting point for upgrading the business and IT scenarios of an SAP solution. It provides scenario-specific descriptions of preparation, execution, and follow-up of an upgrade. It also refers to other documents, such as the upgrade guides and SAP Notes.

- Target group:
 - Technology consultants
 - Project teams for upgrades
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/instguides>

The **upgrade guide** describes the technical upgrade of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
 - Technology consultants
 - Project teams for upgrades
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/instguides>

Release notes are documents that contain short descriptions of new features or changes in SAP NetWeaver or an SAP application since the previous release. Release notes about ABAP developments enable the SAP system to generate delta and upgrade IMGs.

- Target group:
 - Consultants
 - Project teams for upgrades
- Current version:
 - On SAP Service Marketplace at <http://service.sap.com/releasenotes>
 - In the SAP menu of the SAP system under ► *Help* → *Release Notes* ◀ (only ABAP developments)

Documentation in the SAP Service Marketplace

You can find this document at the following address: <http://service.sap.com/securityguide>

SAP AG

Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 34
F +49/18 05/34 34 20
www.sap.com