SAP Advanced Planning and Optimization 7.0
Including Enhancement Package 4
Using SAP enhancement package 4 for SAP SCM or SAP enhancement package 8 for SAP ERP 6.0
# Typographic Conventions

## Table 1

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Example&gt;</code></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 <code>&lt;User Name&gt;</code>”.</td>
</tr>
<tr>
<td><code>Example ➔ Example</code></td>
<td>Arrows separating the parts of a navigation path, for example, menu options</td>
</tr>
<tr>
<td><code>Example</code></td>
<td>Emphasized words or expressions</td>
</tr>
<tr>
<td><code>Example</code></td>
<td>Words or characters that you enter in the system exactly as they appear in the documentation</td>
</tr>
<tr>
<td><code>www.sap.com</code></td>
<td>Textual cross-references to an internet address</td>
</tr>
<tr>
<td><code>/example</code></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><code>123456</code></td>
<td>Hyperlink to an SAP Note, for example, SAP Note <code>123456</code></td>
</tr>
<tr>
<td><code>Example</code></td>
<td>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</td>
</tr>
<tr>
<td><code>Example</code></td>
<td>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</td>
</tr>
<tr>
<td><code>EXAMPLE</code></td>
<td>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, <code>SELECT</code> and <code>INCLUDE</code></td>
</tr>
<tr>
<td><code>EXAMPLE</code></td>
<td>Keys on the keyboard</td>
</tr>
</tbody>
</table>
Caution
Before you start the implementation, make sure you have the latest version of this document. You can find the latest version on SAP Service Marketplace service.sap.com/instguides.

The following table provides an overview on 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>Initial version</td>
</tr>
</tbody>
</table>
# Content

1. Introduction ................................................................. 7
2. Before You Start ............................................................. 10
3. Technical System Landscape ............................................... 12
5. User Administration and Authentication ..................................... 16
   5.1 User Management ...................................................... 16
   5.2 User Data Synchronization ............................................ 19
   5.3 Integration Into Single Sign-On Environments .......................... 20
6. Authorizations ............................................................... 21
   6.1 Standard Roles .......................................................... 21
   6.2 Roles for SAP APO ..................................................... 22
   6.3 Maintaining Authorizations for SAP APO ............................... 22
   6.4 Authorizations for Service Parts Planning ............................. 23
   6.5 Maintaining Authorizations for Integration with SAP Components .......... 24
   6.6 Maintaining Authorizations for Enterprise Services ..................... 25
7. Session Security Protection ................................................ 26
8. Network and Communication Security ...................................... 27
   8.1 Communication Channel Security ..................................... 27
   8.2 Network Security ...................................................... 28
   8.3 Communication Destinations .......................................... 29
   8.4 Internet Communication Framework Security ........................... 31
9. Data Storage Security ........................................................ 33
10. Data Protection ............................................................. 36
    10.1 Deletion of Personal Data ............................................. 37
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Security for Additional Applications</td>
<td>39</td>
</tr>
<tr>
<td>12</td>
<td>Enterprise Services Security</td>
<td>40</td>
</tr>
<tr>
<td>13</td>
<td>Other Security-Relevant Information</td>
<td>41</td>
</tr>
<tr>
<td>14</td>
<td>Security-Relevant Logging and Tracing</td>
<td>42</td>
</tr>
<tr>
<td>15</td>
<td>Services for Security Lifecycle Management</td>
<td>43</td>
</tr>
<tr>
<td>A</td>
<td>Appendix</td>
<td>45</td>
</tr>
<tr>
<td>A.1</td>
<td>Related Security Guides</td>
<td>45</td>
</tr>
<tr>
<td>A.2</td>
<td>Related Information</td>
<td>45</td>
</tr>
</tbody>
</table>
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 also apply to SAP Advanced Planning & Optimization (SAP APO). To assist you in securing your SAP APO component, we provide this Component Security Guide.

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

About This Document
As SAP APO provides two deployment options, this document describes both options in parallel:

- **SAP APO as part of** SAP Supply Chain Management (SAP SCM)
  - This deployment option requires the use of **SAP enhancement package 4 for SAP SCM 7.0** (including SAP APO).
  - **SAP enhancement package 4 for SAP SCM 7.0** is based on **SAP NetWeaver 7.5**.

- **SAP APO as add-on for** SAP Enterprise Resource Planning (SAP ERP)
  - This deployment option requires the use of **SAP enhancement package 4 for SAP APO 7.0 on SAP enhancement package 8 for SAP ERP 6.0**.
  - **SAP enhancement package 8 for SAP ERP 6.0** is based on **SAP NetWeaver 7.5**.

This Security Guide provides an overview of the security-relevant information that applies to both SAP APO deployment options.

Overview of the Main Sections
The Security Guide comprises the following main sections:

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

- **Technical System Landscape**
This section provides an overview of the technical components and communication paths that are used by the SAP APO component.

- **Security Aspects of Data, Data Flow and Processes**
  This section provides an overview of the data flow for an SAP ERP sales order entry, with subsequent Global ATP check in SAP APO as an example for security aspects. It also covers the publishing of transaction data from SAP APO to SAP ERP as another example.

- **User Administration and Authentication**
  This section provides an overview of the following user administration and authentication aspects:
  - Recommended tools to use for user management.
  - User types that are required by the SAP APO component.
  - Standard users that are delivered with the SAP APO component.
  - Overview of the user synchronization strategy, if several components or products are involved.
  - Overview of how integration into Single Sign-On environments is possible.

- **Authorizations**
  This section provides an overview of the authorization concept that applies to the SAP APO component.

- **Session Security Protection**
  This section provides an overview of secure session management practises for AS ABAP.

- **Network and Communication Security**
  This section provides an overview of the communication paths used by the SAP APO component and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

- **Internet Communication Framework Security**
  This section lists the services that must be activated for the SAP APO application to run in your system.

- **Data Storage Security**
  This section provides an overview of any critical data that is used by the SAP APO component and the security mechanisms that apply.

- **Security for Third-Party or Additional Applications**
  This section provides security information that applies to third-party or additional applications that are used with the SAP APO component.

- **Enterprise Services Security**
  This section lists chapters of the SAP NetWeaver Security Guide that are relevant for all enterprise services delivered with SAP APO.

- **Other Security-Relevant Information**
  This section contains information about:
  - User Frontend
  - Virus Check of Document Attachments

- **Security-Relevant Logging and Tracing**
  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 lists the services that are available from Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.
Appendix
This section provides references to further information.

SAP Fiori apps
For more information regarding SAP Fiori apps, see SAP Library at help.sap.com/scm under SAP Fiori for SAP SCM.
2 Before You Start

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

<table>
<thead>
<tr>
<th>Guide/Documentation</th>
<th>Full Path to the Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver Security Guides</td>
<td><a href="help.sap.com/nw75">help.sap.com/nw75</a> Security Information</td>
</tr>
<tr>
<td>SAP NetWeaver Documentation</td>
<td><a href="help.sap.com/nw75">help.sap.com/nw75</a></td>
</tr>
<tr>
<td>SAP APO Documentation</td>
<td><a href="help.sap.com/scm704">help.sap.com/scm704</a> Application Help</td>
</tr>
<tr>
<td>SAP APO Installation Note</td>
<td>SAP Note 1792146</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>25591</td>
<td>Changing the DBM, SYSDBA and DBA user passwords</td>
<td>This SAP Note provides information on changing the passwords.</td>
</tr>
<tr>
<td>30724</td>
<td>Data protection and security in SAP Systems</td>
<td></td>
</tr>
<tr>
<td>128447</td>
<td>Trusted/Trusting Systems</td>
<td></td>
</tr>
<tr>
<td>305634</td>
<td>RFC destination for working globally with the liveCache</td>
<td></td>
</tr>
<tr>
<td>400434</td>
<td>Authorizations in APO Demand Planning</td>
<td>A brief explanation of the concept behind authorizations in SAP APO for Demand Planning</td>
</tr>
<tr>
<td>447543</td>
<td>APO: Authorizations too comprehensive/not user-specific</td>
<td></td>
</tr>
<tr>
<td>SAP Note Number</td>
<td>Title</td>
<td>Comment</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>510007</td>
<td>Setting-up SSL on the Web Application Server ABAP</td>
<td></td>
</tr>
<tr>
<td>616555</td>
<td>liveCache &gt;= 7.4: Password change</td>
<td></td>
</tr>
<tr>
<td>821200</td>
<td>Standard user must be known to the DBM server</td>
<td></td>
</tr>
<tr>
<td>1072949</td>
<td>Role for managing the liveCache and LCA routines</td>
<td></td>
</tr>
<tr>
<td>1394093</td>
<td>Collective Security Note</td>
<td></td>
</tr>
<tr>
<td>1515223</td>
<td>SAP NetWeaver Process Integration: Release Recommendation</td>
<td>This SAP Note sets out our recommendation on which release of SAP NetWeaver PI you should use. This SAP note is only relevant for SAP APO as part of SAP SCM.</td>
</tr>
<tr>
<td>1511041</td>
<td>Missing Authorization Check in ECC-DIMP</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
For more SAP Notes about security, see SAP Service Marketplace at the following locations:
- [service.sap.com/security ➔ SAP Security Notes ➔](service.sap.com/security)
- [service.sap.com/securitynotes ➔](service.sap.com/securitynotes)

**Additional Information**
For more information about specific topics, see the addresses on SAP Service Marketplace as shown in the table below.

<table>
<thead>
<tr>
<th>Table 5: Quick Links to Additional Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Quick Link on the SAP Service Marketplace or SDN</td>
</tr>
<tr>
<td>Security</td>
<td><a href="sdn.sap.com/irj/sdn/security">sdn.sap.com/irj/sdn/security</a> ➔ <a href="service.sap.com/security">service.sap.com/security</a></td>
</tr>
<tr>
<td>Security Guides</td>
<td><a href="service.sap.com/securityguide">service.sap.com/securityguide</a> ➔</td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td><a href="service.sap.com/notes">service.sap.com/notes</a> ➔</td>
</tr>
<tr>
<td>Released Platforms</td>
<td><a href="service.sap.com/pam">service.sap.com/pam</a> ➔ <a href="service.sap.com/platforms">service.sap.com/platforms</a></td>
</tr>
<tr>
<td>Network Security</td>
<td><a href="service.sap.com/securityguide">service.sap.com/securityguide</a> ➔</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td><a href="service.sap.com/solutionmanager">service.sap.com/solutionmanager</a> ➔</td>
</tr>
<tr>
<td>SAP NetWeaver</td>
<td><a href="sdn.sap.com/irj/sdn/netweaver">sdn.sap.com/irj/sdn/netweaver</a> ➔</td>
</tr>
</tbody>
</table>
3 Technical System Landscape

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

Table 6: 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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical System Landscape</td>
<td>SAP APO Master Guide</td>
<td>service.sap.com/instguides</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP Business Suite Applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP SCM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP APO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using SAP Enhancement Package 4 for SAP APO 7.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Master Guide</td>
</tr>
<tr>
<td>Technical Configuration, High Availability</td>
<td>Technical Infrastructure Guide</td>
<td>service.sap.com/installNW75</td>
</tr>
</tbody>
</table>
4 Security Aspects of Data, Data Flow and Processes

This section provides an overview of the data flow for an SAP ERP sales order entry, with subsequent Global ATP check in SAP APO as an example for security aspects. It also covers the publishing of transaction data from SAP APO to SAP ERP as another example.

Global ATP Check for Sales Orders in SAP ERP

The figure below shows an overview of the data flow for the SAP ERP sales order entry, with subsequent Global ATP check in SAP APO.

The table below shows security aspects to be considered for the process steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User submits sales order line item creation</td>
<td>User type: Dialog user</td>
</tr>
<tr>
<td>2</td>
<td>Determine APO RFC destination</td>
<td>Not applicable</td>
</tr>
<tr>
<td>3</td>
<td>Call APO-gATP check</td>
<td>User type: Dialog user&lt;br&gt;For detailed setup, see section Maintaining Authorizations for Integration with SAP Components [page 24]</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Security Measure</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>CIF select all objects in SAP ERP that are contained in the integration model</td>
<td>Not applicable</td>
</tr>
<tr>
<td>2</td>
<td>Objects are sent to SAP APO by qRFC</td>
<td>User type: Communication user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For detailed setup, see section Maintaining Authorizations for Integration with SAP Components [page 24]</td>
</tr>
<tr>
<td>3</td>
<td>Create/modify/delete objects in SAP APO</td>
<td>Not applicable</td>
</tr>
<tr>
<td>4</td>
<td>Check the status of qRFC queues</td>
<td>User type: Communication user</td>
</tr>
</tbody>
</table>

**SAP ERP Initial Dataload for Master Data and Transaction Data**

![Diagram of SAP ERP Initial Dataload](image)

**Table 8**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CIF select all objects in SAP ERP that are contained in the integration model</td>
<td>Not applicable</td>
</tr>
<tr>
<td>2</td>
<td>Objects are sent to SAP APO by qRFC</td>
<td>User type: Communication user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For detailed setup, see section Maintaining Authorizations for Integration with SAP Components [page 24]</td>
</tr>
<tr>
<td>3</td>
<td>Create/modify/delete objects in SAP APO</td>
<td>Not applicable</td>
</tr>
<tr>
<td>4</td>
<td>Check the status of qRFC queues</td>
<td>User type: Communication user</td>
</tr>
</tbody>
</table>
For detailed setup, see section Maintaining Authorizations for Integration with SAP Components [page 24]

Publishing Transaction Data from SAP APO to SAP ERP

Table 9

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SAP APO planning applications change orders and publish their keys to CIF</td>
<td>Not applicable</td>
</tr>
<tr>
<td>2</td>
<td>SAP APO CIF extracts changed orders</td>
<td>Not applicable</td>
</tr>
<tr>
<td>3</td>
<td>Orders are sent to SAP ERP by qRFC</td>
<td>User type: Communication user For detailed setup, see section Maintaining Authorizations for Integration with SAP Components [page 24]</td>
</tr>
<tr>
<td>4</td>
<td>Change the respective orders in SAP ERP</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
User Administration and Authentication

The SAP APO component uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide also apply to the SAP APO component.

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

- **User Management [page 16]**
  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the SAP APO component.

- **User Data Synchronization [page 19]**
  The SAP APO component shares user data with SAP NetWeaver. This topic describes how the user data is synchronized with these other sources.

- **Integration Into Single Sign-On Environments [page 20]**
  This topic describes how the SAP APO component supports Single Sign-On mechanisms.

### 5.1 User Management

User management for the SAP APO component 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 to the SAP APO component, see the sections below. In addition, we provide a list of the standard users required for operating the SAP APO component.

#### User Administration Tools

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

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</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>
<td></td>
</tr>
<tr>
<td>Profile Generator (transaction PFCG)</td>
<td>Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.</td>
<td></td>
</tr>
<tr>
<td>Central User Administration (CUA)</td>
<td>Use the CUA to centrally maintain users for multiple ABAP-based systems. Synchronization with a directory server is also supported.</td>
<td></td>
</tr>
</tbody>
</table>
Tool | Detailed Description | Prerequisites
--- | --- | ---
User Management Engine (UME) administration console | Use the Web-based UME administration console to maintain users, roles and authorizations in Java-based systems that use the UME for the user store, for example, the SAP J2EE Engine and the Enterprise Portal. The UME also supports various persistency options, such as the ABAP Engine or a directory server. |  

**Note**

For a detailed description of the user management tools available in SAP NetWeaver, see the SAP NetWeaver Security Guide under *User Administration and Authentication > User Management*.

**User Types**

It can be 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 which background processing jobs run.

The user types that are required for the SAP APO component include:

- **Individual users:**
  - Dialog users are used for individual, interactive system access.

- **Technical users** comprise the following types:
  - 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.

**Note**

For more information about these user types, see the SAP NetWeaver Security Guide under *User Administration and Authentication > User Management*.

**Standard Users**

The following table shows the standard users that are necessary to operate SAP APO:

<table>
<thead>
<tr>
<th>System</th>
<th>User ID</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
<th>Deployment Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP SCM 7.0</td>
<td>&lt;sapsid&gt;adm</td>
<td>SAP System Administrator</td>
<td>To be entered</td>
<td>See SAP Marketplace at service.sap.com/</td>
<td>Required for SAP APO as part of SAP SCM</td>
</tr>
<tr>
<td>System</td>
<td>User ID</td>
<td>Type</td>
<td>Default Password</td>
<td>Detailed Description</td>
<td>Deployment Option</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SAP SCM 7.0</td>
<td>SAPService &lt;sapsid&gt;</td>
<td>SAP System Service Administrator</td>
<td>To be entered</td>
<td>See Installation Guides for SAP EHP 4 for SAP SCM 7.0 and choose your database/operating system</td>
<td>Required for SAP APO as part of SAP SCM (SAP APO as add-on for SAP ERP uses SAP ERP standard users)</td>
</tr>
<tr>
<td>SAP SCM / SAP APO</td>
<td>RFC communication users (you need an RFC communication user for each RFC destination in the section <em>Communication Destination</em>)</td>
<td>Communicating user</td>
<td>The authorizations of the user depend on the business case. For more information, see section <em>Authorizations</em> [page 21].</td>
<td>See sections <em>Communication Destinations</em> [page 29] and <em>Authorizations</em> [page 21]</td>
<td>Both deployment options</td>
</tr>
<tr>
<td>SAP SCM / SAP APO</td>
<td>Business processing users (you need a user in each component,</td>
<td>Dialog user</td>
<td>To be entered</td>
<td>SAP SCM documentation and section <em>Authorizations</em> [page 21]</td>
<td>Both deployment options</td>
</tr>
<tr>
<td>System</td>
<td>User ID</td>
<td>Type</td>
<td>Default Password</td>
<td>Detailed Description</td>
<td>Deployment Option</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>SAP liveCache</td>
<td>&lt;lcid&gt;adm</td>
<td>Operating system user</td>
<td>To be changed</td>
<td>See SAP Marketplace at service.sap.com/instguides under SAP Business Suite Applications &gt; SAP SCM &gt; Using SAP enhancement package 3 for SAP SCM Server 7.0 &gt; Installation Guides &gt; Installation Guides for SAP EHP 3 for SAP SCM 7.0 &gt; Generic Installation Guides and choose your database/operating system; see also SAP Notes 25591 and 616555.</td>
<td>Both deployment options</td>
</tr>
<tr>
<td>SAP liveCache</td>
<td>SAP&lt;sapid&gt;liveCache</td>
<td>MaxDB database user</td>
<td>To be changed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP liveCache</td>
<td>CONTROL liveCache</td>
<td>MaxDB database user</td>
<td>To be changed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP liveCache</td>
<td>SUPERDBA liveCache</td>
<td>MaxDB database user</td>
<td>To be changed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommendation**

We recommend that you change the user IDs and passwords that are automatically created during installation.

### 5.2 User Data Synchronization

To avoid administrative effort, you can use user data synchronization in your system landscape. Since the SAP APO component is based on SAP NetWeaver, all the mechanisms for user data synchronization of SAP NetWeaver are available for SAP APO.

**Note**

For information about user data synchronization, see the SAP NetWeaver Security Guide under User Administration and Authentication > User Management > Identity Management > Identity Management for System Landscapes > Integration of User Management in Your System Landscape.
5.3 Integration Into Single Sign-On Environments

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

**Note**

For more information about integration into Single Sign-On environments based on SAP NetWeaver, see the SAP NetWeaver Security Guide under [User Administration and Authentication] > [User Authentication and Single Sign-On].

For more information about authentication on the SAP Web application server ABAP, see the SAP NetWeaver Security Guide under [Security Guides for SAP NetWeaver Functional Units] > [Security Guides for the Application Server] > [SAP NetWeaver Application Server ABAP Security Guide] > [User Authentication].

The most widely-used supported mechanisms are listed below.

- **Secure Network Communications (SNC)**
  
  SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.

  For more information, see the SAP NetWeaver Security Guide under [Network and Communication Security] > [Transport Layer Security] > [Secure Network Communications (SNC)].

- **SAP logon tickets**

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

  For more information about integration into Single Sign-On environments based on SAP NetWeaver, see the SAP NetWeaver Security Guide under [User Administration and Authentication] > [User Authentication and Single Sign-On].

- **Client certificates**

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

  For more information about integration into Single Sign-On environments based on SAP NetWeaver, see the SAP NetWeaver Security Guide under [User Administration and Authentication] > [User Authentication and Single Sign-On].
6 Authorizations

SAP APO uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to the SAP APO component.

The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, you can use the Profile Generator (transaction PFCG) when using ABAP.

Note
For information about role maintenance and the Profile Generator, see SAP NetWeaver Security Guide under User Administration and Authentication > User Management > Identity Management > User and Role Administration of Application Server ABAP > AS ABAP Authorization Concept > Organizing Authorization Administration.

Note
For information about the authorization concept of SAP NetWeaver, see SAP NetWeaver Security Guide under User Administration and Authentication > User Management > Identity Management > User and Role Administration of Application Server ABAP > AS ABAP Authorization Concept.

SAP Fiori apps
For more information regarding roles for SAP Fiori apps, see SAP Library at help.sap.com/scm under SAP Fiori for SAP SCM.

6.1 Standard Roles

With SAP APO, SAP delivers SAP standard roles to cover the common business cases. These roles can be used as examples, or as a copy master for your own roles.

Using input help, you can find the SAP standard roles in the Profile Generator (transaction code PFCG). You can use search terms to restrict the selection to the required standard roles. For example, the search term *APO* lists all APO-relevant SAP standard roles. The role short text helps you find the role for your business needs. The role documentation provides you with a detailed description of the role content.

Some of the components in SAP APO have additional authorization methods. The relevant components and Customizing activities are shown in the following sections.

For more information, refer to the SAP NetWeaver Security Guide.
6.2 Roles for SAP APO

For information about roles in SAP APO, see the SAP APO application help on SAP Help Portal under "SAP Advanced Planning and Optimization (SAP APO) > Roles for SAP APO".

6.3 Maintaining Authorizations for SAP APO

Procedure

This procedure allows you to maintain authorizations for SAP Advanced Planning & Optimization (SAP APO).

Maintaining Master Data (iPPE)

1. In Customizing for SAP SCM, to define iPPE user profiles, choose "Advanced Planning and Optimization > Master Data > Integrated Product and Process Engineering (iPPE) > Settings for the iPPE Workbench Professional > Define User Profiles for the iPPE Workbench Professional".

2. Change the iPPE user profiles defined by SAP in this Customizing activity by changing, copying, renaming, or creating new user profiles.

   The SAP system includes the following user profiles:

   Table 12: Standard User Profiles

<table>
<thead>
<tr>
<th>User Profile</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_PFEALL (Total Display)</td>
<td>This profile includes all the settings you need to work with the iPPE Workbench.</td>
</tr>
<tr>
<td>S_ASTACT (Process Structure)</td>
<td>Part of the S_PFEALL profile; calls up a process structure as a selection tree in the detail area of the iPPE Workbench.</td>
</tr>
<tr>
<td>S_ASTCMP (Product Structure)</td>
<td>Part of the S_PFEALL profile; calls up a product structure as a selection tree in the detail area of the iPPE Workbench.</td>
</tr>
<tr>
<td>S_ASTFLO (Factory Layout)</td>
<td>Part of the S_PFEALL profile; calls up a line structure as a selection tree in the detail area of the iPPE Workbench.</td>
</tr>
</tbody>
</table>

3. Change, copy, and rename the profiles, or create new profiles with the following options:
   - Model Definitions:
     You define how the model definitions between the objects are displayed in the navigation area.
   - Product Lifecycle Management (PLM) Environment:
     Here you define how objects from the PLM environment are displayed in the navigation area of the iPPE Workbench.
   - Reports:
     You define the reports to be available for this profile in the iPPE Workbench Professional. You can only choose reports that you have already defined in the activity Define Reports for the Reporting Tree.

4. Save your entries.
Maintaining Authorizations for Supply Chain Planning

1. In Customizing for SAP SCM, to specify the person (planner) responsible, choose Advanced Planning and Optimization > Supply Chain Planning > Specify the Person (Planner) Responsible.

2. To assign planning privileges to planners, you have to maintain the applications for which each planner is responsible as follows:
   1. Choose New Entries.
   2. Enter an identifier and description for each planner.
   3. Select each area for which you want the planner to have privileges.
   4. Save your entries.

Maintaining Authorizations for Supply Network Planning and Demand Planning

As of SAP SCM 4.1, planning books within Supply Network Planning (SNP) and Demand Planning (DP) have a new authorization concept. The main advantage is that the creation or the modification of planning books is controlled by authorizations and not by the system change option for the SAP APO component.

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

Note

Passwords / RFC Interface SAP APO does not use passwords; access is granted using RFC interfaces.

Trace Reads / Gateway User

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

Passwords / RFC Interface

SAP APO does not use passwords; access is granted using RFC interfaces.

6.4 Authorizations for Service Parts Planning

Assigning Planners in Service Parts Planning

In Service Parts Planning (SPP), you can assign users to various planners at the location product level. For more information, see the SAP APO application help SAP Help Portal under SAP Advanced Planning and Optimization (SAP APO) > Service Parts Planning (SPP) > Master Data and General Functions for SPP > Assigning Planners in Service Parts Planning.
Roles in Service Parts Planning

For information about roles in SPP, see the SAP APO application help SAP Help Portal under SAP Supply Chain Management (SAP SCM) > SAP Advanced Planning and Optimization (SAP APO) > Roles for SAP APO > Roles for Service Parts Planning (SPP).

6.5 Maintaining Authorizations for Integration with SAP Components

Procedure

Maintaining Authorizations for SAP APO – SAP ERP Integration

Using Standard Roles for SAP APO – SAP ERP Integration

To integrate SAP APO and SAP ERP, use the following authorization roles for the RFC destination users:

- **SAP_SCM_INTEGRATION_SCM**: Authorization role for the SAP APO–SAP ERP integration for background users in SAP APO.
- **SAP_SCM_INTEGRATION_DIMP**: Authorization role for the SAP APO–SAP ERP integration for background users in SAP ERP.

See SAP Note 1511041 for information about role SAP_SCM_INTEGRATION_DIMP (only relevant for releases lower than ECC-DIMP 606).

Maintaining Authorizations for Available-to-Promise (ATP)

Available-to-Promise (ATP) plays an important role in the integration of SAP APO and SAP ERP: The ATP check needs an RFC connection with a dialog user to perform the check. Since a dialog user within RFC connections is a safety flaw, you must minimize this flaw by performing the following steps:

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

   **Note**
   

2. In Customizing for SAP APO, to assign the RFC connection to the ATP application, choose (Integration with SAP Components) > Integration via Core Interface (CIF) > Basic Settings for Creating the System Landscape > Assign RFC Destinations to Various Application Cases.

3. For each SAP ERP user, create a corresponding ATP user in SAP APO.

4. Assign one or more of the following authorization roles to the user(s) in SAP APO:
   - SAP_APO_ATP_CO_3 (ATP Controller)
   - SAP_APO_ATP_CU (APO: ATP Customizing User)
   - SAP_APO_ATP_EU (APO: ATP Expert User)
   - SAP_APO_ATP_SU (APO: ATP Standard User)
   - SAP_APO_ATP_RSP_ALL (APO: ALL ATP Authorizations)
5. Assign the authorization `S_RFCACL_ALL` to the users in SAP APO. This authorization is necessary to perform RFC calls.

Note
For more information about the role maintenance and the SAP Profile Generator, see the SAP NetWeaver Security Guide under | User Administration and Authentication | User Management | Identity Management | User and Role Administration of Application Server ABAP | AS ABAP Authorization Concept | Organizing Authorization Administration |.

Maintaining Authorizations for Data Transfer to SAP NetWeaver BI

Limiting Authorizations for Extraction

Note
You can exclude DataSources from the extraction to SAP NetWeaver BI. Data that is stored in the extract structure of this DataSource cannot be transferred to SAP NetWeaver BI.

1. In Customizing choose | Integration with SAP Components | Data Transfer to the SAP Business Information Warehouse | General Settings | Limit Authorizations for Extraction |.
2. Choose New Entries.
3. Choose a DataSource that you want to exclude from the extraction.
4. Choose the SAP NetWeaver BI system for which you want no more data for this DataSource to be extracted.
5. In the field Excl. Extr., enter whether you want to exclude the DataSource from the extraction.
6. Save your entries.
7. Specify a transport request.

6.6 Maintaining Authorizations for Enterprise Services

Note
SAP APO-specific services are not part of the SAP APO add-on deployment option. They are currently only available in SAP APO as part of SAP SCM. Consider this essential point when you decide which of the two SAP APO deployments you want to use.

Accessing SAP functions via Web services follows the standard SAP authorization concept, which is based on authorizations for specific authorization objects. During the execution of a Web service, the system checks for the required authorization for an authorization object. If a user does not have this authorization, the execution is terminated, and an error message is displayed.

Enterprise services use standard authorization objects, such as authorization default values for Web services, that are available for SAP SCM. In addition, you need the authorization `S_SERVICE` to start external services. To create and use Web services, you need the authorizations that belong to the role `SAP_BC_WEBSERVICE_ADMIN` and authorization for the Internet Communication Framework (`S_ICF_ADMIN`).

For more information about authorizations for Web services, see the SAP NetWeaver Security Guide under | Security Guides for Connectivity and Interoperability Technologies | Security Aspects for Web Services | Web Service Runtime Configuration | Authentication for Web Services |.
7 Session Security Protection

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

Features

Session Security Protection on the AS ABAP

To prevent access in JavaScript or plug-ins to the SAP logon ticket and security session cookies (SAP_SESSIONID_<SID>_<CLIENT>), activate secure session management. With an existing security session, users can then start applications that require a user logon without logging on again. When a security session is ended, the system also ends all applications that are linked to this security session.


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

SAP Advanced Planning and Optimization 7.0 Including Enhancement Package 4

Session Security Protection
Network and Communication Security

Your network infrastructure is 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 backend system’s database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

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

- **Communication Channel Security** [page 27]
  This topic describes the communication paths and protocols used by the SAP APO component.

- **Network Security** [page 28]
  This topic describes the recommended network topology for the SAP APO component. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate the SAP APO component.

- **Communication Destinations** [page 29]
  This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

- **Internet Communication Framework Security** [page 31]
  This topic describes the services that must be activated for the applications running in your system.

For more information, see the following sections in the SAP NetWeaver Security Guide:

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

### 8.1 Communication Channel Security

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

Since communication channels transfer your business data, they should be protected against unauthorized access. SAP offers general recommendations to protect your system landscape, which is based on SAP NetWeaver.
Caution
You should activate the Secure Network Communication (SNC) in all communication channels in SAP APO to achieve a secure system landscape.


For a detailed description of all communication channels within the SAP APO component, see SAP Service Marketplace at service.sap.com/scm > SAP SCM Technology > Architecture Overview.

Note
For more information about the communication security of SAP NetWeaver, see the SAP NetWeaver Security Guide under Network and Communication Security.

For more information about security aspects for connectivity and interoperability of SAP NetWeaver 7.0, see the SAP NetWeaver Security Guide under SAPNet Security Guides for Connectivity and Interoperability Technologies.

SAP APO – SAP ERP

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

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

If you use the cross-system navigation function to navigate from orders in SAP APO to SAP ERP, then for security reasons you must fill in the RFC destination manually, so that the CIF connection is not used.

When single sign-on is enabled, you must ensure that your user exists in both SAP APO and SAP ERP. When single sign-on is not enabled, you are prompted to enter your user name and password in order to proceed to SAP ERP.

Note
For more information about the integration of SAP APO and SAP ERP, see the SAP SCM application help on SAP Help Portal under SCM Basis > Integration via Core Interface (CIF) > Technical Integration.

8.2 Network Security

Your network infrastructure plays a key role in protecting your system. A well-defined network topology can eliminate many security threats based on software flaws (at the operating system and application level) or network attacks such as eavesdropping.

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

Note
A minimum security demand for your network infrastructure is the use of a firewall for all your services that are provided over the Internet.

A more secure variant is to protect your systems (or groups of systems) by locating the system groups in different network segments. Each system group has a firewall that protects it from unauthorized access. External security attacks can also come from the inside, if the intruder has already taken control of one of your systems.

### Note
For information about the technical components of your SAP APO component, see SAP Service Marketplace at service.sap.com/scm > SCM in Detail > Technology.

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

#### Network Security for Enterprise Services
For more information about network security for Web services, see the SAP NetWeaver Security Guide under Security Guides for Connectivity and Interoperability Technologies > Security Aspects for Web Services.

### 8.3 Communication Destinations

#### Caution
If communication destinations are not implemented and used with care, their users and authorizations can cause high security flaws.

The following is a list of the “Golden Rules” for connection users and authorizations:

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

The table below shows an overview of the communication destinations used by the SAP APO component.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="SAP APO Supply Chain Cockpit (SCC)" /> <img src="image" alt="SAP Business Warehouse (BW)" /></td>
<td>No</td>
<td>RFC – ERP</td>
<td>Background user in SAP source system (ALEREMOTE) with authorization profile S_BW-RFC; see <img src="image" alt="SAP Business Information Warehouse Security Guide" /> User Administration and</td>
<td>SAP APO Customizing: <img src="image" alt="Advanced Planning and Optimization" /> <img src="image" alt="Supply Chain Cockpit (SCC)" /> <img src="image" alt="Define Default BW Destination (RFC)" />. Also refer to the SAP NetWeaver BI Security Guide.</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>&lt;SAP_APO_name&gt;CLNT &lt;client&gt;</td>
<td>No</td>
<td>RFC – ERP</td>
<td>Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.</td>
<td>SAP APO Customizing: Integration via Core Interface (CIF) Basic Settings for Creating the System Landscape Assign RFC Destinations to Various Application Cases. SAP SCM Customizing: Integration with SAP Components Integration via APO Core Interface (CIF) Basic Settings for Creating the System Landscape Assign RFC Destinations to Various Application Cases.</td>
</tr>
<tr>
<td>&lt;SAP_APO &gt; SAP ERP</td>
<td>No</td>
<td>RFC – ERP</td>
<td>Use the Profile Generator (transaction code PFCG) and assign one or more of the following roles: SAP_APO_ATP_CO_3 SAP_APO_ATP_CU SAP_APO_ATP_EU SAP_APO_ATP_SU SAP_APO_ATP_RSP_ALL</td>
<td>See section Maintaining Authorizations for Integration with SAP Components Maintaining Authorizations for Available-to-Promise (ATP).</td>
</tr>
<tr>
<td>&lt;System_ID&gt;CLNT &lt;Client_number&gt; (SAP liveCache)</td>
<td>No</td>
<td>RFC – ERP</td>
<td>&lt;liveCache_user_ID&gt;; &lt;liveCache_Authorization&gt; (see SAP Note 305634)</td>
<td>SAP Note: 305634</td>
</tr>
<tr>
<td>OPTSERVER_ &lt;Optimizer&gt;01</td>
<td>Yes</td>
<td>RFC – TCP/IP</td>
<td>Not applicable</td>
<td>The delivered destinations must be adapted; see the Installation Guide for SAP SCM Optimizer at SAP Service Marketplace under Installation and Upgrade Guides SAP Business Suite Applications SAP SCM SAP SCM Server Using SAP enhancement</td>
</tr>
</tbody>
</table>
### 8.4 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For the SAP APO application, the following services are needed:

- `/default_host/sap/public/bc/icons`
- `/default_host/sap/public/bc/webdynpro`
- `/default_host/sap/public/bc/webicons`
- `/default_host/sap/xi/engine`
- `/default_host/sap/public/bc/UR`
- Service path: `/default_host/sap/bc/gui/sap/its/
  Service names: amon, amon_statist, clpglobal, clpsdp, clppromcal, clpbid, webgui`
- Service path: `/default_host/sap/bc/srt/rfc/SAPAPO/
  Service names: (All services)`
- Service path: `/default_host/sap/bc/srt/xip/SAPAPO/
  Service names: (All services)`
- Service path: `/default_host/sap/bc/srt/xip/SCMB/
  Service names: (All services)`
- Service path: `/default_host/sap/bc/webdynpro/sapapo/
  Service names: (All services)`
- Service path: `/default_host/sap/bc/webdynpro/scf/spp
  Service names: (All services spp*)`
  This service is only relevant for the SAP APO as part of SAP SCM deployment option.
- Service path: `/default_host/sap/bc/webdynpro/scmb/
  This service is only relevant for the SAP APO as part of SAP SCM deployment option.
  Service names: (All services)`

Use the transaction `SICF` to activate these services. If your firewalls use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.
For more information, see the SAP NetWeaver application help in SAP Help Portal under help.sap.com/nw75

SAP NetWeaver Library > SAP NetWeaver by Key Capability > Application Server > Application Server Infrastructure > Connectivity > Components of SAP Communication Technology > Communication Between ABAP and Non-ABAP Technologies > Internet Communication Framework - Development > Server-Side Development > Creating and Configuring ICF Services > Activating and Deactivating ICF Services

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

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

Note

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

All business data in SAP APO is stored in the system database. If SAP liveCache is used, some business data is also stored there. This business data is protected by the authorization concept of SAP NetWeaver and SAP APO.

In some special cases, business-relevant data is stored in another location, such as a file system. The special cases are listed below:

**SAP SCM Optimizer**

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

\<Drive>:\usr\sap\<SID>\<Gxx>\log (for Windows)

or

\usr\sap\<SID>\<Gxx>\log (for Linux)

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

\<GXX> = Gateway number

You must protect this folder on your server against unauthorized, third-party access.

**Using Logical Path and Filenames to Protect Access to the File System**

Scenario: Generate Characteristic Value Combinations from File

The **Generate Characteristic Value Combinations from File** scenario uses data as source in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

**Data Storage:**

The application uses characteristic value lists as a source file in the file system. The file is stored by another application or manually, and is used as a source in Characteristic Value Combination creation. Read-access for existing data is required.

**Data Protection:**

As the content of source file is displayed by the report (in case the structure of the file fits the Planning Object Structure), it is recommended to restrict the directory to be used as source to one specified for the application. To achieve this protection, specify the physical path for the logical filename /SAPAPO/FCS_CHAR_COMBIS_CREATE. Note that default settings do not protect data due to downward compatibility.

The following lists show the logical file names and paths used by the **Generate Characteristic Value Combinations from File** scenario and for which programs these file names and paths apply:
Logical File Names Used in This Scenario
The logical file name /SAPAPO/FCS_CHAR_COMBIS_CREATE has been created in order to enable the validation of physical file names.

Programs using this logical file name and parameters used in this context:
- The generated programs for CVC maintenance for the Planning Object Structure (generated out of /SAPAPO/TS_PSTRU_SAMPLE)

Parameters used in this context: N/A

Logical Path Names Used in This Scenario
The logical file names listed above all use the logical file path /SAPAPO/FCS_CHAR_COMBIS_CREATE.

Scenario: Realignment/Copy of Characteristic Value Combinations from File
The Realignment/Copy of Characteristic Value Combinations from File scenario uses data as source in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

Data Storage:
The application uses Spreadsheet with Realignment/Copy steps as a source file in the file system. The file is stored by another application or manually, and is used as a source in Characteristic Value Combination Realignment/Copy. Read-access for existing data is required.

Data Protection:
As the content of the source file can be used by the report to execute realignment/copy of characteristic-value combinations (in case the structure of the spreadsheet fits the Realignment/Copy table for the Planning Object Structure/Planning Area), it is recommended to restrict the directory to be used as source to one specified for the application. To achieve this protection, specify the physical path for the logical filename /SAPAPO/FCS_RLGCOPY.
Default settings do not protect data due to downward compatibility.

The following lists show the logical file names and paths used by the Realignment/Copy of Characteristic Value Combinations from File scenario and for which programs these file names and paths apply:

Logical File Names Used in This Scenario
The logical file name /SAPAPO/FCS_RLGCOPY has been created in order to enable the validation of physical file names.

Programs using this logical file name and parameters used in this context:
- The generated programs for Realignment for the Planning Object Structure (generated out of /SAPAPO/TS_PSTRU_SAMPLE_REALIG)

Parameters used in this context: N/A

Logical Path Names Used in This Scenario
The logical file names listed above all use the logical file path /SAPAPO/FCS_RLGCOPY.

Scenario: Generate List with TSDM Combinations
The Generate List with TSDM Combinations uses data as source in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.
Data Storage:
The application uses *Location-Products* list as a file in the file system. The file is stored at the end of the report run. Write-access to existing and non-existing data is required.

Data Protection:
As the destination file is overwritten by the report, it is recommended to restrict the directory to be used as destination to one specified for the application. To achieve this protection, specify the physical path for the logical filename `/SAPAPO/TSDM_PLOB_LIST_GENER` and/or `/SAPAPO/TSDM_PLOB_LIST_GENER_INT` (for logical filename as input). Default settings do not protect data due to downward compatibility.

The following lists show the logical file names and paths used by the *Generate List with TSDM Combinations* scenario and for which programs these file names and paths apply:

**Logical File Names Used in This Scenario**
The following logical file names have been created in order to enable the validation of physical file names:

- `/SAPAPO/TSDM_PLOB_LIST_GENER`
  Programs using this logical file name and parameters used in this context: `/SAPAPO/TSDM_PLOB_LIST_GENER`
  Parameters used in this context: N/A

- `/SAPAPO/TSDM_PLOB_LIST_GENER_INT`
  Programs using this logical file name: `/SAPAPO/TSDM_PLOB_LIST_GENER`
  Parameters used in this context: N/A

**Logical Path Names Used in This Scenario**
The logical file names listed above use the logical file paths:

- `/SAPAPO/TSDM_PLOB_LIST_GENER`
- `/SAPAPO/TSDM_PLOB_LIST_GENER_INT`

**Activating the Validation of Logical Path and File Names**
These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see:

- The SAP NetWeaver application help under [help.sap.com/nw75](http://help.sap.com/nw75) \> *SAP NetWeaver Library: Function-Oriented View* \> *Application Server* \> *Application Server ABAP* \> *Other Services* \> *Services for Application Developers* \> *Logical File Names*

- The SAP NetWeaver Security Guide under [Security Guides for SAP NetWeaver Functional Units](http://help.sap.com/saphelp_nw75/helpdata/en/aa/27e49a9e3cfb50d98c70000e71a4e7_745.html) \> *Security Guides for the Application Server* \> *SAP NetWeaver Application Server ABAP Security Guide* \> *Special Topics* \> *Protecting Access to the File System Using Logical Path and File Names*

- The SAP NetWeaver Security Guide under [Security Aspects for Lifecycle Management](http://help.sap.com/saphelp_nw75/helpdata/en/aa/27e49a9e3cfb50d98c70000e71a4e7_745.html) \> *Auditing and Logging* \> *The Security Audit Log*
10 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

**Note**

In the majority of cases, compliance with data privacy laws is not a product feature.

SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data.

SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Information about an identified or identifiable natural person.</td>
</tr>
<tr>
<td>Business purpose</td>
<td>A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.</td>
</tr>
<tr>
<td>Blocking</td>
<td>A method of restricting access to data for which the primary business purpose has ended.</td>
</tr>
<tr>
<td>Deletion</td>
<td>Deletion of personal data so that the data is no longer usable.</td>
</tr>
<tr>
<td>Retention period</td>
<td>The time period during which data must be available.</td>
</tr>
<tr>
<td>End of purpose (EoP)</td>
<td>A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorization.</td>
</tr>
</tbody>
</table>

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

- **Access control**: Authentication features as described in section *User Administration and Authentication* [external document]
- **Authorizations**: Authorization concept as described in section *Authorizations* [external document]
- **Availability control** as described in:
Section Data Storage Security [external document]

SAP NetWeaver Database Administration documentation


- Separation by purpose: Is subject to the organizational model implemented and must be applied as part of the authorization concept.

Caution

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped in Customizing for Cross-Application Components under Data Protection.

Additional industry-specific, scenario-specific or application-specific configuration might be required. For information about the application-specific configuration, see the application-specific Customizing.

10.1 Deletion of Personal Data

SAP SCM may process personal data that is subject to the data protection laws applicable in specific countries, as described in SAP Note 1825544.

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle, including the storage, retention, blocking, and deletion of data. The ERP system from which customer or vendor is transferred to SAP SCM as a location uses SAP ILM to support the deletion of personal data.

SAP delivers a where-used check (WUC) for customer/vendor locations in SAP SCM during the blocking of original customers/vendors in ERP.

All applications register in ERP either a WUC or an end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the customer and vendor master. For information about the Customizing of blocking and deletion for SAP SCM customer/vendor locations triggered from ERP, see Configuration: Simplified Blocking and Deletion section below. For SAP SCM customer/vendor locations, just the WUC is implemented.

Features

Where-Used Check (WUC)

A where-used check is a simple check to ensure data integrity in case of potential blocking. The WUC in SAP SCM checks whether any ERP customer/vendor is known to the SAP SCM system, that is to say, if it exists in table /SAPAPO/LOCMAP. If dependent data (customer/vendor location) exists, the ERP system does not block the customer/vendor master.

If you still want to block the customer/vendor data in ERP, both the location master data and all the dependent data must be deleted in SAP SCM by using the existing archiving and deletion tools or by using any other customer-specific solution.
Relevant Application Objects and Available Deletion Functionality

### Table 15

<table>
<thead>
<tr>
<th>Application</th>
<th>Detailed Description</th>
<th>Provided Deletion Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP SCM customer/vendor location</td>
<td>For more information, see SAP Help Portal at <a href="http://help.sap.com">help.sap.com</a> under <a href="http://help.sap.com">SAP Business Suite ➤ SAP ERP ➤ Security Information ➤ Security Guide</a></td>
<td>You can run the report /SAPAPO/DELETE_LOCATIONS from the <a href="http://help.sap.com">SAP Easy Access menu</a> under <a href="http://help.sap.com">SAP Menu ➤ SCM Basis ➤ Master Data ➤ Location ➤ Location select the location, then choose Extras ➤ Delete Locations</a></td>
</tr>
</tbody>
</table>

Relevant Application Objects and Available EoP/WUC Functionality

### Table 16

<table>
<thead>
<tr>
<th>Application</th>
<th>Implemented Solution (EoP or WUC)</th>
<th>Further Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP SCM customer/vendor location</td>
<td>WUC</td>
<td>WUC for table /SAPAPO/LOCMAP</td>
</tr>
</tbody>
</table>

### Process Flow

1. Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM) in ERP.

2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.

3. You do the following:
   - Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA).
   - Run transaction BUPA_PRE_EOP to enable the EoP check function for the central business partner.
   - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and vendor master in ERP (ILM objects: FI_ACCPAYB, FI_ACCRECV, FI_ACCKNVK).
   - Run transaction CVP_PRE_EOP to enable the EoP check function for the customer master and vendor master in ERP.

4. Business users can request unblocking of blocked data by using the transaction BUP_REQUEST Unblock.

5. If you have the needed authorizations, you can unblock data by running the transactions BUPA_PRE_EOP and CVP_UNBLOCK_MD.

6. You delete data by using the transaction ILM_DESTRUCTION for the ILM objects.

For information about how to configure blocking and deletion for SAP SCM customer/vendor locations transferred from ERP, see *Configuration: Simplified Blocking and Deletion* section below.

### Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of customer and vendor master data in SAP ERP Customizing, under [Logistics - General ➤ Business Partner ➤ Deletion of Customer and Vendor Master Data](http://help.sap.com)
11 Security for Additional Applications

SAP MaxDB

The SAP MaxDB Security Guide is relevant for SAP liveCache. For more information about the security of SAP MaxDB, see the SAP MaxDB Security Guide.
12 Enterprise Services Security

Note
SAP APO-specific SOA services are not part of the SAP APO add-on deployment option. They are currently only available in SAP APO as part of SAP SCM. Consider this essential point when you decide which of the two SAP APO deployments you want to use.

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

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

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

User Front End
Web Browser as a User Front End
To use the Web browser as a user front end, you must first activate JavaScript (Active Scripting), to ensure a working user interface. This could, however, conflict with your security policy regarding Web services.

SAP NetWeaver Business Client as a User Front End
For more information about SAP NetWeaver Business Client (SAP NWBC) with PFCG connection, see the SAP NetWeaver application help on SAP Help Portal at help.sap.com/nw75 SAP NetWeaver Library: Function-Oriented View Application Server Application Server ABAP UI Technologies SAP NetWeaver Business Client Security Aspects

Virus Check of Document Attachments
Use of SAP APO allows you to check documents using a virus scanner before they are uploaded to the SAP APO system.

Prerequisites
You must have a virus scanner that is correctly installed and configured.

Note
For more information, in Customizing for SAP NetWeaver, choose Application Server System Administration Virus Scan Interface
14 Security-Relevant Logging and Tracing

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

For more information about auditing and logging for the SAP SCM component, see the SAP NetWeaver Security Guide under [Security Aspects for Lifecycle Management > Auditing and Logging](#).

There are several options for auditing in SAP APO. We recommend that you use the application log in SAP APO, which you can access via transaction SLG1. For more information, see the SAP NetWeaver Security Guide under [Security Aspects for Lifecycle Management > Auditing and Logging > Logging of Specific Activities > Application Logging](#).

Security Audit Log Triggered by Virus Scan Interface (VSI)

The class CL_VSI automatically creates entries in the Security Audit Log for infections and scanned errors, with the following information:

- Profile
- Profile step allowing the detection of the scanner-group
- Kind of virus found, with internal virus ID of the scan engine, if available
- User name and timestamp

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

Audit Information System (AIS)

For more information about auditing and logging for the Audit Information System (AIS), see the SAP NetWeaver Security Guide under [Security Aspects for Lifecycle Management > Auditing and Logging > The Audit Information System (AIS)](#).
15 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.

Features

Security Chapter in the EarlyWatch Alert (EWA) Report
This service regularly monitors the Security chapter in the EarlyWatch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.
  In this case, analyze and implement the identified notes, if possible. If you cannot implement the notes, the report should be able to help you decide on how to handle the individual cases.

- Whether an accumulation of critical basis authorizations has been identified.
  In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation satisfactory, you should still check for any significant changes compared to former EWA reports.

- Whether standard users with default passwords have been identified on your system.
  In this case, change the corresponding passwords to non-default values.

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

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

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

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

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

For more 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 chapters 2.6.3, 3.6.3 and 5.6.3)
Appendix

A.1 Related Security Guides

You can find more information about the security of SAP applications on the SAP Service Marketplace at service.sap.com/security. Security guides are available at service.sap.com/securityguide.

A.2 Related Information

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

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on the SAP Service Marketplace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides</td>
<td>service.sap.com/instguides service.sap.com/ibc</td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td>service.sap.com/notes</td>
</tr>
<tr>
<td>Released platforms</td>
<td>service.sap.com/platforms</td>
</tr>
<tr>
<td>Network security</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>Technical infrastructure</td>
<td>service.sap.com/installNW70</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td>service.sap.com/solutionmanager</td>
</tr>
<tr>
<td>SAP Supply Chain Management</td>
<td>service.sap.com/scm</td>
</tr>
</tbody>
</table>