SAP Enhancement Package 4 for SAP® Supply Network Collaboration (SAP SNC) 7.0
Using SAP NetWeaver® 7.5
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

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 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.

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

**Table 1**

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; &gt;</td>
<td>Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your <em>User Name</em>”.</td>
</tr>
<tr>
<td>⦁ ⦀ ⦀</td>
<td>Arrows separating the parts of a navigation path, for example, menu options</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Words or characters that you enter in the system exactly as they appear in the documentation</td>
</tr>
<tr>
<td><strong>Example</strong> ➤</td>
<td>Textual cross-references to an internet address, for example, <a href="http://www.sap.com">www.sap.com</a></td>
</tr>
<tr>
<td>/example</td>
<td>Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web</td>
</tr>
<tr>
<td>123456 ➤</td>
<td>Hyperlink to an SAP Note, for example, SAP Note 123456 ➤</td>
</tr>
</tbody>
</table>
| **Example** | • 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** | • 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: service.sap.com/securityguide.

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2016-01-27</td>
<td>First version</td>
</tr>
</tbody>
</table>
# Content

1. **Introduction** ................................................................. 7
2. **Before You Start** ............................................................ 9
3. **Information About the Technical System Landscape** ..................... 14
4. **Security Aspects of Data, Data Flow, and Processes** ....................... 15
5. **User Administration and Authentication** .................................. 17
   5.1 User Management .......................................................... 17
   5.2 User Data Synchronization ............................................... 20
   5.3 Integration Into Single Sign-On Environments ........................ 20
6. **Authorizations** .................................................................. 22
   6.1 Maintaining Authorizations for SAP Supply Network Collaboration ........ 28
   6.2 Maintaining Authorizations for Integration with SAP Components .... 29
7. **Session Security Protection** ............................................... 30
8. **Network and Communication Security** .................................... 31
   8.1 Communication Channel Security ...................................... 31
   8.2 Network Security ........................................................... 33
   8.3 Communication Destinations ............................................ 33
   8.4 Internet Communication Framework Security .......................... 40
9. **Data Storage Security** ..................................................... 42
10. **Security for Additional Applications** ...................................... 43
11. **Enterprise Services Security** ............................................... 44
12. **Other Security-Relevant Information** ...................................... 45
13. **Trace and Log Files** .......................................................... 47
14. **Services for Security Lifecycle Management** .............................. 48
A. **Reference** ......................................................................... 50
   A.1 The Main SAP Documentation Types .................................... 50
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 Business Warehouse
- SAP ERP 6.0 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.

Table 3: Fundamental Security Guides

<table>
<thead>
<tr>
<th>Security Guide</th>
<th>Full path to the Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA Security Guide</td>
<td>help.sap.com/hana_platform Security</td>
</tr>
<tr>
<td>SAP SCM Component Security Guide</td>
<td>service.sap.com/securityguide</td>
</tr>
</tbody>
</table>

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 service.sap.com/instguides.

Related Security Guides and Documentation
The following table provides an overview of all related Security Guides and important documentation for SAP SNC.

Table 4

<table>
<thead>
<tr>
<th>Guide/Documentation</th>
<th>Full Path to Guide/Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Advanced Planning and Optimization Security Guide</td>
<td>help.sap.com/apo/security</td>
</tr>
<tr>
<td>Master Guide for SAP SCM</td>
<td>service.sap.com/instguides</td>
</tr>
<tr>
<td>SAP SCM documentation</td>
<td>help.sap.com/scmserver</td>
</tr>
<tr>
<td>SAP SCM Installation Guide</td>
<td>service.sap.com/instguides</td>
</tr>
<tr>
<td>Master Guide for SAP Enhancement Package 4 for SAP SNC 7.0</td>
<td>service.sap.com/instguides</td>
</tr>
<tr>
<td>SAP SNC documentation</td>
<td>help.sap.com/snc704</td>
</tr>
<tr>
<td>SAP Portfolio and Project Management Security Guide</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>SAP SNC Business Scenarios: Configuration Documentation</td>
<td>help.sap.com/instguides</td>
</tr>
<tr>
<td>SAP NetWeaver Identity Management Security Guide</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>SAP NetWeaver Installation Guide</td>
<td>service.sap.com/instguides</td>
</tr>
<tr>
<td>SAP NetWeaver Process Integration (PI): Configuration</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>SAP NetWeaver Gateway Security Guide</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>SAP NetWeaver documentation</td>
<td>help.sap.com/netweaver</td>
</tr>
<tr>
<td>BI Content documentation</td>
<td>help.sap.com/bicontent</td>
</tr>
</tbody>
</table>

Important SAP Notes
The most important SAP Notes that apply to the security of SAP SNC are shown in the following table.
<table>
<thead>
<tr>
<th>Title</th>
<th>SAP Note Number</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collective Security Note</td>
<td>1394093</td>
<td>This note cover release-independent information concerning security-related issues for SAP systems.</td>
</tr>
<tr>
<td>Security Guide: SAP Supply Chain Management</td>
<td>700659</td>
<td>The note covers all problems discovered after the publication of the security guide and contains additional information about security issues.</td>
</tr>
<tr>
<td>Trusting/Trusted Systems</td>
<td>128447</td>
<td>Discusses the issues relevant to setting up a trusted/trusting system relationship between two SAP systems.</td>
</tr>
<tr>
<td>Release strategy for the ABAP add-on SAP SNC</td>
<td>2242851</td>
<td>Information about planning the installation and upgrades of the ABAP add-on SAP SNC (as of release EHP4 for SAP SNC 7.0).</td>
</tr>
<tr>
<td>Adobe Acrobat Reader Creates Temporary Files</td>
<td>853497</td>
<td>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.</td>
</tr>
<tr>
<td>Business Partners in SAP SNC</td>
<td>1122502</td>
<td>The note enhances the Display Partner, User, Location Assignments transaction (/SCA/USRPRTPLOC). With the enhanced transaction, you can display all users without business partner assignment (see also User Management [page 17]).</td>
</tr>
<tr>
<td>Consulting Note – How to switch off authorization check in selection modes</td>
<td>1113695</td>
<td>Provides instructions on how to switch off authorization checks in selection mode configuration.</td>
</tr>
<tr>
<td>Configuration of e-mail, fax, paging, or SMS using SMTP</td>
<td>455140</td>
<td>Provides instructions on how to configure e-mail, fax, paging, or SMS in the SAP NetWeaver Application Server using SMTP. It also explains, which prerequisites and settings are required outside the SAP system.</td>
</tr>
<tr>
<td>Title</td>
<td>SAP Note Number</td>
<td>Comment</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure e-mail: Encryption, digital signature</td>
<td>149926</td>
<td>Provides instructions on how to encrypt or assign a digital signature to an e-mail when you send them from SAP systems.</td>
</tr>
<tr>
<td>Integrating a virus scan into SAP applications</td>
<td>817623</td>
<td>Provides instructions on how to integrate a virus scan.</td>
</tr>
<tr>
<td>Virus scan profile update</td>
<td>1695265</td>
<td>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.</td>
</tr>
<tr>
<td>Antivirus protection within SAP applications</td>
<td>639486</td>
<td>Provides information about antivirus protection.</td>
</tr>
<tr>
<td>Data protection and security in SAP Systems</td>
<td>30724</td>
<td>Questions on the topic of data protection in SAP systems and in R/3 in particular.</td>
</tr>
<tr>
<td>Super user feature in SNC</td>
<td>1430757</td>
<td>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 is not supported by default anymore.</td>
</tr>
<tr>
<td>Setting up SSL on Web Application Server ABAP</td>
<td>510007</td>
<td>Provides a brief description of the steps required to set up SSL on the Web Application Server ABAP.</td>
</tr>
<tr>
<td>New start authorization check for Web Dynpro ABAP</td>
<td>1413011</td>
<td>Provides details about the new start authorization check for Web Dynpro ABAP applications. This note is relevant for the business-process roles we deliver.</td>
</tr>
<tr>
<td>HTML5 applications using Web Services via Gateway as a hub</td>
<td>1760422</td>
<td>Recommendations about how to use SAP NetWeaver Gateway as dedicated hub in your landscape.</td>
</tr>
</tbody>
</table>

### Additional Information

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

**Table 6: Quick Links to Additional Information**

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on the SAP Service Marketplace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>service.sap.com/security</td>
</tr>
<tr>
<td>Content</td>
<td>Quick Link on the SAP Service Marketplace</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Security Guides</td>
<td>service.sap.com/securityguides</td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td>service.sap.com/notes</td>
</tr>
<tr>
<td>Released Platforms</td>
<td>apps.support.sap.com/sap/support/pam</td>
</tr>
<tr>
<td></td>
<td>service.sap.com/platforms</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td>support.sap.com/solutionmanager</td>
</tr>
</tbody>
</table>

3 Information About the Technical System Landscape

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

Table 7: More Information About the Technical System Landscape

<table>
<thead>
<tr>
<th>Topic</th>
<th>Guide/Tool</th>
<th>Quick Link to the SAP Service Marketplace or SDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical system landscape and installation procedure for SAP Supply Chain Management (SAP SCM) and SAP ERP</td>
<td>SAP SCM Installation Guide SAP ERP Installation Guide</td>
<td>service.sap.com/instguides</td>
</tr>
<tr>
<td>Installation of SAP SNC</td>
<td>SAP Note 2242851</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td>service.sap.com/security</td>
</tr>
</tbody>
</table>

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


For more information about the system landscape, see the SAP SNC Master Guide on SAP Service Marketplace at service.sap.com/instguides.

CUSTOMER
© Copyright 2016 SAP SE or an SAP affiliate company.
All rights reserved.

SAP Enhancement Package 4 for SAP® Supply Network Collaboration (SAP SNC) 7.0

Information About the Technical System Landscape
4 Security Aspects of Data, Data Flow, and Processes

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

Table 8

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate Download</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Save Download to KPro</td>
<td>Not available</td>
</tr>
<tr>
<td>3</td>
<td>Initiate Delivery of Mail with Attachment</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Deliver Mail</td>
<td>Not available</td>
</tr>
</tbody>
</table>

Data Flow of File Upload from an Inbound E-Mail

Figure 2: Data Flow for File Upload

Table 9

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Send Mail (via SMTP)</td>
<td>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.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Security Measure</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>2</td>
<td>Deliver Mail to SAP System</td>
<td>Not available</td>
</tr>
<tr>
<td>3</td>
<td>Mail Inbound Processing</td>
<td>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 Supply Network Collaboration under Tools &gt; File Transfer &gt; Determine Accepted E-Mail Addresses for File Upload.</td>
</tr>
<tr>
<td>4</td>
<td>Run Virus Check</td>
<td>You must check the uploaded file for viruses. The virus scanner can be located on another system, therefore consider that master data or transactional data can pass through an unsecured network.</td>
</tr>
<tr>
<td>5</td>
<td>Save Upload in KPro</td>
<td>Not available</td>
</tr>
<tr>
<td>6</td>
<td>Schedule Job for Upload</td>
<td>Not available</td>
</tr>
<tr>
<td>7</td>
<td>Scheduled Job Updates Data in Database</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 17]
  
  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 20]
  
  This topic describes how the user data is synchronized with other sources.

- **Integration Into Single Sign-On Environments** [page 20]
  
  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 following sections. In addition, we provide a list of the standard users required for operating SAP SNC.

User Administration Tools

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

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management for the ABAP Engine (transaction SU01)</td>
<td>Use the user management transaction SU01 to maintain users in ABAP-based systems.</td>
</tr>
<tr>
<td>User Administration on the SAP SNC web user interface using the User Administration web screen</td>
<td>Use the User Administration web screen to maintain users for the leading business partner in a supplier collaboration, as well as for its business partners.</td>
</tr>
<tr>
<td>User Administration in the SAP NetWeaver Identity Management system</td>
<td>Use Identity Management to maintain users centrally in a dedicated SAP NetWeaver Identity Management system. For more information, see Documentation Center – SAP NetWeaver Identity Management 7.1 or 7.2 at service.sap.com/instguides.</td>
</tr>
</tbody>
</table>

SAP Enhancement Package 4 for SAP® Supply Network Collaboration (SAP SNC) 7.0

User Administration and Authentication

CUSTOMER

© Copyright 2016 SAP SE or an SAP affiliate company. All rights reserved.
### User Administration and Authentication

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Generator (transaction PFCG)</td>
<td>Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.</td>
</tr>
<tr>
<td>Central User Administration (CUA)</td>
<td>Use the CUA to maintain users centrally for multiple ABAP-based systems. Synchronization with a directory server is also supported.</td>
</tr>
<tr>
<td>User Management Engine (UME) administration console</td>
<td>Use the web-based UME administration console to maintain users, roles, and authorizations in Java.</td>
</tr>
<tr>
<td>SAP J2EE Engine user management using the Visual Administrator</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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.


### Standard Users

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

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver</td>
<td>Communication users for the connection between SAP SNC and SAP NetWeaver</td>
<td>No</td>
<td>Dialog User</td>
<td>To be entered</td>
<td>For more information, see the SAP NetWeaver Installation Guide under <a href="http://help.sap.com/nw75">Ensuring User Security</a>.</td>
</tr>
<tr>
<td>SAP SNC</td>
<td>Business partner users</td>
<td>No</td>
<td>Dialog User</td>
<td>To be entered</td>
<td>For more information, see the references below.</td>
</tr>
</tbody>
</table>

### 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 that you assign them to business partners. In addition, when you synchronize users in SAP SNC and in other SAP NetWeaver based systems, also make sure that 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/USRPRTLLOC) 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
  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

- SAP NetWeaver Password Rules
  For more information, see the Application Help for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75. In Application Help, choose Function-Oriented View » Security » Identity Management » User and Role Administration of Application Server ABAP » Configuration of User and Role Administration » First Installation Procedure » Logon and Password Security in SAP NetWeaver Application Server ABAP » Password Rules.

- User Management in SAP NetWeaver Gateway
If you use the simplified UI for purchase order collaboration, then, in addition to the user management in SAP SNC, you must take care of the user management in SAP NetWeaver Gateway as well, depending on the deployment option of SAP NetWeaver Gateway (central hub deployment or embedded deployment).

SAP NetWeaver Gateway utilizes the user and role administration functions of SAP NetWeaver Application Server ABAP. For more information about user management in SAP NetWeaver Gateway, see the User Management chapter in the Security Guide for SAP NetWeaver Gateway and the User, Developer and Administrator Authorizations chapter in the Configuration Guide for SAP NetWeaver Gateway on SAP Help Portal at help.sap.com/nwgateway.

5.2 User Data Synchronization

By using user data synchronization in your system landscape, you can avoid administration effort. SAP enhancement package 4 for SAP Supply Network Collaboration (SAP SNC) 7.0 is based on SAP NetWeaver 7.5. For more information about user data synchronization, see the Security Guide for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75 under Security Information. In the Security Guide, choose User Administration and Authentication > User Management > Identity Management > Identity Management for System Landscapes > Integration of User Management in Your System Landscape.

Integration of SAP SNC with SAP NetWeaver Identity Management


Integration of SAP SNC with SAP NetWeaver Gateway

The simplified UI for purchase order collaboration uses SAP NetWeaver Gateway for RESTful communication with SAP SNC. Users must have the same user name in SAP NetWeaver Gateway as they do in the SAP SNC system. You can use the Central User Administration (CUA) or your existing identity management system to ensure user names match in both systems.

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

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.
  

- **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.
  

- **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.
  
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.

For more information about how to create roles, see the Application Help for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75. In Application Help, choose Function-Oriented View > Security > Identity Management > User and Role Administration of Application Server ABAP > Administration of Roles and Users.

## Standard Roles

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_SCM_ICH_DISPLAY</td>
<td>SAP SNC: Display User</td>
</tr>
<tr>
<td>SAP_SMI_SUPERUSER</td>
<td>SAP SNC: Superuser</td>
</tr>
<tr>
<td>SAP_SMI_MD</td>
<td>SAP SNC: Master Data Maintenance</td>
</tr>
<tr>
<td>SAP_SMI_EXT_MD_SUPERUSER</td>
<td>SAP SNC: Master Data Superuser</td>
</tr>
<tr>
<td>SAP_SMI_SELASSN</td>
<td>SAP SNC: Selection Assignments</td>
</tr>
<tr>
<td>SAP_SMI_SELECTIONS</td>
<td>SAP SNC: Selection Maintenance</td>
</tr>
<tr>
<td>SAP_SCM_ICH_ALRT_TYP</td>
<td>SAP SNC: Alert Display</td>
</tr>
<tr>
<td>SAP_SCM_ICH_AMON</td>
<td>SAP SNC: Alert Monitor Maintenance</td>
</tr>
<tr>
<td>SAP_SMI_ASNDIPLAY</td>
<td>Supplier Collaboration: ASN Display</td>
</tr>
<tr>
<td>SAP_SMI_ASNSUPERUSER</td>
<td>Supplier Collaboration: ASN Superuser</td>
</tr>
<tr>
<td>SAP_LIME_USER_2</td>
<td>General Basis Authorizations</td>
</tr>
<tr>
<td>SAP_SCM_ICH_IV_SUP_2</td>
<td>Invoice Maintenance (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICHASN_SUP_2</td>
<td>ASN Maintenance (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICHRK_SUP_2</td>
<td>Release and Kanban Processing (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICHDR_SUP_2</td>
<td>Dynamic Replenishment (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICHFCS_CUS_2</td>
<td>Forecast Collaboration (Customer)</td>
</tr>
</tbody>
</table>
### Table 13: Standard Business-Process Roles as of SAP SNC 7.04

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_SCM_ICH_FCS_SUP_2</td>
<td>Forecast Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_OMO_CUS_2</td>
<td>Outsourced Manufacturing: Order Processing (Customer)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_OMO_SUP_2</td>
<td>Outsourced Manufacturing: Order Processing (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_OMP_CUS_2</td>
<td>Outsourced Manufacturing: Planning (Customer)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_PO_SUP_2</td>
<td>Purchase Order Processing (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_QN_SUP_2</td>
<td>Quality Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_RP_SUP_2</td>
<td>Replenishment Processing (Supplier)</td>
</tr>
<tr>
<td>SAP_IICH_PlANNER_2</td>
<td>Responsive Replenishment: Planner (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_SU_CUS_2</td>
<td>Supplier Collaboration: Superuser (Customer)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_SU_SUP_2</td>
<td>Supplier Collaboration: Superuser and Administrator (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_ADM_CUS_2</td>
<td>Supplier Collaboration: Administrator (Customer)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_DPA_SUP</td>
<td>Supplier Performance Management (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_DPA_CUS</td>
<td>Supplier Performance Management (Customer)</td>
</tr>
</tbody>
</table>

### 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 [help.sap.com/snc702](http://help.sap.com/snc702). In SAP Library, choose [SAP Supply Network Collaboration (SAP SNC) > Cross-Application Functions > Partner and User Management > Roles for SAP Supply Network Collaboration (SAP SNC)](http://help.sap.com/snc) and SAP Note 1413011.

### Table 14: Obsolete Standard Roles as of SAP SNC 7.02

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_LIME_USER</td>
<td>General Basis Authorizations</td>
</tr>
<tr>
<td>SAP_SCM_ICH_IV_SUP</td>
<td>Invoice Maintenance (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_ASN_SUP</td>
<td>ASN Maintenance (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_RK_SUP</td>
<td>Release and Kanban Processing (Supplier)</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>SAP_SCM_ICH_DR_SUP</td>
<td>Dynamic Replenishment (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_FCS_CUS</td>
<td>Forecast Collaboration (Customer)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_FCS_SUP</td>
<td>Forecast Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_QM_CUS</td>
<td>Forecast Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_QM_SUP</td>
<td>Forecast Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_OPO_CUS</td>
<td>Forecast Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_OPO_SUP</td>
<td>Forecast Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_POR_SUP</td>
<td>Forecast Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_QN_SUP</td>
<td>Quality Collaboration (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_RP_SUP</td>
<td>Replenishment Processing (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_PAS_SUP</td>
<td>Responsive Replenishment: Planner (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_SU_CUS</td>
<td>Supplier Collaboration: Superuser (Customer)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_SU_SUP</td>
<td>Supplier Collaboration: Superuser and Administrator (Supplier)</td>
</tr>
<tr>
<td>SAP_SCM_ICH_ADM_CUS</td>
<td>Supplier Collaboration: Administrator (Customer)</td>
</tr>
</tbody>
</table>

**Roles for SAP SNC**

With SAP SNC, SAP delivers 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 assigning roles for the Supplier Managed Inventory and Release Processing business scenarios, see the configuration documentation in SAP Solution Manager under Solutions/Applications > Basic Configuration > Configuration Structures > Supplier Managed Inventory or Release Processing > Configuration > SAP SCM > Configuration Structures > SCM 7.0: Basic Settings - Supplier Managed Inv. & Release Pr. > Business Customizing in SAP SNC > Users and Authorizations.

**Roles for SAP NetWeaver Process Integration (PI)**

In SAP NetWeaver, there are 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 SAP NetWeaver Process Integration (PI), see the configuration documentation in SAP Solution Manager under Solutions/Applications > Basic Configuration > Configuration Structures > SAP NetWeaver 7.5 > Process Integration > Configuring Process Integration (PI) Dual Stack > 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 an RFC destination for the connection between cFolders and SAP SNC.

For RFC communication between cFolders and SAP SNC, you must 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 that 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:

<table>
<thead>
<tr>
<th>User</th>
<th>System</th>
<th>Role</th>
<th>Authorization Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNCUSER1</td>
<td>cFolders</td>
<td>CFX_USER</td>
<td>Not relevant</td>
</tr>
<tr>
<td>SNCUSER1</td>
<td>SAP SNC</td>
<td>Not relevant</td>
<td>C_SNC_CF</td>
</tr>
<tr>
<td>CFOLDERUSER</td>
<td>cFolders</td>
<td>SAP_CFX_ADMINISTRATOR and SAP_CFX_USER</td>
<td>Not relevant</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFX_OBJ</td>
<td>CFX_OBJ</td>
<td>COL</td>
<td>Authorization for collaborations in the collaborative scenario</td>
</tr>
<tr>
<td>CFX_OBJ</td>
<td>ACTVT</td>
<td>01</td>
<td>Adding or creating objects</td>
</tr>
<tr>
<td>CFX_USER</td>
<td>USER_TYPE</td>
<td>USER</td>
<td>The user needs this field value to use cFolders.</td>
</tr>
<tr>
<td>ACO_SUPER</td>
<td></td>
<td></td>
<td>The authorization for reading, writing, or managing specified object types. Possible values for cFolders are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>area</strong>: Authorization for all existing collaborations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>stat_prof</strong>: Authorization for all status profiles</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>usrgrp</strong>: Authorization for all user groups</td>
</tr>
</tbody>
</table>

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 follows:

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>ACTVT</td>
<td>16</td>
<td>Execute</td>
</tr>
<tr>
<td>S_RFC</td>
<td>RFC_NAME</td>
<td>From CFX_ACO to CFX_ACO*</td>
<td></td>
</tr>
</tbody>
</table>
### Authorization Objects

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>From <strong>CFX_API</strong> to <strong>CFX_API</strong>*</td>
<td>Type of RFC object to be protected: function group</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CFX_MA_UI</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CFX_UI_API</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CFX_UI_BADI</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CPR0_API</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RFC1</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>SDIFRUNTIME</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>SYST</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>SYSU</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>UWLCONN</strong></td>
<td></td>
</tr>
<tr>
<td><strong>S_RFC</strong></td>
<td>RFC_TYPE</td>
<td><strong>FUGR</strong></td>
<td></td>
</tr>
<tr>
<td><strong>S_RFCACL</strong></td>
<td>RFC_SYSID</td>
<td>System ID of cFolders system</td>
<td></td>
</tr>
<tr>
<td><strong>S_RFCACL</strong></td>
<td>RFC_CLIENT</td>
<td>Client of cFolders system</td>
<td></td>
</tr>
<tr>
<td><strong>S_RFCACL</strong></td>
<td>RFC_EQUSER</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td><strong>S_RFCACL</strong></td>
<td>RFC_TCODE</td>
<td>se37</td>
<td></td>
</tr>
<tr>
<td><strong>S_RFCACL</strong></td>
<td>ACTVT</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

### 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 must 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:

### Table I8: Standard Authorization Objects for Batch Jobs in File Transfer

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_BTCH_NAM</td>
<td>BTCUNAME</td>
<td>*</td>
</tr>
</tbody>
</table>

**Note**

By listing users maintained in transaction SU01 or user administration for SAP SNC here, you ensure...
Authorization Object | Field | Value
--- | --- | ---
 |  | that the user assigned to the SAPconnect service can only run batch jobs for those users.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_BTCH_JOB</td>
<td>JOBACTION</td>
<td>RELE</td>
</tr>
<tr>
<td>S_BTCH_JOB</td>
<td>JOBGROUP</td>
<td>*</td>
</tr>
<tr>
<td>S_BTCH_ADM</td>
<td>BTCADMIN</td>
<td>Y</td>
</tr>
</tbody>
</table>

**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 (SO50). 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:

<table>
<thead>
<tr>
<th>Table 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Object</td>
</tr>
<tr>
<td>S_RFC</td>
</tr>
<tr>
<td>S_RFC</td>
</tr>
<tr>
<td>S_RFC</td>
</tr>
</tbody>
</table>

**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 help.sap.com/snc704. In SAP Library, choose » SAP Supply Network Collaboration (SAP SNC) » 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 help.sap.com/snc704. In SAP Library, choose » SAP Supply Network Collaboration (SAP SNC) » 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 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 Warehouse (SAP NetWeaver BW). Data that is stored in the extraction structure of this DataSource cannot be transferred to SAP NetWeaver BW.

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.
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 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 cookies, we recommend activating secure session management. We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on SAP NetWeaver AS ABAP

In case you use the simplified UI for purchase order collaboration you must activate session security on SAP NetWeaver AS ABAP. To do this, set the corresponding profile parameters, and activate the session security for the clients using the transaction SICF_SESSIONS.

We recommend activating extra protection of security-related cookies. The HttpOnly flag instructs the browser to deny access to the cookie through client side script. As a result, even if a cross-site scripting (XSS) flaw exists, and a user accidentally accesses a link that exploits this flaw, the browser will not reveal the cookie to a third party. The Secure flag tells the browser to send the cookie only if the request is being sent over a secure channel such as HTTPS. This helps protect the cookie from being passed over unencrypted requests.

These additional flags are configured through the following AS ABAP profile parameters:

<table>
<thead>
<tr>
<th>Table 20</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile Parameter</strong></td>
</tr>
<tr>
<td>icf/set_HTTPonly_flag</td>
</tr>
<tr>
<td>login/ticket_only_by_https</td>
</tr>
</tbody>
</table>
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 31]
  This topic describes the communication paths and protocols used by SAP SNC.

- **Network Security** [page 33]
  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 33]
  This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the Security Guide for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75 under Security Information:

- **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.

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front-end client using a Web browser to application server</td>
<td>HTTPS</td>
<td>Application data</td>
<td>Passwords</td>
</tr>
<tr>
<td>Application server to application server</td>
<td>RFC</td>
<td>Application data</td>
<td>Passwords</td>
</tr>
<tr>
<td>Communication Path</td>
<td>Protocol Used</td>
<td>Type of Data Transferred</td>
<td>Data Requiring Special Protection</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>SAP NetWeaver Gateway to SAP SNC back-end</td>
<td>RFC</td>
<td>Application data</td>
<td>Application data (depending on individual security requirements and the sensitivity of data)</td>
</tr>
</tbody>
</table>

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 the Security Guide for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75 under Security Information. In the Security Guide, choose 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 service.sap.com/scm ➝ Technology ➝ Architecture overview.
For more information, see the section about communication security in the Security Guide for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75 under Security Information.
For more information about security aspects for connectivity and interoperability of SAP NetWeaver see the Security Guide for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75 under Security Information.

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 Help Portal at help.sap.com/nwpi71/ ➝ Security Information.

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.
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 more information about network security, see the section about Network and Communication Security in the Security Guide for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75 under Security Information.

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

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

### Table 22: Connection Destinations

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
</table>
| SAP SNC ➤ SAP NetWeaver <LCRSAPRFC> | No        | RFC – TCP/IP    |                      | For more information, see the configuration documentation in SAP Solution Manager under  
|                      |           |                 |                      |  
|                      |           |                 |                      | Solutions/Applications ➤ Basic Configuration ➤ Configuration Structures ➤ SAP NetWeaver 7.5 ➤ Process Integration ➤ Configuring Process Integration (PI) Dual Stack ➤ Basic Configuration for SAP NetWeaver Process Integration (PI) ➤ Manual Configuration for SAP NetWeaver Process Integration ➤ Creating Destinations on the ABAP Server  
|                      |           |                 |                      | and  
|                      |           |                 |                      | Solutions/Applications ➤ Basic Configuration ➤ Configuration Structures ➤ SAP NetWeaver 7.5 ➤ Process Integration ➤ Configuring Process Integration (PI) Dual Stack ➤ Configuration of Business Systems with Integration Engine  
|                      |           |                 |                      |  
| SAP SNC ➤ SAP NetWeaver <SAPSLDAPI> | No        | RFC – TCP/IP    |                      | For more information, see the configuration documentation in SAP Solution Manager under  
|                      |           |                 |                      |  
|                      |           |                 |                      | Solutions/Applications ➤ Basic Configuration ➤ Configuration Structures ➤ SAP NetWeaver 7.5 ➤ Process Integration ➤ Configuring Process Integration (PI) Dual Stack ➤ Basic Configuration for SAP NetWeaver Process Integration (PI) ➤ Manual Configuration for SAP NetWeaver Process Integration ➤ Creating Destinations on the ABAP Server  
|                      |           |                 |                      | and  
|                      |           |                 |                      | Solutions/Applications ➤ Basic Configuration ➤ Configuration Structures ➤ SAP NetWeaver 7.5 ➤ Process Integration ➤ Configuring Process Integration (PI) Dual Stack ➤ Configuration of Business Systems with Integration Engine  
|                      |           |                 |                      |  
| ERP system ➤ SAP NetWeaver <LCRSAPRFC> | No        | RFC – TCP/IP    |                      | For more information, see the configuration documentation in SAP Solution Manager under  
|                      |           |                 |                      |  
|                      |           |                 |                      | Solutions/Applications ➤ Basic Configuration ➤ Configuration Structures ➤ SAP NetWeaver 7.5 ➤ Process Integration  

---

CUSTOMER  
© Copyright 2016 SAP SE or an SAP affiliate company.  
All rights reserved.  
SAP Enhancement Package 4 for SAP® Supply Network Collaboration (SAP SNC) 7.0  
Network and Communication Security
<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERP system</td>
<td>No</td>
<td>RFC – TCP/IP</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under</td>
<td>Configuring Process Integration (PI) Dual Stack &gt; Basic Configuration for SAP NetWeaver Process Integration (PI) &gt; Manual Configuration for SAP NetWeaver Process Integration (PI) Dual Stack &gt; Basic Configuration for SAP NetWeaver Process Integration (PI) &gt; Manual Configuration for SAP NetWeaver Process Integration (PI) &gt; Connecting to the Integration Server</td>
</tr>
<tr>
<td>SAP NetWeaver</td>
<td>No</td>
<td>RFC – TCP/IP</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under</td>
<td>Configuring Process Integration (PI) Dual Stack &gt; Basic Configuration for SAP NetWeaver Process Integration (PI) &gt; Manual Configuration for SAP NetWeaver Process Integration (PI) &gt; Creating Destinations on the ABAP Server</td>
</tr>
<tr>
<td>SAP NetWeaver</td>
<td>No</td>
<td>RFC – TCP/IP</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under</td>
<td>Configuring Process Integration (PI) Dual Stack &gt; Basic Configuration for SAP NetWeaver Process Integration (PI) &gt; Manual Configuration for SAP NetWeaver Process Integration (PI) &gt; Creating Destinations on the ABAP Server</td>
</tr>
<tr>
<td>SAP Enhancement</td>
<td>No</td>
<td>RFC – TCP/IP</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under</td>
<td>Configuring Process Integration (PI) Dual Stack &gt; Basic Configuration for SAP NetWeaver Process Integration (PI) &gt; Manual Configuration for SAP NetWeaver Process Integration (PI) &gt; Creating Destinations on the ABAP Server</td>
</tr>
<tr>
<td>SAP Enhancement</td>
<td>No</td>
<td>RFC – TCP/IP</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under</td>
<td>Configuring Process Integration (PI) Dual Stack &gt; Basic Configuration for SAP NetWeaver Process Integration (PI) &gt; Manual Configuration for SAP NetWeaver Process Integration (PI) &gt; Creating Destinations on the ABAP Server</td>
</tr>
<tr>
<td>Enhancement Package 4 for SAP® Supply Network Collaboration (SAP SNC) 7.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination</td>
<td>Delivered</td>
<td>Type</td>
<td>User, Authorizations</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SAP NetWeaver Process Integration (PI) ➔ SAP SNC ➔</td>
<td>No</td>
<td>RFC – HTTP Connections to ABAP System</td>
<td></td>
<td>For more information, see the configuration documentation in SAP Solution Manager under Solutions/Applications ➔ Basic Configuration ➔ Configuration Structures ➔ SAP NetWeaver 7.5 ➔ Process Integration ➔ Configuring Process Integration (PI) Dual Stack ➔ Manual Configuration for SAP NetWeaver Process Integration (PI) ➔ Creating Destinations on the ABAP Server and Solutions/Applications ➔ Basic Configuration ➔ Configuration Structures ➔ SAP NetWeaver 7.5 ➔ Process Integration ➔ Configuring Process Integration (PI) Dual Stack ➔ Configuration of Business Systems with Integration Engine.</td>
</tr>
<tr>
<td>SAP SNC ➔ SAP NetWeaver Process Integration (PI) ➔</td>
<td>No</td>
<td>RFC – HTTP Connections to ABAP System</td>
<td>User role: SAP_XI_APPL_SERV_USER</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under Solutions/Applications ➔ Basic Configuration ➔ Configuration Structures ➔ SAP NetWeaver 7.5 ➔ Process Integration ➔ Configuring Process Integration (PI) Dual Stack ➔ Manual Configuration for SAP NetWeaver Process Integration (PI) ➔ Creating Destinations on the ABAP Server and Solutions/Applications ➔ Basic Configuration ➔ Configuration Structures ➔ SAP NetWeaver 7.5 ➔ Process Integration ➔ Configuring Process Integration (PI) Dual Stack ➔ Configuration of Business Systems with Integration Engine.</td>
</tr>
<tr>
<td>ERP system ➔ SAP NetWeaver Usage Type PI ➔</td>
<td>No</td>
<td>RFC – HTTP Connections to ABAP System</td>
<td></td>
<td>For more information, see the configuration documentation in SAP Solution Manager under Solutions/Applications ➔ Basic Configuration ➔ Configuration Structures ➔ SAP NetWeaver 7.5 ➔ Process Integration ➔ Configuring Process Integration (PI) Dual Stack ➔ Manual Configuration for SAP NetWeaver Process Integration (PI) ➔ Creating Destinations on the ABAP Server and Solutions/Applications ➔ Basic Configuration ➔ Configuration Structures ➔ SAP NetWeaver 7.5 ➔ Process Integration ➔ Configuring Process Integration (PI) Dual Stack.</td>
</tr>
<tr>
<td>Destination</td>
<td>Delivered</td>
<td>Type</td>
<td>User, Authorizations</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>SAP NetWeaver Usage Type PI » ERP system</strong></td>
<td>No</td>
<td>RFC – HTTP Connections to ABAP System</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under <strong>Solutions/Applications » Basic Configuration » Configuration Structures</strong> » SAP NetWeaver 7.5 » Process Integration » Configuring Process Integration (PI) Dual Stack » Basic Configuration for SAP NetWeaver Process Integration (PI) » Manual Configuration for SAP NetWeaver Process Integration » Creating Destinations on the ABAP Server and <strong>Solutions/Applications » Basic Configuration » Configuration Structures</strong> » SAP NetWeaver 7.5 » Process Integration » Configuring Process Integration (PI) Dual Stack » Configuration of Business Systems with Integration Engine.</td>
<td></td>
</tr>
<tr>
<td><strong>SAP NetWeaver Usage Type PI » ERP system</strong></td>
<td>No</td>
<td>RFC – ABAP Connections</td>
<td>For more information, see the configuration documentation in SAP Solution Manager under <strong>Solutions/Applications » Basic Configuration » Configuration Structures</strong> » SAP NetWeaver 7.5 » Process Integration » Configuring Process Integration (PI) Dual Stack » Integration of Business Systems without Integration Engine » Integration Using the IDoc Adapter (Integration Engine) » Maintaining the Integration Server.</td>
<td></td>
</tr>
<tr>
<td><strong>ERP system » SAP NetWeaver Usage Type PI</strong></td>
<td>No</td>
<td>RFC – ABAP Connections</td>
<td>User role: <strong>SAP_XI_APPL_SERV_USER</strong> For more information, see the configuration documentation in SAP Solution Manager under <strong>Solutions/Applications » Basic Configuration » Configuration Structures</strong> » SAP NetWeaver 7.5 » Process Integration » Configuring Process Integration (PI) Dual Stack » Integration of Business Systems without Integration Engine » Integration Using the IDoc Adapter (Integration Engine) » Maintaining the IDoc Sender System.</td>
<td></td>
</tr>
<tr>
<td><strong>ERP system » SAP SNC</strong></td>
<td>No</td>
<td>RFC – ABAP Connections</td>
<td>You must set up an RFC connection for master data integration using Core Interface.</td>
<td></td>
</tr>
<tr>
<td><strong>SAP SNC » Collaboration Folders</strong></td>
<td>No</td>
<td>RFC – ABAP Connections</td>
<td>We recommend that you set up an RFC connection to the Collaboration Folders</td>
<td></td>
</tr>
<tr>
<td>Destination</td>
<td>Delivered</td>
<td>Type</td>
<td>User, Authorizations</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| SAP SNC    | No        | RFC – ABAP Connections | Service user and password, RFC authorization | If you are running the following visibility processes in SAP SNC, you must set up an RFC connection to SAP EM:  
• SNC Visibility Process for Inbound Message  
• SNC Visibility Process for Purchase Order  
• SNC Visibility Process for Replenishment Order |
| SAP Event Management | No | RFC – ABAP Connections | If you are running the following visibility processes in SAP SNC, you must set up an RFC connection to SAP SNC:  
• SNC Visibility Process for Inbound Message  
• SNC Visibility Process for Purchase Order  
• SNC Visibility Process for Replenishment Order |
| SAP SCM    | No        | RFC – HTTP Connections to ABAP System | 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, you must set up this RFC connection to ensure the integration of XML services.  
For more information, see the configuration documentation in SAP Solution Manager under Solutions/Applications Basic Configuration Configuration Structures SAP NetWeaver 7.5 Process Integration Configuring Process Integration (PI) Dual Stack Basic Configuration for SAP NetWeaver Process Integration (PI) Manual Configuration for SAP NetWeaver Process Integration Configuring Destinations on the ABAP Server and  
Solutions/Applications Basic Configuration Configuration Structures SAP NetWeaver 7.5 Process Integration Configuring Process Integration (PI) Dual Stack Configuration of Business Systems with Integration Engine. |

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, you must set up this RFC connection to ensure the integration of XML services.  
For more information, see the configuration documentation in SAP Solution Manager under Solutions/Applications Basic Configuration Configuration Structures SAP NetWeaver 7.5 Process Integration Configuring Process Integration (PI) Dual Stack Basic Configuration for SAP NetWeaver Process Integration (PI) Manual Configuration for SAP NetWeaver Process Integration Configuring Destinations on the ABAP Server and  
Solutions/Applications Basic Configuration Configuration Structures SAP NetWeaver 7.5 Process Integration Configuring Process Integration (PI) Dual Stack Configuration of Business Systems with Integration Engine. |
<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replenishment Orders business process and the</td>
<td>No</td>
<td>RFC – ABAP</td>
<td></td>
<td>Replenishment Orders business process and the Dynamic Replenishment business process, you must set up this RFC connection to ensure integration using the IDoc adapter. For more information, see the configuration documentation in SAP Solution Manager under Solutions/Applications ▶ Basic Configuration ▶ Configuration Structures ▶ SAP NetWeaver 7.5 ▶ Process Integration ▶ Configuring Process Integration (PI) Dual Stack ▶ Integration of Business Systems without Integration Engine ▶ Integration Using the IDoc Adapter (Integration Engine) ▶ Maintaining the IDoc Sender System ▶.</td>
</tr>
</tbody>
</table>
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 activating and deactivating ICF services, see the Application Help for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75. In Application Help, choose Function-Oriented View ➤ Application Server ➤ Application Server Infrastructure ➤ Connectivity ➤ Components of SAP Communication Technology ➤ Communication Between ABAP and Non-ABAP Technologies ➤ Internet Communication Framework ➤ Development ➤ Server-Side Development ➤ Creating and Configuring an ICF Service ➤ Activating and Deactivating ICF Services.
9 Data Storage Security

SAP Supply Network Collaboration (SAP SNC) including enhancement package 4 is based on SAP NetWeaver 7.5. The data storage security of SAP NetWeaver and the components that are installed on that base is described in detail in the SAP NetWeaver Security Guide.

**Note**

The SAP SNC business data is stored in the system database.
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 the Application Help for SAP NetWeaver 7.5 on SAP Help Portal at help.sap.com/nw75. In Application Help, choose Function-Oriented View > UI Technologies in SAP Netweaver > SAP GUI > SAP Graphics > Internet Graphics Service > Internet Graphics Service Security.

Web Dynpro
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:

- User Administration and Authentication
- Network and Communication Security
- Security Guide for SAP NetWeaver Process Integration (PI)
- ABAP: Security Guide Web Services
- RFC/ICF Security Guide
- Security Guides for Operating System and Database Platforms
- Security Guides for AS ABAP
- SAP Process Integration Security Guide
- Enabling Business-to-Business Processes: Security Aspects

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 NetWeaver Application Server. For this, SAP SNC uses the standard BCS interface. The SAP NetWeaver 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 NetWeaver 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 SAP NetWeaver Process Integration (PI) 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 (BAdI) 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 (BAdIs) for SAP SNC ➔ Basic Settings ➔ Processing Inbound and Outbound Messages ➔ BAdI: 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 in SAP Supply Chain Management, see also the SAP SCM Component Security Guide.
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 Section in the EarlyWatch Alert (EWA) Report**

This service regularly monitors the Security section 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 that 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 that 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: service.sap.com/ewa
- Comprehensive list of Security Notes: service.sap.com/securitynotes
- Configuration Validation: service.sap.com/changecontrol
- RunSAP Roadmap, including the Security and the Secure Operations Standard: service.sap.com/runsap
  (See the RunSAP sections 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.

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 help.sap.com/glossary
  - In the SAP system in transaction STERN

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 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 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 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 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 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 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 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 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 service.sap.com/releasenotes
  - In the SAP menu of the SAP system under Help > Release Notes (only ABAP developments)