## Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Security Guide - General Concepts</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>2 Introduction</strong></td>
<td>9</td>
</tr>
<tr>
<td>2.1 Target Group of This Guide</td>
<td>9</td>
</tr>
<tr>
<td>2.2 How to Use this Guide</td>
<td>9</td>
</tr>
<tr>
<td>2.3 Using SAP Solution Manager as a Service Provider</td>
<td>10</td>
</tr>
<tr>
<td><strong>3 Overview</strong></td>
<td>11</td>
</tr>
<tr>
<td>3.1 Changes and News in General Concept: Document History</td>
<td>11</td>
</tr>
<tr>
<td>3.2 Overview: Capabilities/Functions</td>
<td>14</td>
</tr>
<tr>
<td>3.3 Overview: Solution Manager Functions Integration</td>
<td>17</td>
</tr>
<tr>
<td>3.4 Overview: Third Party Products to Be Used with Solution Manager</td>
<td>20</td>
</tr>
<tr>
<td><strong>4 Authorization Concept for SAP Solution Manager</strong></td>
<td>21</td>
</tr>
<tr>
<td>4.1 User and Roles Concept in SAP Solution Manager</td>
<td>21</td>
</tr>
<tr>
<td>4.2 PFCG Roles Types Delivered in SAP Solution Manager</td>
<td>26</td>
</tr>
<tr>
<td>4.3 Authorization Object Classes</td>
<td>29</td>
</tr>
<tr>
<td>4.4 Authorization Object Status in Roles</td>
<td>30</td>
</tr>
<tr>
<td>4.5 Authorizations and Roles for Infrastructure</td>
<td>31</td>
</tr>
<tr>
<td>4.6 User Interfaces in SAP Solution Manager</td>
<td>36</td>
</tr>
<tr>
<td>4.7 Guided Procedure Framework</td>
<td>49</td>
</tr>
<tr>
<td>4.8 Using SAP Solution Manager with Java Stack</td>
<td>50</td>
</tr>
<tr>
<td>4.9 Using SAP Solution Manager with Customer Relationship Management (CRM)</td>
<td>50</td>
</tr>
<tr>
<td>4.10 Using SAP Solution Manager with Business Warehouse (BW)</td>
<td>53</td>
</tr>
<tr>
<td>4.11 Using the Help Center</td>
<td>61</td>
</tr>
<tr>
<td>4.12 Critical SAP BASIS Authorization Objects</td>
<td>61</td>
</tr>
</tbody>
</table>

*Note: The table includes page numbers for each section.*
Function Calls: Authorization Object S_RFC and S_DEV_REMO. ............................................. 63
Table Maintenance: Authorization Objects S_TABU_DIS, S_TABU_NAM, and S_TABU_CLI. .............. 64
ABAP Objects: Authorization Object S_DEVELOP. ................................................................. 68
Start Authorization Objects S_START, S_TCODE, and S_SERVICE. ........................................ 69
4.13 Authorization Object SM_SETUP. ..................................................................................... 72
4.14 How to Build Your Own Authorization Concept. .............................................................. 72
4.15 Creating Configuration User Roles for SAP Solution Manager Using IMG Project. ............ 73
1 Security Guide - General Concepts

Use

⚠️ Caution

Usage Rights for SAP Solution Manager

For Usage Rights, check the following information in the Service Marketplace at: [http://support.sap.com/solution-manager/usage-rights.html](http://support.sap.com/solution-manager/usage-rights.html)


For any issues with security, authorizations, roles, and user management for SAP Solution Manager use SV-SMG-AUT.

⚠️ Caution

Before you start the implementation and configuration of SAP Solution Manager, make sure you have the latest version of this document. You can find the latest version at the following location: [http://service.sap.com/instguides/SAP Components > SAP Solution Manager > <current release>](http://service.sap.com/instguides/SAP Components > SAP Solution Manager > <current release>)

The following table provides an overview of the most important document changes.
Table 1:

<table>
<thead>
<tr>
<th>Support Package Stacks (Version)</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| SP01                            | 2015 / 12 / 11 | **General Information**<br>● As of Release 7.2, the security information is published within four separate guides:<br>○ SAP Solution Manager Authorization Concept<br>   This guide contains all information referring to the general concept of security and authorizations for the complete stack for SAP Solution Manager.<br>○ SAP Solution Manager Secure Configuration Guide<br>   This guide contains all information referring to security aspects, users, User Management, authorizations, Role Management used in transactions SOLMAN_SETUP and SMUA. In addition, users and authorization for the migration procedure for the process documentation are included.<br>○ SAP Solution Manager Application Security Guide<br>   This guide contains all information referring to security aspects and authorizations for individual scenarios/applications.<br>**New Process Documentation Functionality**<br>○ Obsolete Transactions and Authorizations<br>Transactions SOLAR01, SOLAR02, SOLAR_PROJECT_ADMIN are obsolete. All relevant authorizations and roles are obsolete. New roles are delivered SAP_SM_SL_* (process documentation) and SAP_SM_KW_* (Document Management). For more information, see sections on Authorization and Roles for Infrastructure and Process Documentation (see Application - Specific Guide).<br>○ All formerly relevant authorization objects for Process Documentation are contained in roles SAP_SOLPRO_OLD with full authorization and SAP_SOLPRO_DISP_OLD with display authorization.<br>○ Solution Content Activation (Migration) Information<br>Information on the migration of existing projects and solutions to the new process documentation functionality is given in the Landscape Setup Guide: Secure Configuration.<br>**Work Center Role Navigation Concept**<br>○ All roles SAP_SMWORK_BASIC_* are obsolete, see sections on Work Center Navigation Roles and Authorizations for User Interfaces..<br>○ All single roles calling ABAP WebDynpro Application receive new start transaction authorization object $START, due to new SAP Basis Release 7.40, see section on User Interface Authorizations.<br>**Authorization Object Status**<br>○ New section describing authorization objects status in role for SAP Solution Manager (Software Component ST)<br>**Critical Authorization Objects**<br>○ extension of existing sections on SAP_BASIS authorization objects
<table>
<thead>
<tr>
<th>Support Package Stacks (Version)</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>○ additional section on Solution Manager authorization object <strong>SM_SETUP</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ <strong>SAP Fiori User Interface / NWBC</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP Fiori User Interface can be used with SAP Solution Manager, see section on <strong>User Interfaces in SAP Solution Manager</strong>. The Fiori Launchpad can be called from the My Home work center. Assign role <strong>SAP_SMWORK_MYHOME</strong> to your respective users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Some scenarios, such as <strong>ITPPM</strong>, require NWBC as a User Interface in addition to SAP Fiori Launchpad and Tiles. The transaction is included in role <strong>SAP_SM_FIORI_LP_EMBEDDED</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Section: Authorizations and Roles for Infrastructure</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Authorization object <strong>AI_LMDB_PS</strong> is obsolete, and only included in roles <strong>SAP_SYSTEM_REPOSITORY_</strong>* with <strong>ACTVT 03 (Display)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Information on <strong>Embedded Search</strong> functionality, (used in a number of scenarios)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Dashboard Builder</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>● New framework for Dashboards delivered and new roles for it, see section Using SAP Solution Manager with Business Warehouse (BW).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following roles as of Release 7.1 are obsolete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ <strong>SAP_SM_DASHBOARDS_DISP_ALM</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ <strong>SAP_SM_DASHBOARDS_DISP_CIO_BPO</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ <strong>SAP_SM_DASHBOARDS_DISP_EEM</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ <strong>SAP_SM_DASHBOARDS_DISP_LMDB</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ <strong>SAP_SM_DASHBOARDS_DISP_SAM</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ <strong>SAP_SM_DASHBOARDS_DISP_VBD</strong></td>
</tr>
</tbody>
</table>

| SP02                            |      | **SAP Fiori User Interface** |
|                                 |      | ● added information in regards to **VSCAN** Documentation for upload of data. |
## Integration

Security topics are relevant for the following phases:

- Installation and Upgrade
- Configuration
- Operation

**Recommendation**

Use this guide during all phases. For a detailed overview of which documentation is relevant for each phase, see guides reference on the Service Marketplace at: [http://service.sap.com/instguides](http://service.sap.com/instguides) ➔ SAP Components ➔ SAP Solution Manager 7.2 ➔
More Information

For a complete list of the available SAP Security Guides, see the SAP Service Marketplace: http://service.sap.com/securityguides
2 Introduction

2.1 Target Group of This Guide

The purpose of SAP Solution Manager is to provide an implementation and administration environment to allow for better managing your systems and business processes in a transparent way.

The target groups of this guide are readers who are familiar with SAP Solution Manager and configuration procedures in an implementation or upgrade project, that is technical consultants, system administrators or application consultants.

- **Technology Consultants**
  They work with technical processes supported by SAP software during implementation, when deciding which settings to make.

- **System Administrators**
  They optimize the SAP Solution Manager system during and after implementation.

- **Application Consultants**
  They map a company’s actual business processes to the processes and functions supported by SAP software during implementation, and when deciding which settings to make.

- **SAP Security Professionals**
  They secure the system landscape settings.

2.2 How to Use this Guide

Setting up an authorization concept for your own company for SAP Solution Manager is not simple. It requires approaching the topic from a technical as well as content-oriented perspective.

Authorizations are strongly tied to configuration topics for certain scenarios, as well as security relevant technical information. The knowledge for these sectors is seldom found within one department, as technical and application components must be aligned for a successful concept. Especially with SAP Solution Manager this is important, as the product is aimed at the support for the life-cycle of systems (maintained by technical staff), but also the life-cycle of solutions (maintained by application-oriented staff).

Therefore, as described in the former section, this guide is directed to differing groups with different focus on SAP Solution Manager. These groups can be organizationally divided.

This guide addresses the resulting differing ways of approaching authorizations and their maintenance from a content-oriented view (for instance application consultant), and a technically oriented view (for instance system administrator).

➤ Recommendation

To set up a stable authorization concept, both views are to be considered, and involved.
The following sections give you a short guidance to how to use this guide, depending on your main tasks when setting up an authorization concept or authorization roles for SAP Solution Manager.

How to use the guide from a content-oriented perspective

What do we mean by content-oriented perspective? The SAP Solution Manager is an SAP product that supports your business. Roles and authorization objects are delivered to allow your end-users to work within the limits of their tasks. In other words, they should only be allowed to execute and see what they need in their daily work. These tasks depend on your specific business processes. As a logical consequence, the authorizations and roles assigned to your users depend heavily on the business processes you deploy, and are depending on the configuration of your system accordingly. The concept of your configuration needs to be considered for the concept of your authorizations. Although we deliver template roles for your use, they can hardly ever be applied without modification to your business. Therefore, before tailoring authorizations or using SAP template roles, you need to consider your business processes, the content of your business.

If you are already acquainted with the authorization concept in SAP Solution Manager, we strongly recommend to read the Document History for changes in roles and authorization objects, and in addition the Operations Guide for SAP Solution Manager on the Service Marketplace at: http://service.sap.com/instguides

2.3 Using SAP Solution Manager as a Service Provider

As a service provider, you provide services to your customers or subsidiaries using SAP Solution Manager. The service-provider scenario extends the standard scenario setup for specific customer contexts, for example special data separation and master data import.

If you use your SAP Solution Manager application for one of the above mentioned contexts, you can use it as a service provider scenario. For this purpose, you also need to add some additional configuration and specific authorizations for you, as the service provider, and your customers or subsidiaries.

For more information on the service provider scenario and definition, see https://support.sap.com/solution-manager/partners/sp.html.
3 Overview

3.1 Changes and News in General Concept: Document History

⚠️ Caution

Before you start the implementation and configuration of SAP Solution Manager, make sure you have the latest version of this document. You can find the latest version at the following location: [http://service.sap.com/instguides](http://service.sap.com/instguides) > SAP Components > SAP Solution Manager > <current release>

The following table provides an overview of the most important document changes.
Table 2:

<table>
<thead>
<tr>
<th>Support Package Stacks (Version)</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP01</td>
<td>2015 / 11</td>
<td>General Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- As of Release 7.2, the security information is published within four separate guides:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP Solution Manager Authorization Concept</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This guide contains all information referring to the general concept of security and authorizations for the complete stack for SAP Solution Manager.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP Solution Manager Secure Configuration Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This guide contains all information referring to security aspects, users, User Management, authorizations, Role Management used in transactions SOLMAN_SETUP and SMUA. In addition, users and authorization for the migration procedure for the process documentation are included.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP Solution Manager Application Security Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This guide contains all information referring to security aspects and authorizations for individual scenarios/applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New Process Documentation Functionality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Obsolete Transactions and Authorizations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transactions SOLAR01, SOLAR02, SOLAR_PROJECT_ADMIN are obsolete. All relevant authorizations and roles are obsolete. New roles are delivered SAP_SM_SL_* (process documentation) and SAP_SM_KW_* (Document Management). For more information, see sections on Authorization and Roles for Infrastructure and Process Documentation (see Application - Specific Guide).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ All formerly relevant authorization objects for Process Documentation are contained in roles SAP_SOLPRO_OLD with full authorization and SAP_SOLPRO_DISP_OLD with display authorization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Solution Content Activation (Migration) Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information on the migration of existing projects and solutions to the new process documentation functionality is given in the Landscape Setup Guide: Secure Configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Work Center Role Navigation Concept</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ All roles SAP_SMWORK_BASIC_* are obsolete, see sections on Work Center Navigation Roles and Authorizations for User Interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ All single roles calling ABAP WebDynpro Application receive new start transaction authorization object S_START, due to new SAP Basis Release 7.40, see section on User Interface Authorizations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authorization Object Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ New section describing authorization objects status in role for SAP Solution Manager (Software Component ST)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical Authorization Objects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ extension of existing sections on SAP_BASIS authorization objects</td>
</tr>
<tr>
<td>Support Package Stacks (Version)</td>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ additional section on Solution Manager authorization object SM_SETUP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP Fiori User Interface / NWBC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP Fiori User Interface can be used with SAP Solution Manager, see section on User Interfaces in SAP Solution Manager. The Fiori Launchpad can be called from the My Home work center. Assign role SAP_SMWORK_MYHOME to your respective users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Some scenarios, such as ITPM, require NWBC as a User Interface in addition to SAP Fiori Launchpad and Tiles. The transaction is included in role SAP_SM_FIORI_LP_EMBEDDED.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Section: Authorizations and Roles for Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Authorization object AI_LMDB_PS is obsolete, and only included in roles SAP_SYSTEM_REPOSITORY_* with ACTVT 03 (Display)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Information on Embedded Search functionality, (used in a number of scenarios)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dashboard Builder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● New framework for Dashboards delivered and new roles for it, see section Using SAP Solution Manager with Business Warehouse (BW).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following roles as of Release 7.1 are obsolete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP_SM_DASHBOARDS_DISP_ALM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP_SM_DASHBOARDS_DISP_CIO_BPO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP_SM_DASHBOARDS_DISP_EEM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP_SM_DASHBOARDS_DISP_LMDB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP_SM_DASHBOARDS_DISP_SAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ SAP_SM_DASHBOARDS_DISP_VBD</td>
</tr>
<tr>
<td>SP02</td>
<td></td>
<td>SAP Fiori User Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● added information in regards to VSCAN Documentation for upload of data.</td>
</tr>
<tr>
<td>Support Package Stacks (Version)</td>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SP03                           | 2016 / 08 / 15 | **SAP Fiori User Interface**  
  added information in regards to:  
  ● calling an application independently  
  ● refinement of SAP Fiori tile groups for specific purposes  
  ● adding additional SAP Fiori relevant services  
  **Guided Procedure Framework**  
  Adapted role SAP_SM_GP_ADMIN (new transaction DSWP_GPC_FAR):  
  **Authorization and Roles for Infrastructure**  
  ● Added information regarding Digital Signature for Test Plan Management.  
  **Default Users Created in Earlier Releases**  
  Please check passwords for default users created within transaction SOLMAN_SETUP in earlier releases. See SAP Note 2293011.  
  **Dashboard Builder Framework**  
  ● reduced role scope from separate application specific dashboard builder roles to one display Dashboard role for all applications. In case you want to minimize authorizations, see according section for Dashboard Builder. |
| SP04                           | 2016 / 12 / 19 | **SAP Notes**  
  2250709 - Solution Manager 7.2: Roles and Authorizations Corrections as of SP01 and higher |

### 3.2 Overview: Capabilities/Functions

The following table gives you an overview over the functions covered in this guide and which work center/ scenario/specific guide they belong to.

<table>
<thead>
<tr>
<th>Specific Functions</th>
<th>Work Center / Scenario/Specific Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>System, Host, Database Monitoring</td>
<td>Technical Monitoring (Application Operation)</td>
</tr>
<tr>
<td>Specific Functions</td>
<td>Work Center / Scenario/Specific Guide</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>PI Monitoring</td>
<td></td>
</tr>
<tr>
<td>BI and HANA Monitoring</td>
<td></td>
</tr>
<tr>
<td>End-User Experience Monitoring</td>
<td></td>
</tr>
<tr>
<td>Channel Monitoring</td>
<td></td>
</tr>
<tr>
<td>Self Monitoring</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Monitoring</td>
<td></td>
</tr>
<tr>
<td>Message Flow Monitoring</td>
<td></td>
</tr>
<tr>
<td>BI - Reporting</td>
<td>Technical Monitoring</td>
</tr>
<tr>
<td></td>
<td>Test Management</td>
</tr>
<tr>
<td></td>
<td>Incident Management</td>
</tr>
<tr>
<td></td>
<td>Solution Manager Administration</td>
</tr>
<tr>
<td></td>
<td>Business Process Operations</td>
</tr>
<tr>
<td></td>
<td>Change Management / Change Request Management</td>
</tr>
<tr>
<td></td>
<td>DVM</td>
</tr>
<tr>
<td>Project Management</td>
<td>Implementation and Upgrade</td>
</tr>
<tr>
<td></td>
<td>Solution Manager Administration</td>
</tr>
<tr>
<td></td>
<td>Change Request Management</td>
</tr>
<tr>
<td>Road Maps</td>
<td>Implementation and Upgrade</td>
</tr>
<tr>
<td>Process Documentation</td>
<td>Change Request Management</td>
</tr>
<tr>
<td>Business Functions</td>
<td></td>
</tr>
<tr>
<td>Customizing Distribution</td>
<td></td>
</tr>
<tr>
<td>BC-Set Activities</td>
<td></td>
</tr>
<tr>
<td>Help Center</td>
<td></td>
</tr>
<tr>
<td>Learning Maps</td>
<td></td>
</tr>
<tr>
<td>Digital Signature</td>
<td></td>
</tr>
<tr>
<td>Document Management</td>
<td>Implementation and Upgrade</td>
</tr>
<tr>
<td></td>
<td>Test Management</td>
</tr>
<tr>
<td></td>
<td>Change Management / Change Request Management</td>
</tr>
<tr>
<td>Specific Functions</td>
<td>Work Center / Scenario/Specific Guide</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Test Automation</td>
<td>Test Management</td>
</tr>
<tr>
<td>Test Plans, Test Packages</td>
<td></td>
</tr>
<tr>
<td>Test Information</td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td></td>
</tr>
<tr>
<td>Test Workbench Workflow</td>
<td></td>
</tr>
<tr>
<td>Extended Capabilities</td>
<td></td>
</tr>
<tr>
<td>TBOMs</td>
<td>Test Management / Business Process Change Analyzer</td>
</tr>
<tr>
<td>Change Analyzer</td>
<td>Test Management / Business Process Change Analyzer</td>
</tr>
<tr>
<td>Incident Management</td>
<td>Incident Management</td>
</tr>
<tr>
<td>Job Management</td>
<td>Job Management</td>
</tr>
<tr>
<td>Issue Management</td>
<td>SAP Engagement and Service Delivery</td>
</tr>
<tr>
<td>Support Requests</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td></td>
</tr>
<tr>
<td>Expert on Demand</td>
<td></td>
</tr>
<tr>
<td>Service Level Reporting</td>
<td></td>
</tr>
<tr>
<td>Security Optimization Service</td>
<td></td>
</tr>
<tr>
<td>Early Watch Alert (SDCCN)</td>
<td>SAP Engagement and Service Delivery</td>
</tr>
<tr>
<td></td>
<td>Root Cause Analysis (Landscape Setup Guide)</td>
</tr>
<tr>
<td>Work Mode Management</td>
<td>Technical Administration</td>
</tr>
<tr>
<td>MDM Administration Cockpit</td>
<td></td>
</tr>
<tr>
<td>Notification Management</td>
<td></td>
</tr>
<tr>
<td>IT Calendar</td>
<td></td>
</tr>
<tr>
<td>IT Event</td>
<td></td>
</tr>
<tr>
<td>IT Task Inbox</td>
<td></td>
</tr>
<tr>
<td>IT Task Planner</td>
<td></td>
</tr>
<tr>
<td>Service Availability Management</td>
<td></td>
</tr>
</tbody>
</table>
### Guided Procedure

<table>
<thead>
<tr>
<th>Guided Procedure</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross - Database Comparison</td>
<td>Business Process Operations</td>
</tr>
<tr>
<td>Business Process Monitoring</td>
<td></td>
</tr>
<tr>
<td>Business Process Analytics</td>
<td></td>
</tr>
<tr>
<td>Change Request Management</td>
<td>Change Management</td>
</tr>
<tr>
<td>cProjects</td>
<td>Implementation</td>
</tr>
<tr>
<td>Retrofit</td>
<td>Quality Gate Management</td>
</tr>
<tr>
<td>Configuration Validation</td>
<td></td>
</tr>
<tr>
<td>System Recommendation</td>
<td></td>
</tr>
<tr>
<td>Quality Gate Management</td>
<td>Quality Gate Management</td>
</tr>
<tr>
<td>Data Volume Management</td>
<td>Data Volume Management</td>
</tr>
<tr>
<td>Measurement Platform</td>
<td>Measurement Platform</td>
</tr>
<tr>
<td>Custom Code Life - Cycle Management</td>
<td>Custom Code Life - Cycle Management</td>
</tr>
<tr>
<td>Custom Code Analysis</td>
<td></td>
</tr>
<tr>
<td>CBTA</td>
<td>Test Management / Business Process Change Analyzer</td>
</tr>
</tbody>
</table>

### 3.3 Overview: Solution Manager Functions Integration

This section gives you an overview about integration of functions. Only those functions are listed which rely on cross-work center usage.

More details are described in the scenario-specific guides.

**How to read the table**

The header determines in which function the integration is placed. For instance, the integration of TBOMs into Business Blueprint/Configuration can be done in transaction SOLAR01/02. In this case read: Header Line for Business Blueprint/Configuration number 1 and check the integration with vertical number for Business Process Change Analyzer number 7.

1. Process Management
2. CDMC
3. Customizing Distribution
4. Document Management
5. Alert Inbox
6. Project Management  
7. Business Process Change Analyzer  
8. Incident Management  
9. Issue Management  
10. Test Management  
11. Business Process Monitoring  
12. Change Request Management  
13. Job Management  
14. SAP Engagement and Service Delivery  
15. Root Cause Analysis  
16. Technical Monitoring  
17. Notification Management (Instant Notification)  
18. Quality Gate Management  
19. Configuration Validation  
20. Data Volume Validation  
21. Exception Management  
22. Guided Procedure Browser  
23. CBTA  
24. cProject  
25. IT Calendar  
26. Message Flow Monitoring  
27. Work Mode Management  
28. Service Availability Management  
29. BI Reporting  
30. Dashboards

|   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | X | X | X | X | X | X | X | X | X | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 2 | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 3 | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 4 | X |    | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 5 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 6 | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 7 | X |    | X |    | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 8 | X |    | X |    | X | X | X | X | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 9 | X |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
3.4 Overview: Third Party Products to Be Used with Solution Manager

In this section you find an overview over Third Party Integration with individual scenarios. For more details see the scenario-specific guide section *External Integration*. For more information on security for external tools, see the according documentation for the tool.

1. Implementation
2. Incident Management
3. Test Management (Partner Test Management)
4. Business Process Change Analyzer
5. Job Management

Table 5:

| Business Process Management Suite (NW CE) | X |
| Enterprise Service Repository (PI)       | X |
| SAP Productivity Pak by RWD              | X |
| Service Desk                             | X |
| HP QC                                    | X |
| ECatt                                    | X |
| Test Tools                               | X |
| IBM Rational Test Management Tool        | X |
| SAP TAO                                  | X |
| SAP CPS                                  | X |
4 Authorization Concept for SAP Solution Manager

4.1 User and Roles Concept in SAP Solution Manager

SAP User Definitions

Within the context of business processes users are relevant. These users represent human users within a business scenario, who are mapped in a system such as SAP Solution Manager by a user ID, in transaction SU01 (User Management). Each user in a business scenario has specified tasks to execute. These may vary from company to company. For instance, in a financial environment you find accountants and controllers.

These user definitions do not contain the full range of functions which are possible for one scenario, but rather the Core Business.

Example

For instance, using Process Documentation requires a specific number of roles to execute the main transactions/applications which are absolutely necessary for the process, such as Project administration, Document Management, and so on.

Using SAP Solution Manager, a number of business scenarios exist; see Application - Specific Guides. Therefore, we deliver defined users for explicit tasks.

Example

For instance, in Incident Management you always have a number of so called key users, users in business systems who create messages for errors or insufficient functions within the systems they are working in. In addition, we have a so called processor who solves the Incident messages or sends them to SAP for solving. This business process and the according user definition is clearly defined.

Due to these user definitions it is possible to deliver according authorization roles, which map the defined tasks. This is done for all scenarios and user definitions within SAP Solution Manager. Therefore, in the application - specific guides, you find a chapter for user definitions and their according user roles as defined by SAP. The user definitions delivered cannot display the business as done by varying companies. Therefore, the user definitions as well as the user roles can only be regarded as templates for your own authorization concepts.
**User Differentiation**

Considering SAP Solution Manager as a management platform for other systems (system landscape), and business solutions (application cycle), we differentiate between users, who:

1. **configure** the SAP Solution Manager scenario, see section *Configuration Users in SAP Solution Manager*
2. **administer** the SAP Solution Manager system itself
3. **use** SAP Solution Manager to manage other systems

This differentiation of tasks can overlap. For instance, the user responsible for the setup, administration, and operation of the SAP Solution Manager system may also be able to administer other systems in the landscape. Another user may only be responsible for the configuration of one of the systems in the landscape:

- **Configuration of SAP Solution Manager**
  The user responsible for the tasks area of setup and configuration is called SAP Solution Manager Configuration User, with User ID by default `SOLMAN_ADMIN`. This user is first created during the automated basic settings configuration via transaction `SOLMAN_SETUP`. We differentiate between different roles for this user when setting up the *basic system landscape*, and roles for *scenario-specific setup*. During automated basic setup (in transaction `SOLMAN_SETUP` or SAP Solution Manager configuration work center) the Solution Manager configuration user is authorized to automatically create users and assign roles. Due to the automatic assignment, the authorization values in these roles are delivered with predefined authorization values. *All* fields which could not be determined by SAP, because they can only be restricted to certain values by the customers, are delivered with value ‘*’ (asterisks defines full authorization). If you want to restrict authorizations during setup, you need to do this manually.

  ➤ **Recommendation**
  
  We recommend using the delivered Standard SAP roles as displayed in the User Interface by the guided procedure in the system.

  ➤ **Note**
  
  Roles for scenario-specific configuration in transaction `SPRO` are not delivered. For these configurations, we recommend creating so called configuration roles from projects. The procedure is described in the *How-To Document* on how to create configuration users in this guide. Alternatively, you can use SAP profiles `SAP_ALL` and `SAP_NEW`.

- **Administration of SAP Solution Manager**
  To be able to administer SAP Solution Manager, you need to assign roles for the Solution Manager Administration Work Center to your user `SAP_SOLMAN_ADMIN_COMP`, see also section on Solution Manager Administration in the application specific guide. There are specific administration users for the scenario-specific setup in transaction `SOLMAN_SETUP`.

  ➤ **Note**
  
  You can use default user `SOLMAN_ADMIN` also for administration when adding the above mentioned role. Nevertheless, we recommend to have a separate user for administration.

- **End - Users of SAP Solution Manager**
  For each scenario, we deliver user definitions and according composite roles with the technical name ending `*_COMP` according to the principle of Segregation of Duty. For each scenario more than one user definition is
delivered. There is always a user with full administration authorization and a user with display authorization delivered (see section Multilevel Separation).

Composite Roles

According to the user definitions, composite roles are shipped, which contain all relevant single roles needed to fulfil the required tasks.

All delivered composite roles contain an appropriate number of single roles. The single roles represent individual functions in the system (see section Modular Separation). Software Components (see section Software Component Separation), whereas these two overlap in most cases. A further differentiation relates to the roles usage as defining the navigation and related authorizations (see section Navigation/UI/Backend Separation). This definition can vary according to your own needs. Therefore, all roles shipped by SAP are only template roles for you to copy and adapt.

- Business Core Roles = ST related roles for business tasks (scenario-related)
- Technical Authorization Roles = ST related authorization roles for technical frameworks like Extractor Framework, and so on
- CRM roles = roles related to CRM 7.01
- Reporting roles = roles related to BW - reporting
- Navigation Roles = role related to the User Interface
- J2EE roles = related to Java Stack authorizations

All roles are delivered in the SAP name space starting with SAP_. The technical role name represents the scenario it is used for, the level of authorizations it contains, and the technical information whether it is a composite role or a single role. For instance, the technical role name SAP_SUPPDESK_PROCESS_COMP represents the following information: It is delivered by SAP <SAP>, used for scenario Incident Management <SUPPDESK>, user definition is processor <PROCESS>, and it is the composite role <COMP>.

The following sections explain in more detail the multilevel segregation, the module/software component segregation, and navigation/UI/back-end separation for all roles:

Caution

The composite roles are not shipped with a menu included. If more than one navigation role is contained in such a composite role, the system cannot handle both navigation structures and can only display the first navigation role in the list. For more information, see SAP Note 1246860.

Multilevel Separation

The principle of Segregation of Duty requires that each user in a system has exactly the authorizations he/she requires for the tasks they are to execute. In this respect, we deliver according single roles.

The definition of the users varies from scenario to scenario. All roles are built on top of each other. This means, that the authorizations for a display user are included in the authorizations for an operations user, and in turn the authorizations for the operations user are included in the authorizations for the administration user.
Example

For instance, in Technical Administration a user may be required, who has authorizations for all system administration tasks with technical name *ADMIN* in addition to a display user. In Incident Management or Change Request Management, the scenario is defined by a sequential process, a key user creates incidents, a processor processes the incidents, and an administrator is allowed to create business partners and other configuration tasks. Here, the roles are defined for the user purpose, for instance with the technical role name *PROCESS*.

Module Separation

SAP Solution Manager roles are composite roles, which contain a number of single roles, which easily allow a further restriction of authorizations for a user. Each single role defines the authorization for one specific function/module/transaction. The composite roles then contain all relevant authorization for one user in a scenario. This may include roles for work center navigation, work center authorization, BW-related authorizations, CRM-related authorizations, function-related authorizations, and so on. The composite roles can therefore be easily extended or reduced with authorizations. The clear demarcation simplifies the role maintenance and prevents the unintentional assignment of authorizations that are not required.

Example

Even though, some authorization objects may appear in more than one single role in different scenarios, see section Integration of Functions/Capabilities. They are then maintained only for the purpose within the scenario.

In the case of composite role SAP_SUPPDESK_PROCESS_COMP for Incident Management, role:

- **SAP_BI_E2E** contains all authorization for BW activation
- **SAP_SUPPDESK_PROCESS** contains all authorization to run the application as a processor in SAP Solution Manager
- **SAP_SMWORK_*** contain UI access information to run the work center
- **SAP_SM_CRM_UIU_*** contain all authorizations to run the application in the new CRM WebClient UI
- **SAP_SM_FIORI_LP_EMBEDDED** contains all UI access information for Embedded Fiori Launchpad

Software Component Separation

SAP Solution Manager uses in its applications a variety of different Software Components, which also demand a mapping in the authorization concept. Therefore, we differentiate between them by defined single roles, for instance BW-related roles contain BW-related authorization objects, because they are delivered with Software Component ST-BCO. The following Software Components are used within SAP Solution Manager:

- **SAP BASIS**
- **CRM**
- **ST-BCO**
As of SP02, authorization roles for BW - reporting for SAP Solution Manager are delivered in Software Component ST-BCO (before BI_CONT).

- ST
- ST-PI
- ST-UI
- ST-A/PI
- ST-ICC
- ST-TST

Example

For instance, a clear-cut differentiation between roles for BW is necessary due to the possibility to run BW in different scenarios. Depending whether the BW runs in SAP Solution Manager or separate, roles must be assigned to users. For this to be realized, some roles must be deliverable for BW systems, which can deploy software component ST-BCO. Therefore, roles for BW - reporting that must be present in a remote BW system are delivered with ST-BCO. Roles which are relevant for BW - reporting in the SAP Solution Manager system, for instance for displaying BW - reports, are delivered with software component ST.

These roles can be present in one composite role.

In the case of composite role SAP_SUPPDESK_PROCESS_COMP in Incident Management, roles:

- **SAP_BI_E2E** for BW activation is delivered with ST-BCO
- **SAP_SM_CRM_UIU_*** are relevant for CRM component CRM WebClient UI, delivered with ST
- **SAP_SUPPDESK_PROCESS** and **SAP_SMWORK_*** are relevant for SAP Solution Manager component delivered with ST

For more information, see sections on Using SAP Solution Manager with CRM and Using SAP Solution Manager with BW in this guide.

Navigation/UI/Backend

Due to the use of different clients and the concept of work centers (and SAP NWBC, SAP Fiori), we differentiate between navigation roles and back-end roles, which contain authorizations. For more information, see section on Work Center Navigation Role Concept. In this respect, we consider User Interface authorizations separately. For more information, see section Authorization for User Interfaces.

In the case of composite role SAP_SUPPDESK_PROCESS_COMP in Incident Management, roles:

- **SAP_BI_E2E**, **SAP_SUPPDESK_PROCESS** contain back-end authorizations
- **SAP_SMWORK_INCIDENT_MAN**, **SAP_SM_CRM_UIU_SOLMANPRO** are navigation roles for work center and CRM WebClient UI. These roles contain no authorization objects and are solely defined by their menu.
- **SAP_SM_CRM_UIU_SOLMANPRO_PROC**, **SAP_SM_CRM_UIU_FRAMEWORK** are UI roles and contain authorization objects which define the UI for the work center and the CRM WebClient UI.
- **SAP_SM_FIORI_LP_EMBEDDED** contains all UI access information for Embedded Fiori Launchpad.
4.2 PFCG Roles Types Delivered in SAP Solution Manager

Infrastructure Roles

Infrastructure Authorization Roles are all roles which contain authorization objects for specific functions that are relevant for all scenarios or at least many scenarios in SAP Solution Manager, such as LMDB (Technical Systems), Process Documentation, Users, RFCs, or Business Partners. For more information, see section Authorizations and Roles for Infrastructure.

Example

The role(s) that are meant are highlighted.

Composite Role: SAP_SUPPDESK_PROCESS_COMP

Single Roles:
- SAP_SMWORK_INCIDENT_MAN
- SAP_SM_BI_INCMAN_REPORTING
- SAP_SM_CRM_UIU_FRAMEWORK
- SAP_SM_CRM_UIU_SOLMANPRO
- SAP_SM_CRM_UIU_SOLMANPRO_PROC
- SAP_SUPPDESK_PROCESS
- SAP_SM_FIORI_LP_EMBEDDED
- SAP_SM_SL_DISPLAY

Core (Business) Roles

To run an application, a user needs to have a large number of varying authorization objects assigned to, which can belong to basic functions or infrastructure functions, and also specific to the application that is run. Each scenario in SAP Solution Manager contains a number of authorization objects which are only specific for the application. These specific authorization objects are contained in specific core roles. Core roles are those single roles in a composite role which contain the authorization objects that are only relevant for the application. These roles are roles containing authorization objects, therefore they need to be copied into your name space.

Example

The role(s) that are meant are highlighted.

Composite Role: SAP_SUPPDESK_PROCESS_COMP

Single Roles:
- SAP_SMWORK_INCIDENT_MAN
- SAP_SM_BI_INCMAN_REPORTING
- SAP_SM_CRM_UIU_FRAMEWORK
Navigation Roles for Work Center, NWB, and SAP Fiori

Work Centers have a specific navigation bar and specific views. These User Interface navigations are controlled by coding and a specific role. Without assigning the navigation role for Work Centers to the user, the user is not allowed to access the Work Center. All Work Center navigation roles have the following naming convention: `SAP_SMWORK_<WorkCenter>`. As navigation roles are simply defining navigation possibilities, the roles do not contain any relevant authorization objects, and should not be copied into a separate name space. For more information on User Interface authorization, see section Authorizations for User Interfaces.

**Example**

The role(s) that are meant are highlighted.

**Composite Role:** SAP_SUPPDESK_PROCESS_COMP

**Single Roles:**
- SAP_SMWORK_INCIDENT_MAN
- SAP_SM_BI_INCMAN_REPORTING
- SAP_SM_CRM_UIU_FRAMEWORK
- SAP_SM_CRM_UIU_SOLMANPRO
- SAP_SM_CRM_UIU_SOLMANPRO_PROC
- SAP_SUPPDESK_PROCESS
- SAP_SM_SL_DISPLAY
- SAP_SM_FIORI_LP_EMBEDDED

Navigation Roles for CRM WebClient

Similar to work centers, the CRM WebClient has a specific navigation bar and specific views, and are therefore controlled by a specific role. Without assigning the navigation role for the CRM WebClient to the user, the user is not allowed to access the CRM WebClient. All CRM WebClient navigation roles have the following naming convention: `SAP_SM_CRM_UIU_<SOLMANPRO, SOLREQUEST...>`. As navigation roles are simply defining navigation possibilities, the roles do not contain any relevant authorization objects, and should not be copied into a separate name space. For more information on CRM integration, see section Using SAP Solution Manager with Customer Relationship Management (CRM).

**Example**

The role(s) that are meant are highlighted.
UIU_COMP Authorization Roles

The CRM WebClient is controlled by a specific User Interface authorization object UIU_COMP with profiles. The default authorization objects for the overall frame used are contained in role SAP_SM_CRM_UIU_FRAMEWORK. Any additional profiles of this authorization object, which are needed for specific navigation purposes are contained in a separate “delta” role with the naming convention SAP_SM_CRM_UIU***. These roles are roles containing authorization objects, therefore they need to be copied into your name space. For more information on User Interface authorization, see section Authorizations for User Interfaces.

Example

The role(s) that are meant are highlighted.

Composite Role: SAP_SUPPDESK_PROCESS_COMP

Single Roles:
- SAP_SMWORK_INCIDENT_MAN
- SAP_SM_BI_INCMAN_REPORTING
- SAP_SM_CRM_UIU_FRAMEWORK
- SAP_SM_CRM_UIU_SOLMANPRO
- SAP_SM_CRM_UIU_SOLMANPRO_PROC
- SAP_SUPPDESK_PROCESS
- SAP_SM_SL_DISPLAY
- SAP_SM_FIORI_LP_EMBEDDED

BW Authorization Roles

Some scenarios require BW reporting authorizations. For these scenarios specific BW authorization objects are required by the user, and therefore specific roles are required. These roles are roles containing authorization objects, therefore they need to be copied into your name space. For more information on BW integration, see section Using SAP Solution Manager with Business Warehouse (BW).
Example

The role(s) that are meant are highlighted.

Composite Role: SAP_SUPPDESK_PROCESS_COMP

Single Roles:

- SAP_SMWORK_INCIDENT_MAN
- SAP_SM_BI_INCMAN_REPORTING
- SAP_SM_CRM_UIU_FRAMEWORK
- SAP_SM_CRM_UIU_SOLMANPRO
- SAP_SM_CRM_UIU_SOLMANPRO_PROC
- SAP_SUPPDESK_PROCESS
- SAP_SM_SL_DISPLAY
- SAP_SM_FIORI_LP_EMBEDDED

J2EE/Java Roles

In case an application is based on Java, such as Root Cause Analysis, specific Java role are required for the user. These roles have the same names as the security group in the User Management Engine (UME) of the Java stack. As navigation roles are simply defining navigation possibilities, the roles do not contain any relevant authorization objects, and should not be copied into a separate name space. For more information on Java integration, see section Using SAP Solution Manager with Java Stack.

4.3 Authorization Object Classes

Authorization objects in roles are clustered in authorization classes. Authorization classes relate to shipped Software Components. The following authorization classes are part of SAP Solution Manager roles:

- **AAAA**
  
  This class contains all authorization objects that are obsolete. Here, you can find all authorization objects which have become obsolete with the change of Release

- **BC**
  
  These classes contain all authorization objects which are relevant for SAP Basis components in the system. All authorization objects included in this class start with convention `S_`. Authorization objects of this class are always to be checked in the coding.

- **CRM**
  
  All authorization objects included in this class come from CRM component. Authorization objects in this class start with `CRM_`. CRM authorization objects are required for all applications, which are based on CRM WebClient, such as ITSM scenarios. For more information on the CRM Authorization integration within SAP Solution Manager, see the according section in this guide.

- **RS**
  
  All authorization objects included in this class come from the BW component (Software Component `ST_BCO`). Authorization objects in this class start with `RS_`. BW authorization objects are required for all applications,
which use BW - Reporting. For more information on the BW Authorization integration within SAP Solution Manager, see the according section in this guide.

- **HR**
  The relevant authorization object contained in this class is **PLOG**. This is an organization related authorization object used in HR organization. If you are using an organizational model within SAP Solution Manager, you need to maintain this object according to your needs.

- **SM**
  All authorization objects relevant for SAP Solution Manager and shipped with Software Component ST are contained in this authorization class.

- **SMD**
  All authorization objects related to Solution Manager Documents. Currently these are:
  - **S_SMDATT**
  - **S_SMDDOC**
    Both objects are contained in roles **SAP_SM_KW_***.

- **SMPI**
  All authorization objects delivered within Software Component ST-PI, which relate to Solution Manager.

- **SMBI**
  All authorization objects delivered within Software Component ST-BCO, which relate to Solution Manager.

### 4.4 Authorization Object Status in Roles

Within SAP Solution Manager roles, you find a number of roles with authorization objects having varying status descriptions. When maintaining authorization objects within a role, the system displays various status of authorization objects. The following status are displayed:

- **Standard**
  This object displays value entries in authorization fields which are default, and the object is retrieved from customer tables maintained in transaction **SU24**.

- **Changed**
  The default field values of this object have been changed.

- **Maintained**
  The changed values have been maintained.

- **Manually**
  The object has been added manually by using the button **Manually**.

For more information on transaction **SU24** and transaction **SU25**, see SAP NetWeaver documentation.

### Menu Tab and Authorization Tab Dependencies in Roles

Whenever an application is entered in the **Menu** tab of a role, the associated authorization objects are displayed by the system in the **Authorization** tab with status **Standard**. In case, the **Standard** is adapted or maintained the authorization object receives either status **Maintained** or **Changed**.
Within SAP Solution Manager the following applications are maintained in the Menu tab for roles for end-users:

- Web Dynpro Applications
- Transactions
- BSP Applications (in case of CRM WebClient applications)
- OData Gateway Services (in case of SAPUI5 applications and external services)

For the authorization objects related to one of these applications to appear in the role as an authorization object, you need to fill your customer tables with all the default values for authorization objects that are shipped by SAP. This is part of the SAP Solution Manager configuration procedure in step Initialize or Update SU24 Authorizations.

If you run transaction SU25 steps 1 or 2 after any update Support Package, your customer tables are filled with the delivered values. You can adapt these values for your own purposes in transaction SU24. For more information, see SAP NetWeaver documentation for this topic.

### Authorization Object Status in End-User Roles

Most end-user roles contain authorization objects referring to standard, changed, and maintained authorization objects. Still, you may find authorization objects which have been added to the role manually. This can be the case if the authorization object in question belongs to an SAP Basis application which is not fully integrated into SAP Solution Manager. It can also be that authorization objects that belong to the User Interface are not added as per Standard but manually.

⚠️ **Caution**

Transaction and Web Dynpro Applications AGS_WORKCENTER and WD_SISE_FWK_WIZARD are not maintained with default authorization values as they represent a technical framework for other applications to run in. Any framework authorizations are therefore maintained with status Manually in the according roles.

### Authorization Object Status in Configuration Roles and Roles for Technical Users

Configuration roles and roles for technical users mainly contain authorization objects in status Manually, as the roles and the maintained authorization objects are specifically designed with field values, as the technical user should only be able to perform the tasks necessary. These objects should not be changed by the administrator/customer.

### 4.5 Authorizations and Roles for Infrastructure

In the context of the SAP Solution Manager, we use the term Infrastructure for all entities related to systems, hosts, databases, business process documentation, business partners, and RFCs. These units form the basis for all scenarios.
Which of the units is used depends on the "position" of the scenario in the end-to-end process of your solution's life cycle, relative to whether you are in preparation of going life, or whether you are already life. If you are preparing for going life with your project, you are primarily using process documentation for your basis. If you are already life with your processes, you are primarily using process documentation or only systems.

Given the basic nature of these entities, process documentation authorizations, and system authorizations are required by any user in different scenarios. It must be possible to maintain these authorizations in a way, that they are only to be maintained once, even if used for different functions. Therefore, we have extrapolated these authorizations into specific user roles for infrastructure:

- **Systems:** `SAP_SYSTEM_REPOSITORY_*`
  These roles contain all relevant authorizations for the system repository or LMDB (Landscape Management Data Base)

- **Process documentation:** `SAP_SM_SL_*`
  These roles contain all relevant authorizations for process documentation

In addition to these general infrastructure roles, Solution Manager delivers as well roles for the following infrastructure related functions:

- **RFC Maintenance:** `SAP_SM_RFC_*`
  Due to the relevance of the extensive use of RFC - communication between the Solution Manager system, the managed systems, and the BW-system, a separate role for maintenance of RFC - connections is shipped, which contains authorizations for transaction `SM59`.

- **Business Partner Assignment:** `SAP_SM_BP_*`
  Business Partners are used by many applications running in Solution Manager. These roles contain all necessary authorizations for their usage.

### Note

If these roles (or the corresponding authorization objects) are not assigned to a user, this user will not be able to display the **Business Partner** tab in transaction LMDB, or be able to filter in the POWL queries `SMWORK_TSYS_DIAG_REL` and `SMWORK_DIAG_ALL`.

Within transaction LMDB, you are able to go to the **Business Partner detail** screen of the CRM WebClient application. To be able to do so, you need to additionally assign the following two roles to your user:

- `SAP_SM_CRM_UIU_SOLMANPRO` (do **not** copy into your name space) for navigation access
- `SAP_SM_CRM_UIU_SOLMANPRO_PROC` (do copy into your name space) for authorization access

- **Document Management and Digital Signature:** `SAP_SM_KW_*`
  Document Management is used by a number of related applications such as Implementation and Change Request Management. These roles contain all relevant authorizations for Document Management.

### Table 6:

<table>
<thead>
<tr>
<th>Role</th>
<th>Included Authorization Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>SAP_SM_SL_DISPLAY</code></td>
<td>The role contains all relevant authorizations for process documentation in display mode.</td>
</tr>
</tbody>
</table>
Role | Included Authorization Objects
--- | ---
SAP_SM_SL_EDIT | The role contains all relevant authorizations for process documentation for editing processes.
SAP_SM_SL_ADMIN | The role contains all relevant authorizations for process documentation administration.

**Authorization Objects that were relevant in Release 7.1**

Due to the major change in Process Documentation architecture, most formerly relevant authorization objects are obsolete. They are set into authorization class AAAA as obsolete. In case you need to check solutions of Release 7.1, roles SAP_SOLPRO_OLD and SAP_SOLPRO_DISP_OLD contain these authorization objects.

**Document Management and Digital Signature**

<table>
<thead>
<tr>
<th>Role</th>
<th>Included Authorization Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_SM_KW_DIS</td>
<td>The role contains all relevant authorizations for Document Management in display mode.</td>
</tr>
<tr>
<td>SAP_SM_KW_EXE</td>
<td>The role contains all relevant authorizations for Document Management for editing documents.</td>
</tr>
<tr>
<td>SAP_SM_KW_ALL</td>
<td>The role contains all relevant authorizations for Document Management administration.</td>
</tr>
</tbody>
</table>

**Obsolete Authorization Objects**

Two new authorization objects are shipped with Release 7.2. They substitute completely authorization objects S_IWB, S_IWB_ADM, and S_IWB_ATTR. Both objects are shipped with software component SAP_BASIS, and are contained in authorization class SMD.

**New Authorization Object: S_SMDATT**

This object restricts the use of a document depending on the allowed document attributes.

**New Authorization Object: S_SMDDOC**

This object restricts the activities that can be done on a document.

**Note**

Activity 60 (import) is shipped per default in role SAP_SM_KW_ALL. It is used for the migration procedure of documents to import KW documents into the new folders. You can remove the value after having run the migration procedure for documents.

**Digital Signature for Test Management**

As Test Management contains a separate framework for Digital Signature which allows to use a signature process for Test Plans. All relevant authorizations for object C_SIGN for this use case are contained in roles SAP_STWB_2_***, see scenario - specific guide for Test Management.
Embedded Search (TREX and HANA based)

Embedded Search supported by TREX or HANA is used in SAP Solution Manager by various scenarios, such as Process Documentation, Change Request Management, Incident Management or Q-Gate Management.

Authorizations

All authorization objects required by this basic functionality is included in the Core Roles for the various scenarios. All authorization objects related to Embedded Search have the following naming convention: S_ESH_*.

Configuration

Note

Configuration of Embedded Search is currently contained in transaction SOLMAN_SETUP guided procedure for Process Management. It is only required to be configured once, and can be used in all other relevant scenarios.

System Landscape

Table 8:

<table>
<thead>
<tr>
<th>Role</th>
<th>Included Authorization Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_SYSTEM_REPOSITORY_DIS</td>
<td>The role contains all relevant authorizations for systems AI_LMDB_*, as well as:</td>
</tr>
<tr>
<td></td>
<td>• SM_CMDB OB</td>
</tr>
<tr>
<td></td>
<td>• SM_SETUP manually entered</td>
</tr>
<tr>
<td>SAP_SYSTEM_REPOSITORY_ALL</td>
<td>Additional to all authorization objects for SAP_SYSTEM_REPOSITORY_DIS the role includes as well:</td>
</tr>
<tr>
<td></td>
<td>• AI_LMDB_AD</td>
</tr>
<tr>
<td></td>
<td>• S_TCODE; TCD value LMDB</td>
</tr>
</tbody>
</table>

Authorization Object AI_LMDB_OB

Caution

This authorization object allows you restrict your users for systems to display, edit, and so on. It is contained in role SAP_SYSTEM_REPOSITORY_*_. If you restrict AI_LMDB_OB, do not allow System Landscape Directory (SLD) authorizations at the same time. Minimal SLD authorizations have complete read access. For more information, see SLD security guide.

Note

As of Release 7.2, all authorization objects and roles pertaining to transaction SMSY are obsolete.

Authorization Object AI_LMDB_PS
This authorization object is relevant for the restriction of Product Systems in Release 7.1. It is only relevant in Release 7.2 for migration purposes. When you have finished migration, you can remove the object from the role.

**Security-relevant Authorization Object AI_LMDB_TM**

The authorization object **AI_LMDB_TM** protects the transport domain entry in transaction **LMDB**. The **Transport Management** provides a disjoint possibility to store information about systems. In many cases, the systems stored in the Transport Management can be matched to technical systems, that are stored in the **LMDB**. The **LMDB** Web User Interface allows users to access the information about the relationship between Transport Management System + (TMS) information and Technical System information. You can list all systems (system data) provided by TMS via the domain controller data supplier, and you can maintain (assign/de-assign) a link between TMS system information and technical system information. TMS information is not created or modified – only the links to LMDB information are displayed/created/deleted.

**RFC Maintenance**

Table 9:

<table>
<thead>
<tr>
<th>Role</th>
<th>Included Authorization Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_SM_RFC_*</td>
<td>• S_RFC_ADM</td>
</tr>
<tr>
<td></td>
<td>• S_ADMI_FCD</td>
</tr>
<tr>
<td></td>
<td>• S_RFC_TT manually added</td>
</tr>
</tbody>
</table>

Additionally authorization objects **S_TCODE** and **S_SERVICE**

**Business Partner**

Table 10:

<table>
<thead>
<tr>
<th>Role</th>
<th>Included Authorization Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_SM_BP_*</td>
<td>The role contains all relevant authorizations for business partner and product assignment for POI queries SMWORK_TSYS_DIAG_REL and SMWORK_DIAG_ALL</td>
</tr>
<tr>
<td></td>
<td>• B_BUPA_RLT</td>
</tr>
<tr>
<td></td>
<td>• COM_IL</td>
</tr>
</tbody>
</table>

All additional authorization objects for business partners can, but must not necessarily be used.
4.6 User Interfaces in SAP Solution Manager

4.6.1 SAP Fiori Application Configuration

SAP Fiori Launchpad is the generally advised User Interface by SAP. You can use SAP Fiori Launchpad with SAP Solution Manager either:

- **embedded** within SAP Solution Manager (any SAP Solution Manager application running within SAP Fiori Launchpad UI), or
- **on a separate server** in a Central Hub (specific applications for SAP Fiori Launchpad UI)

In the following sections, we explain which roles and authorizations are required to run SAP Solution Manager either way. Specific information regarding individual SAP Fiori Apps are given within the section for the according scenario.

**NWBC**

**Note**

Some scenarios, such as ITPPM, require transaction NWBC as a User Interface in addition to SAP Fiori Launchpad and Tiles. The transaction is included in role SAP_SM_FIORI_LP_EMBEDDED.

### SAP Solution Manager Embedded SAP Fiori Launchpad

To successfully assign SAP Fiori Launchpad authorizations, you need to assign to the end-user:

- **Role** SAP_SM_FIORI_LP_EMBEDDED
  
  All SAP Solution Manager applications that run in the Work Centers can also be called using SAP Fiori Launchpad. Therefore, all users within SAP Solution Manager require single role SAP_SM_FIORI_LP_EMBEDDED, which contain relevant authorizations for the launchpad call. The role is automatically assigned to all users, which are created using transaction SOLMAN_SETUP and available in all relevant composite roles for users.

- **Role** SAP_SMWORK*
  
  To be able to call the User Interface Tiles, you need navigation information assigned to the user. All Catalogue and Group (Tiles) information is delivered within the *Menu Tab* of the already existing Work Center Navigation roles SAP_SMWORK*.

**Note**

○ In case you start SAP Fiori Launchpad directly from the WebDynpro Application of a work center, you can call the Fiori Launchpad from the *Home Work Center*, using the according link in this Work Center. Assign role SAP_SMWORK_MYHOME to your user.
Anytime you assign a new Launchpad - relevant role `SAP_SMWORK`* to a user, you need to empty the launchpad cache. For more information, see IMG activity under `SAP NetWeaver > UI Technologies > SAP Fiori > Data Administration > Invalidate Caches`.

- **Authorization object `S_ESH`*:**
  Each application called requires *Embedded Search* authorizations `S_ESH`*, which are delivered within the core authorization roles for each application.

- **Authorization object `S_SERVICE`**:
  Due to the use of OData - Services, authorization for services is required. You find the specific OData - Services, and their according `S_SERVICE` authorization in the core roles for the scenario in question.

**Note**

If your security requirements do not permit `S_SERVICE` if not needed, you can always set the object inactive or remove the service from the *Menu Tab*.

---

**SAP Fiori App Running on a Central Hub with SAP Solution Manager Backend System**

To successfully assign SAP Fiori Launchpad authorizations, you need to:

**Configure Prerequisites**

To be able to run the SAP Fiori App, you need to configure the following settings with a suitable *Configuration User*.

This Configuration User must have also authorization object `S_RFCACL` assigned.

**Recommendation**

As authorization object `S_RFCACL` is a security-critical authorization object, we recommend to remove this authorization or disable the Configuration User after configuration of the application.

1. Configure the SAP Gateway correctly on the Central Hub.
2. Configure a Trusted RFC - Connection between Solution Manager and Central Hub.
3. Copy the OData - Service in the Front-end system.

**How to Copy the OData - Service**

1. In transaction `SPRO`, go to `SAP NetWeaver > UI Technologies > SAP Fiori > Initial Setup > Initial Launchpad Configuration > Service Maintenance of SAP Gateway`.
2. Call the transaction, and choose the button *Add Service*.
3. In the new dialog, enter the System ID of your Back-end system in the field *System Alias* via F4 Help, in our case SAP Solution Manager system ID.
   The system asks for your Trusted RFC - COnnection to be able to call the OData - Service from the back-end.
4. Press the button *Get Services*.
   The system calls the OData - Services from the SAP Solution Manager into the Front-End system using the Trusted RFC - Connection.
5. Enter the specific OData - Service name (IWSG) which is given in the role description tab of the template role SAP_STUI_<scenario description>_AUTH into the field Technical Service Name.
6. Choose button Add Selected Services.
7. In the appearing dialog, the system displays the name of the service that is to be copied. Here, you can change the name space or leave it as Z.
8. Choose a transport package or use a local package &TMP.
9. Enter.
10. Go back to screen Activate and Maintain Services.
11. Check, if your copied service is available in the list, and double click on it.
12. Check, that the ICF - Node is displayed for the service, and activate the ICF - Node by choosing the button ICF Node -> Activate.
13. For the service to appear later on in the PFCG authorization fields, load the meta data by choosing the button Load Meta Data. Then, call the service once by using the button Call Browser.
14. Check, that the System Alias is also correct.
   You can now add the copied service to your role.

4. Adding the OData Service to Your Role
5. 1. Call transaction PFCG, and choose your role.
   2. Change into edit mode, and open tab Menu.
   3. Choose the button transaction, and here choose entry Authorization Default. The system displays a new dialog.
   4. In the dialog, via F4 help choose in the field Authorization Default entry TADIR Service, and in field Obj Type value SAP Gateway: Service Groups Metadata.
   5. Entere your copied OData service, and choose Copy.
   6. Go back and choose tab Authorizations.
   7. Check that authorization object S_SERVICE is filled, generate the profile, and go back.
   8. Execute the User Comparison on tab User.

For more information, see the SAP Solution Manager Configuration Guide. In addition, you can check the Implementation Guide in the system using transaction SPRO, go to SAP NetWeaver » UI Technologies » SAP Fiori » Initial Setup.

In the Backend System SAP Solution Manager

- Authorization object S_ESH*
  Each application called requires Embedded Search authorizations S_ESH*, which are delivered within the core authorization roles for each application.
- Authorization object S_SERVICE
  Each specific SAP Fiori application is called using an OData - Service (Gateway Service). The Gateway Service is delivered within Menu Tab of the core role for the application. The according authorization object S_SERVICE is delivered with status active.

  **Note**
  If your security requirements do not permit S_SERVICE if not needed, you can always set the object inactive or remove the service from the Menu Tab.

- Authorization objects S_RFC and S_RFCACL
  The front-end components communicate by OData - Services through a Trusted RFC - Destination with the back end Solution Manager system. This requires the user in the back-end to have assigned Remote Function
Call authorization S_RFC and Trusted RFC authorization S_RFCACL. Both authorization objects are delivered in role SAP_SM_FIORI_FRONTEND which needs to be assigned to the user.

**Recommendation**

Role SAP_SM_FIORI_FRONTEND is **not added** to the automatic user generation within transaction SOLMAN_SETUP. Due to the security critical objects, this role **needs to be assigned manually** only to users that are allowed to call the SAP Fiori App.

We highly recommend to maintain authorization object S_RFCACL specifically for this use case (System ID, Client, and User ID).

In the Front-End System (Central Hub) SAP Fiori

You have to assign both types of roles to your user in the frontend-system.

**Roles Delivered with SAP Solution Manager (Software Component ST-UI)**

- **Catalogue and Tiles**
  
  To be able to call the User Interface Tiles, you need navigation information assigned to the user. All Catalogue and Group (Tiles) information is delivered within the *Menu Tab* of navigation roles SAP_STUI_<scenario description>_TCR.

- **Authorization for S_SERVICE (OData - Service)**
  
  Each specific SAP Fiori application is called using an OData - Service (Gateway Service). Within the SAP Fiori environment, you are required to copy this OData-Service into your name space, and then add the copied Service to the *Menu Tab* of the role. The information for the specific Gateway Service is delivered within the *Description Tab* of the role SAP_STUI_<scenario description>_AUTH for the application.

- **Mandatory Additional SAP Fiori Relevant Services**
  
  For SAP Fiori to operate correctly, you need also add in the authorizations role for your application the following Odata - Services or assign role SAP_STUI_GENERAL_AUTH (Please check the *Menu* tab in this role.):
  
  - Service /UI2/INTEROP* (Object Type: IWSV)
  - Service /UI2/PAGE_BUILDER_PERS* (Object Type: IWSV)

**Roles Delivered by SAP Fiori**

- Users require additional access to services and according authorization objects delivered by SAP Fiori.

Execute the according IMG activties under SAP NetWeaver > UI Technologies > SAP Fiori > Initial Setup > Initial Launchpad Configuration > Assign Launchpad Authorization to Users.

**SAP Fiori Catalogues, Groups, and Tiles**

**Concept**

For SAP Solution Manager, each "Work Center" relates to one catalogue. In this catalogue, all relevant applications of the specific Work Center are available as tiles. In addition, specific application tiles are included. Still, not all tiles are displayed by default in the SAP Fiori Launchpad. The system displays only those tiles which are included in a specific group which relates to the according catalogue. You can have a number of different groups referencing to one catalogue.

**Catalogues and Groups**
Catalogues and Groups are delivered within the Solution Manager navigation roles SAP_SMWORK*. Due to this concept, the group associated to the relevant catalogue contains all required tiles that carry functionality which is also present in the Work Centers. If you require to have other groupings of tiles, you need to maintain them in the system (according to SAP Fiori Guidelines), and assign the group to a role manually.

Tiles are displayed by SAP Fiori Launchpad UI, irrespective whether the user has received the according authorizations to run the application or not. If you want to hide specific Tiles, you need to maintain the catalogues and your roles accordingly. In case you do not see any KPI numbers in a tile, the user has not the authorization for the respective OData - Service and related authorizations.

Specific Groups for Applications

If specific groups are required for certain catalogues, these groups are added to the applicable authorization core roles. For instance, in Business Process Monitoring specific groups are required. They are added to the roles for Business Process Monitoring. In addition, the complete group for the work center is available in role SAP_SMWORK_BPO. If you are not working with the Work Center as your central User Interface, you can then remove the role SAP_SMWORK_BPO from your user as tile information is given in the usual authorization roles.

Additional Topics

Personalization

- Tiles can be personalized. If you require just an additional tile in a personalized screen, you can add any tile from any catalogue without specific permissions to add the tile in your Launchpad.

Update Launchpad or SAP Fiori App (Cache Invalidation)

To be able to clear existing UI5 caches and reset the cached Tiles for the Launchpad, run activity Invalidate Caches in transaction SPRO ➔ SAP NetWeaver ➔ UI Technologies ➔ SAP Fiori ➔ Data Administration ➔ Invalidate Caches.

Assignment of Catalogues and Groups to Reference Users

- If you are working with Reference Users, make sure that the Catalogue and Group roles SAP_SMWORK_* are assigned directly to the individual users. SAP Fiori Launchpad does not recognize the navigation menu if only assigned to the Reference User.
- When you use Reference User assignments make sure you invalidate the cache beforehand, and execute all activities mentioned in SAP Note 1947910. You can invalidate the cache by executing IMG activity Invalidate Caches in transaction SPRO. Navigate to SAP NetWeaver ➔ UI Technologies ➔ SAP Fiori ➔ Data Administration ➔ Invalidate Caches.

Enterprise Search in SAP Fiori Launchpad

To be able to use the Embedded Enterprise Search, your user must have authorization object S_ESH* assigned. In general, these authorization objects are contained in the template user roles which are delivered as Standard roles by SAP.
Scan Profiles Used for Attachment Uploads of Documents to SAP Fiori Apps

Attachments uploaded pass through the SAP Virus Scan interface. If you wish to scan the contents of attachments, you must set up and configure the SAP Virus Scan interface. Configuration includes setting up a commercial third party virus scanning product, for more information see SAP Note [786179](https://support.sap.com/).

Once you have configured the SAP Virus Scan interface, you will need to enable the following virus scan profiles:

- `/SIHTTP/HTTP_UPLOAD` checks within Web Dynpro and CRM UI
- `/SCET/GUI_UPLOAD` checks within SAP GUI
- `/SCMS/KPRO_CREATE` checks when saving in all relevant cases

Calling an Application Independently - Standalone

In case, you want to call an application independently from Fiori Launchpad, you need to add the calling BSP application to your user menu, either in your favorites or in the menu of the user roles directly.

4.6.2 Work Center Navigation Role Concept

When using SAP Solution Manager you work within the frame of so called Work Centers. They provide the user with a User Interface that easily allows to access all necessary tools for his/her tasks. Therefore, the important factor of a Work Center is the navigation structure it provides.

To be able to access the Work Centers, the user needs to be assigned to so called Work Center Navigation Roles. For each Work Center one Navigation Role exists.

All composite user roles contain the according navigation role(s): SAP_SMWORK_<WorkCenter> needed for the user to execute tasks.

You can run the work centers in three clients: Internet Browser, SAP Fiori Launchpad, and SAP NWBC.

- Browser: using either the URL itself or calling transaction SM_WORKCENTER in the SAP Easy Access menu.
- SAP NWBC
- SAP Fiori Launchpad (embedded or on a separate central hub)

Work Center Application (Technical Role Names: SAP_SMWORK_<WorkCenter>)

General Information

Work Center Navigation Roles (naming convention: SAP_SMWORK_<WorkCenter>) are based on the concept of authorization roles (transaction PFCG). In the Description Tab, you can find a first introduction and most important information about the navigation role.

Folder Hierarchy in the Menu Tab
The defining factor of the navigation roles is the Menu. The menu information in the role can be found on the tab Menu in the role. Therefore, you do not need to generate any profiles, but you need to execute a user comparison.

The menu always consists of a two - folder hierarchy. It displays the menu hierarchy/entries in the SAP NetWeaver Business Client (NWBC).

The first level is the home page or default page Web Dynpro application (WDA) of the work center (for instance Incident Management). The second level consists of several related links, such as Service Marketplace or Help Portal.

Menu Entries

Every work center navigation role contains a number of menu entries. A mandatory menu entry is the web application AGS_WORKCENTER and its according parameter WORKCENTER with the value <Work Center Application/Component>. In addition, the flag for Default Page must be set.

Work Center Homepage and Related Web Applications

The Work Center framework relies on ABAP WebDynpro application AGS_WORKCENTER for a number of Work Centers this WebDynpro application forms the Home Page. The Home Page information is used in the display of the User Interface. Some Work Centers have specific Home Pages. The Home Page is contained in the first folder level of the navigation role. Web Pages imbedded in the Work Center Framework are often Work Center Components.

Note

If an imbedded Web Page is a Web Dynpro Component, they are not to be activated using transaction SICF. If you want to display such an application separately outside the Work Center framework, this can lead to security-leaks as some Web Dynpro Components might not have separate authorization object checks.

Adaptation of Related Links in the Navigation Panel

We recommend to use the delivered navigation roles. You can also define them for your own purposes. This means, you can add new folders with applications in the Related Links area in the work center navigation panel. You can also delete defined folders. You cannot change entries in the work center areas Common Tasks or Navigation Panel Views in the role. You can adapt these areas using authorization object SM_WC_VIEW.

User Interface Restrictions by Authorization Objects

The following authorization objects can be used to control access to the User Interface for the Work Centers:

- SM_WC_VIEW
- SM_WD_COMP
- SM_APP_ID

For a detailed explanation on these authorization objects, see section on User Interface Authorizations in this guide.

Inactive Authorization Objects

In contrast to authorization roles, which contain a number of authorization objects for authorization purposes, Work Center Navigation roles are only relevant for the navigation in the work center via menu options. They do not contain active authorization objects, except for authorization object S_TCODE with values SOLMAN_WORKCENTER and SM_WORKCENTER.
Nevertheless, in some navigation role menus, you find additional transactions. These transactions must be present in the Menu tab, as they define the transaction navigation in the work center. Having transactions in the Menu tab allows the system to automatically trace all relevant authorization objects, which are connected to this transaction. Authorization objects for these transactions are set inactive.

⚠️ Caution
Do not activate inactive authorization objects in the navigation roles, as this may override your existing authorization concept.

SAP NetWeaver Business Client (NWBC)

⚠️ Caution
SAP NWBC 4.0 and higher is not supported.

The SAP NWBC is an additional client you can use. It needs a so called Control Sequence in the navigation role. This URL is only relevant for the use of work centers in the SAP NetWeaver Business Client (SAP NWBC).

ℹ️ Note
- The folder display in the SAP NWBC is different to SAPGui and Internet Browser. The Related Links section can be found underneath the upper menu.
- If you assign a composite role with any menu entries, the SAP NWBC is not able to display the work center. Any composite role should not have menu entries.

Object Based Navigation (OBN) Targets for Client SAP NWBC

The roles SAP_SMWORK_<WorkCenter> contain Object Based Navigation (OBN) targets. The OBN targets are defined by BOR object: SolManNavigation.

⚠️ Caution
When working with the SAP NWBC, only ONE OBN target entry should be assigned within the roles. Therefore, if you have two work centers assigned to your users, and also two SAP_SMWORK_<WorkCenter> roles, you need to delete the OBN target entries at least from one SAP_SMWORK_<WorkCenter> role. Proceed as follows:

1. Choose transaction PFCG.
2. Choose the SAP_SMWORK_<WorkCenter> role for which you want to delete the OBN target navigation.
3. Go to tab Menu.
4. Choose button Other Node Details.
   The system displays in a column all links which have an OBN target entry.
5. Delete the OBN target entry.
SAP Fiori Launchpad

Each application area (work center) has per default one Catalog and one Group assigned.

Fiori Launchpad Configuration

All work center navigation roles contain SAP delivered entries for Fiori catalogues and groups. This allows you to use the Fiori Launchpad. You can check all configuration entries in transaction 
\texttt{LPD\_CUST}. Here, you can check all tile entries and add your own. If you add new tiles, you have to enter the respective catalogues and groups to the navigation role you are using.

4.6.3 Authorizations for User Interfaces

In general, \textit{User Interface authorizations} regulate whether a user is authorized to see a link which leads to a specific application or button which allows specific actions. Therefore, if a user has the required User Interface authorization, the system displays the access information on the screen. If the user does not have the required User Interface authorization the links or buttons are hidden in the User Interface. In this way, User Interface authorizations can regulate the User Interface appearance and navigation possibilities.

\begin{itemize}
  \item \textbf{Case 1: activity is independent on other context information}
  
  In transaction \texttt{SOLMAN\_SETUP}, the button \textit{Edit} allows users to decide on editing mode for the transaction. This button is controlled by authorization object \texttt{SM\_SETUP}, and specifically with activity 02 \texttt{CHANGE}. If a user does not have this authorization value, the system does not display the button \textit{Edit} in the User Interface.

  \item \textbf{Case 2: activity is dependent on current context information}
  
  A button remains visible, but inactive and greyed out in the User Interface, even if no authorization allows the user to use the application. In this case, another activity in the screen functions as prerequisite. This principle also applies if a button contains an additional drop down menu for specific applications. In case, the user has authorization for one of the displayed activities, the button remains visible in the User Interface, but the user cannot access the restricted application.
\end{itemize}

\begin{itemize}
  \item \textbf{Note}
  
  This principle does not yet apply to all applications in SAP Solution Manager.
\end{itemize}

Since SAP Solution Manager is based on a \textbf{variety of software components}, its user interface technologies are also varied. SAP Solution Manager uses the following technologies, which are integrated with each other:

- \texttt{ABAP WebDynpro}
- \texttt{BSP based technology (CRM 7.01 WebClient UI)}
- \texttt{ABAP SAPGUI transactions}
- \texttt{Java WebDynpro (Java stack)}

All \textit{User Interfaces} can be called via the different Front-end clients. The following sections give an overview of the varying authorizations that determine the User Interfaces.
ABAP WebDynpro Application Authorizations

ABAP WebDynpro is used for most applications in SAP Solution Manager. Especially, newly developed functions are developed in ABAP WebDynpro.

ABAP WebDynpro Application versus ABAP WebDynpro Component

Any ABAP WebDynpro Application is at least restricted by its start authorization object (S_START), and the application itself must be activated as a service in transaction SICF. In contrast, ABAP WebDynpro Components have no start authorization and must not be active in transaction SICF. There is no specific concept as to whether an ABAP WebDynpro Application or an ABAP WebDynpro Component is embedded into the Work Centers.

⚠️ Caution

If you require to call any application, which is embedded in any Work Center, to be called stand-alone, you need to check whether it is an ABAP WebDynpro Application or an ABAP WebDynpro Component. In case of an ABAP WebDynpro Component, find out its application or create your own application for it, and use this application as stand-alone application.

Start Authorization Object: S_START

Before SAP Basis Release 7.4, the maintenance of authorization objects for ABAP WebDynpro in transaction PFCG was mainly done manually, due to former restrictions for this type of technology in transaction PFCG. The start transaction used had been authorization object S_SERVICE. With SAP Basis Release 7.4, a specific start transaction authorization object is introduced: S_START. This authorization object is similar to S_TCODE. S_TCODE is the start authorization for transactions. Therefore, in SAP Solution Manager Release 7.4, authorization object S_SERVICE is substituted by authorization object S_START as ABAP WebDynpro start authorization. For additional information, see section Application Start Authorization Objects.

⚠️ Note

All delivered roles are updated in this regard from Release 7.1 to Release 7.2.


⚠️ Note

See SAP Note 2211213 - How to maintain the authorization for SM_WC_VIEW in a PFCG role.

All work center home page applications are ABAP WebDynpro based. Work Center Views, any Sub-Views, and the Common Task level can be restricted by the authorization object SM_WC_VIEW. This authorization object is contained in the specific core role for the application. In case the authorization object is not granted, the according View, Sub-View or Common Task is hidden by the system in the User Interfaces.

You may need to adapt this authorization object for instance in scenarios in which the user can select copied transaction types in sub-views or views, such as Incident Management or Change Request Management. To be able to adapt, proceed as follows:

2. Choose table AGS_WORK_VIEW.
3. Copy the according entry for the transaction type.
4. Adapt the copied entry.

Table AGS_WORK_VIEW is used as the value help for the authorization object. You can add views and tasks to your work centers and control them using this authorization object. Activate the BAdI Implementation in the IMG for SAP Solution Manager in transaction SPRO.

The BAdI implementation fills the value help table for the authorization object. To use the trace, you must activate the BAdI and go to the work center. The system enters the work center IDs in the value help table AGS_WORK_VIEW. You can then adjust the authorization object in the role.

In a nutshell:

3. Go to transaction PFCG, and call role the according core role.
4. Change the values in the authorization object, for instance only add those views which you want to see, leave out those you do not want to see.
5. Generate the profile, and assign the role to the user.

**Note**

Authorization object SM_WC_VIEW is always checked. If the SM_WC_VIEW check succeeds, then the system checks the authorizations for the specific business function required to use the Web Dynpro Application, Web Dynpro Component or transaction.

The additional User Interface authorization object makes sure; that the User Interface is controlled even when an application does not require specific application relevant authorization restrictions. In addition, this approach has the advantage that you can use the authorization object to remove for instance Common Tasks from a work center, even if the user is technically authorized to use such tasks.

**Example**

In Work Center Incident Management, the Common Task **Manage Substitutes** is not displayed by the system if:

- authorization object SM_WC_VIEW with the according entry is not granted to the user, but the application specific authorizations are granted. This may be the case, if you only want users to maintain substitutes in transaction BP, and not in the work center
- authorization object SM_WC_VIEW is granted, but the application specific authorization object B_BUPR_BZT with value BUR013 is not granted to specific users only.

The Common Task is only displayed by the system, if both authorization objects with the according values are granted to the user.

**Restricting Link and Button Access - URL Framework Authorization Objects SM_WD_COMP and SM_APP_ID**

Specific applications can be restricted by the authorization objects SM_WD_COMP and SM_APP_ID. They are used in the following work centers in SAP Solution Manager:

- Technical Administration
- Technical Monitoring
- SAP Solution Manager Configuration
Both authorization objects restrict views, subviews, URL links, transactions, or buttons leading to separate screens. For all roles delivered as default template roles by SAP, these objects are already maintained according to the user definition by SAP. The authorization objects are included in the applicable core authorization role for the application.

**Example**

For instance, for End-User Experience monitoring (EEM), the core single role is SAP_SM_EEM_*.

The role contains all relevant application IDs for the relevant EEM user role. It does not contain the application ID for the dashboard application for EEM though. This ID is included in the core authorization role dashboards for EEM: SAP_SM_DASHBOARDS_DISP_EEM.

Both authorization objects SM_WC_VIEW and SM_WD_COMP are used to define the User Interface of the above mentioned work centers.

**Caution**

The use of user interface authorizations can lead to misleading ST01 or STAUTHTRACE authorization traces. If you trace one application due to authorization error messages, the analysis of the trace displays all authority checks executed by the system. This also includes user interface authorizations. In case of restrictions to user interfaces by the above-mentioned objects any missing authorizations for them are marked with return code (RC) = 4. If you are not tracing for the user interface element, you can ignore this entry.

You can adapt the authorization objects, and therefore the user interface for all scenarios of these work centers. To do so, you need to apply the so called URL - framework. Here, you can find the according values for the application you want to restrict. Proceed as follows:

1. Call the URL for service: sap/bc/webdynpro/sap/urlapi_app_manager.
2. Open the links for the work center you want to adapt.
3. Check the application view.

The authorization object is displayed on the same page.

**Note**

We recommend not to change the delivered SAP roles.

** Restricting Visibility of Tabs or Logon Screen in the Work Center User Interface **

You can restrict individual tabs in any of the User Interfaces in the Work Centers by using general WebDynpro functionality. For an individual user, proceed as follows:

1. To indicate which tab should be hidden or restricted, bring the cursor in the fields of the tab.
2. Use the left mouse click to display the menu of options.

The system hides the according tab in the User Interface. For more information to restrict a tab system wide for all users, choose documentation link: http://help.sap.com/saphelp_nw70/helpdata/en/46/98ce61f37d19ace10000000a11466f/frameset.htm
BSP CRM WebClient Authorization Object UIU_COMP

BSP based technology is used within the CRM WebClient User Interface, which is called from within the work centers ABAP WebDynpro applications for Incident Management and Change Management applications. Similar to the work center navigation role concept, a CRM navigation role is delivered with the according authorization roles for the authorizations for the User Interface. For more information, see section Using SAP Solution Manager with CRM.

The authorization object for the User Interface for CRM is UIU_COMP. It restricts authorizations for CRM components and its used applications. The authorization object controls which components can be called by the user.

We deliver specific roles for this authorization object, which are again contained in the respective composite roles. All roles for the UIU_COMP authorization object have the naming convention SAP_SM_CRM_UIU_* . They are layered according to the user definition they are defined for. They are additive. For instance, if you use the administrator role for Incident Management, you find two UIU_COMP roles included, as UIU_COMP authorizations in both roles add up. The Incident Management role for the processor includes only one UIU_COMP role. We recommend not to change the delivered SAP roles.

Caution

An ST01 or STAUTHTRACE trace always displays all possible values for this authorization object. Only the objects included in the above-mentioned roles are relevant for SAP Solution Manager applications. For instance, a trace may result in about 500 checks for the authorization object UIU_COMP of which only about 20 checks are relevant for SAP Solution Manager use. We recommend not to change the delivered SAP roles.

ABAP SAPGUI Transactions

ABAP SAPGUI transactions can be called from within ABAP WebDynpro in the work centers. The start authorization for ABAP transactions is contained in authorization object: S_TCODE. To be able to launch a transaction directly from the work center, the transaction AGS_WORK_LAUNCHER must be added to the navigation roles. This is included in Standard Delivery.

UI5 OData - Gateway Services

UI5 Interface technology uses Gateway OData-Services with start authorization object S_SERVICE. As authorization object S_SERVICE is also used for restricting access to External Services, all OData - Services are added to the Menu tab of the respective role.
4.7 Guided Procedure Framework

Guided Procedures (GP) can run in any application of SAP Solution Manager. They are based on the Guided Procedures Framework (GP Framework). We differentiate between the GP Framework and the GP Content. The GP Content is provided by the individual application running and using the GP Framework.

Authorization Roles for GP Framework

Composite role SAP_SM_GP_FRAMEWORK_COMP allows you to access the Framework. The following single roles are necessary for any Guided Framework to run:

- SAP_SM_GP_PLUGIN (Guided Procedure SAP Note Plugin)
- SAP_SM_GP_EXE (Guided Procedure execution)
- SAP_SYSTEM_REPOSITORY_DIS (System display access)
- SAP_SUPPDESK_CREATE (Incident creation)

Caution

The role contains authorization object S_RFC_ADM with value 36 (extended maintenance) for SAP-OSS RFC.

Note

If you want to customize your own Guided Procedure, assign SAP_SM_GP_ADMIN. This role contains critical authorization object S_SYS_RWBO with ACTVT 01, 02, 03, and critical authorization object S_TRANSPRT with ACTVT 01, 02, 03, 07 for Workbench Requests and Customizing Requests. If you do not want to allow the user to create, change, delete or display transports, then you need to deactivate these objects. Additionally, critical authorization object S_CTS_ADMI with value TABL is included in the role. It should not be assigned in combination with transaction codes SE80 or STMS, as it allows super user authorizations in ABAP development environment and transport environment.

In case you need to maintain SAPscript documentation using transaction SE61, you need to assign the following authorization objects to the role:

- S_TCODE with value SE61
- S_DEVELOP with ACTVT 03 (display) for all object types
Authorizations Roles for GP Content

The authorizations for the GP content are provided by the applications. These are explained in the individual scenario-specific guides:

4.8 Using SAP Solution Manager with Java Stack

With Release of SAP Solution Manager 7.2, the Java Stack is separate from the SAP Solution Manager ABAP Stack. You need a Java integration for applications like Root Cause Analysis and SLD usage.

Java Relevant Users

The User Management Engine (UME) of the Java Stack is configured against the ABAP User Store of the Solution Manager ABAP Stack. That means, that the users which are relevant for Java applications, created in the ABAP user store, exist in the Java UME, too.

Java Relevant Roles

As Java relevant roles are assigned to user in the ABAP stack, they do not contain any authorizations, and should not be copied into any name space.

4.9 Using SAP Solution Manager with Customer Relationship Management (CRM)

4.9.1 CRM Web Client UI Navigation Roles

In SAP Solution Manager, the concept of authorizations and navigation for CRM is similar to the work center navigation and authorization concept. We deliver one navigation role and several User Interface authorization roles.
**CRM WebClient UI Navigation Role**

In SAP Solution Manager, such scenarios as Incident Management, Change Management, or Issue Management use the CRM WebClient UI. Therefore, additional CRM UI navigation roles are required for any user for these scenarios. All roles that refer to the CRM WebClient UI have the naming convention SAP_SM_CRM_UIU_*. 

As with work center navigation roles for SAP Solution Manager, the CRM navigation is defined by specific roles: SAP_SM_CRM_UIU_SOLMANPRO, which are included in all relevant composite roles. In SAP Solution Manager only these roles are required. They do not contain any authorization objects, and need only be assigned to the user by user comparison. 

CRM UI authorization roles contain the authorization object UIU_COMP. This authorization object defines which CRM components can be called by the application. By default, they are specifically maintained, which gives unique access to CRM components needed for the required CRM WebClient UI screens for the required scenarios.

- SAP_SM_CRM_UIU_FRAMEWORK: This role contains all UIU_COMP authorization necessary in all scenarios 
- Additional SAP_SM_CRM_UIU_SOLMANPRO_*: These roles contain specifically maintained UIU_COMP authorizations. The roles are complimentary. 

The roles for CRM - specific navigation are also contained in the respective composite roles for a scenario.

**4.9.2 CRM Authorization Concept in SAP Solution Manager**

**General Considerations**

**CRM as Used in SAP Solution Manager Scenarios**

CRM functionality is used by many scenarios in SAP Solution Manager. The CRM WebClient is also used, but not by all scenarios. In this regard, we broadly distinguish between general CRM authorizations and additional CRM WebClient authorizations. The following list reflects CRM authorization objects, which are generally used:

- CRM_ACT 
- CRM_ORD_LP 

**Note**

This object is usually inactive, see section Authorization Method.

- CRM_ORD_OE 
- CRM_ORD_OP 
- CRM_ORD_PR 
- CRM_SEO 
- CRM_TXT_ID 

**Note**

This object is only required if information texts are used.
Note
This object defines the change of status executed by the end-user.

Note
This object defines the change of status executed by the system.

CRM WebClient requires more CRM authorizations, specific navigation roles such as SAP_SM_CRM_UIU_SOLMANPRO (see section CRM Navigation Roles), and specific User Interface authorizations (see section User Interface Authorization Concept).

CRM Customizing
CRM functionality is strongly based on customizing of business processes. That means, that technical entities delivered by SAP are copied into the customer name space. All authorization field values delivered are SAP owned customizing entries. If customizing is executed in a customer system, these values must also be adapted in the required authorization objects. The field values are:

- Transaction Type
- Authorization Key
- Status Profile

Authorization Key and Status Profile are dependent on the Transaction Type. For the various scenarios different Transaction Types are delivered by SAP, which need to be adapted later due to customizing. You can find out which Transaction Type is used for the individual scenarios in the Scenario-Specific Guides.

New Transaction Types
The maintenance of most authorization objects of authorization class CRM are affected. If you customize your own Transaction Types, you need to add them to the according objects.

The standard roles are delivered with standard Transaction Types. If you modify the Transaction Types you use, you need to adapt the according authorization objects in CRM-related roles. This concerns many authorization objects of class CRM, as well as authorization objects B_USERSTAT and B_USERST_T.

Upload and Download of Files in CRM - Related Applications and SAP Fiori Apps

Recommendation
We recommend to use ABAP Virus Scanning Interface (VSI) for virus scans of attachments.
Attackers can abuse a file upload to modify displayed application content or to obtain authentication information from a legitimate user. Usually, virus scanners are not able to detect files designed for this kind of attack. For this reason, the standard SAP virus scan interface includes options to protect the user and the SAP system from potential attacks. For more information about the behavior of the virus scanner when default virus scan profiles are activated.

See SAP Note 1693981 (Unauthorized modification of displayed content)

In all CRM applications the following default VSI profiles are used:

- `/SCET/GUI_UPLOAD`
- `/SIHTTP/HTTP_UPLOAD`

In addition, attachments are scanned using standard Knowledge Warehouse profile `/SCMS/KPRO_CREATE`, specifically for Incidents which are created via an external interface.

### 4.10 Using SAP Solution Manager with Business Warehouse (BW)

#### 4.10.1 General Information

**Scenario Differentiation**

Within the automated basic settings configuration of the SAP Solution Manager system landscape, we differentiate between two possible setup scenarios for Business Warehouse (BW) integration. You run either:

**Standard Scenario**

- BW within Solution Manager system on the same client as the Solution Manager application

**Remote BW Scenario**

- BW within Solution Manager system in another client
- BW in another system

Most BW-related authorizations and roles are shipped with software component ST-BCO.

The following sections give you an overview on the respective configuration of the BW scenarios in regard to the authorizations, users, and RFC-connections, as well as the reporting dashboards based on BI-data.

**BW Setting in Transaction SOLMAN_SETUP**

For the system to be able to configure the data extraction correctly, you need to specify the setup scenario. In transaction SOLMAN_SETUP, you specify the system and the client in which your data extraction runs.
Other BW-related Settings

Other BW-related settings, than those mentioned above are used, such as BW authorization concept, or RFC-connections. For instance, the MDX Parser RFC-Connection is used in various scenarios for SAP Solution Manager, such as Solution Documentation or Business Process Change Analysis. The RFC-connection MDX PARSER (external program) is part of the MDX-interface of BW. For more information, see BW Documentation.

4.10.2 BI - Reporting Data Extraction

The setup of BW for use with SAP Solution Manager is based on the so called Extractor Framework (EFWK). The EFWK is used to collect data, for instance from SAP Solution Manager and Introscope Enterprise Manager, for Business Warehouse by means of various extractors.

The BI reporting role concept is based on the existing role concept of the SAP Solution Manager 7.2. The BI reporting is integrated in the SAP Solution Manager Work Centers for the different applications. At present, we differentiate between three types of extractor use cases in the area of BI-based reporting:

- Reporting data is stored in the SAP Solution Manager system
- Reporting data is stored in the managed systems
- Reporting data is stored in the BW-system

Reporting data extracted from the SAP Solution Manager system

The first type is a combination of a Solution Manager system and a BI system. Here, the data for the reporting is stored in the SAP Solution Manager. The BI-based reporting delivered with the SAP Solution Manager 7.2 contains at the present the following applications:

- Incident Management Reporting (work center Incident Management)
- Test Workbench Reporting (work center Test Management)
- Value Realization

Reporting data extracted from a managed systems

The second type is extracting data from a managed system outside of the SAP Solution Manager system. Managed systems reporting applications:

- End-User Experience Monitoring Reporting (work center Technical Monitoring)
- Process Integration Monitoring Reporting (work center Technical Monitoring)
- Connection Monitoring Reporting (work center Technical Monitoring)
- Root Cause Analysis Reporting (work center Root Cause Analysis)
- Alert Management (work center Technical Monitoring)
- Early Watch Alert (work center Technical Monitoring)
• Database Performance (work center Technical Monitoring)
• Business Process Monitoring Reporting (work center Business Process Operations)
• Job Monitoring Reporting (work center Job Management)
• Data Base Performance Reporting (work center Technical Monitoring)
• Data Volume Management Reporting (work center Data Volume Management)

Reporting data extracted from a managed systems

The third type is extracting data from the BW-system. BW-system reporting applications:
• Value Realization
• Monitoring and Alerting

4.10.3 Configuration of BW and Activation of BW - Content (Step by Step)

Note
See also SAP Note 1487626.

In this section, the configuration and operation process for BW-data extraction and reporting is explained for both main setup scenarios. All users mentioned and their assigned roles are explained in more detail in the chapter on users for BW in the SAP Solution Manager Secure Configuration Guide.

Table 11:

<table>
<thead>
<tr>
<th>Standard Scenario</th>
<th>Remote Scenario</th>
<th>Additional Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure BW and Activate Content</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To use Business Warehouse (BW), you need to initially configure it. This includes the activation of all technical content and the source system in the according BW-client. The system executes the initial configuration via transaction SOLMAN_SETUP (work center SAP Solution Manager configuration) in a number of configuration steps.
**Standard Scenario**

The configuration is done by user **SM_BW_ACT**, who is authorized to plan activation job **CCMS_BI_SETUP** to activate the **BW** content. The user activating the technical content is also user **SM_BW_ACT**.

Since **BW** runs in the same client as the productive Solution Manager, the technical user **SM_TECH_ADM** user is used as the **BW** administration user. Since **BW** - client and Solution Manager client are the same, **RFC** - destination **NONE** is used to connect them.

**Remote Scenario**

The configuration is done by a dedicated **BW** - Administration user in the **BW** - system, for instance **SM_BW_ADMIN**, who is authorized to plan activation job **CCMS_BI_SETUP** to activate the **BW** content. The user activating the technical content is also the **SM_BW_ADMIN** user. The **RFC** - destination used is **SAP_BID**.

**Additional Remarks**

All necessary **RFC** - destinations are created and written in table **E2E_WA_CONFIG**:

- **SAP_BID**: a write **RFC** - destination
  
  **BI_CLNT< BWClient >** with **RFC** - user **SMD_BI_RFC** (in case of its use for content activation, a user parameter **BATCH_USER_ID** requires the administration user)

- **SAP_BIEX**: a read **RFC** - destination
  
  **BW_SM_< BI_SID >CLNT< BIClient >** with **RFC** - user **BW_SM_< SolManSID >**

- **SAP_BILO**: a trusted **RFC** for end-users

---

### 2 Start Extractors in the Managed System, the SAP Solution Manager System, and the BW System

The job **EFWK RESOURCE MANAGER** is scheduled by user **SOLMAN_ADMIN**. **SOLMAN_ADMIN** has the authorization to allow that another technical user **SM_EFWK** can run the program **E2E_EFWK_RESOURCE_MGR**, which is called in the step of the job. In the step, the program is started, and run by user **SM_EFWK**.

The program starts the framework for the extractors. It starts extractors in the local system (Solution Manager) for instance for **CRM** - related data, **TwB** - related data and **ESR** - related data, in the managed systems for **KPI** - related data, and the **BW** - system for **ESR** - related data.

For each extractor the user **SM_EFWK** is assigned separate authorization roles.

Table **E2E_ACTIVE_WLI** contains all extractors which have been started.

---

### 3 Run Extractors in the Managed System, the SAP Solution Manager System, and the BW System
<table>
<thead>
<tr>
<th>Standard Scenario</th>
<th>Remote Scenario</th>
<th>Additional Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extractors in the local system are started by technical user SM_EFWK.</td>
<td>Extractors in the local system are started by technical user SM_EFWK.</td>
<td></td>
</tr>
<tr>
<td>Extractors in the managed systems are run by the READ user as the READ RFC destination is used.</td>
<td>Extractors in the managed systems are run by the READ user as the READ RFC destination is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Extractors in the BW system are run by the technical user SM_BW_&lt;SolManSID&gt; via RFC connection SM_BW_&lt;BI_SID&gt;CLNT&lt;BIclient&gt;.</td>
<td></td>
</tr>
</tbody>
</table>

### 4 Load Data in the BW System

The data, extracted from the various systems into SAP Solution Manager, is downloaded into the BW system.

The data in the SAP Solution Manager client are pushed to the BW component in SAP Solution Manager using RFC NONE. The same user as for executing the extractor program, SM_EFWK, is used to load data into the BI cubes.

The data in the SAP Solution Manager client are pushed to the BW system from Solution Manager using RFC BI_CLNT<BI_Client>. User SMD_BI_RFC is used in this RFC.

Data extracted in the BW system for Value Realization are send to SAP.

Data extracted in the BW system for MAI are pushed into MAI in the Solution Manager system.

### 5 Display BW -Content

According to the individual scenarios, user roles (composite roles) are provided as templates. These composite roles include BW reporting roles (single roles) for the appropriate user. These reporting roles contain all relevant authorizations for displaying BW content. To fetch the data, the RFC NONE is needed for the according dialog user.

According to the individual scenarios, user roles (composite roles) are provided as templates. These composite roles include a BW reporting roles (single roles) for the appropriate user. These reporting roles contain all relevant authorizations for displaying BW content. BI reporting uses Web Templates. In the BW system a query is executed. To fetch the data, an HTTP call is made and a trusted RFC destination SAP_BILO is used to read data. This requires, that the dialog user in the Solution Manager system has a corresponding user in the BW system/client. Both users have trusted authorizations, same User ID and Password.

The RFC destination SAP_BILO is also used for the Monitoring and Alerting Infrastructure (in the Alert Inbox, it is possible to display the Metric Monitor application), and all dashboards which have data in the BW system.

### 6 Reorganize BW Data (Not RCA) and Validate Configuration

For the triggering of reorganization of BW data and configuration validation, a BW Callback RFC destination <SolutionManager-client>CLNT<SolutionManager-ProductiveClient> with technical user BI_CALLBACK is needed in the SAP Solution Manager.

The same RFC destination is used for enriching LMDB data.
4.10.4 Diagnostics Center

The Diagnostics Center is a tool to check your configuration of BI - Reporting by executing checks.

1. A dialog user starts the diagnostic center from the Solution Manager Administration work center:
   - Infrastructure ➔ BW Reporting ➔
2. The checks in the managed system are running with system user SM_<Client>_READ.
3. The checks in the Solution Manager system are running via the logged on dialog user.
4. The checks for the BI are running via RFC destination NONE (dialog user). In the case of a remote scenario, RFC destination BI_CLNT<client> (user SMD_BI/rfc).

4.10.5 BI - Reporting Authorizations and Roles

Using BW reporting requires that the user has BW - authorizations (Authorization object class RS) assigned. In general, these authorizations are included in the relevant BW - composite roles. As BI - reporting is based on the extractor framework, the user needs to have the according BW - reporting authorizations as well as extractor authorizations. For more information, see according Application - Specific Guides.

Software Components Containing Authorization Objects

With each of the software components ST and ST-BCO functionality for the SAP Solution Manager is delivered.

Authorization Check

The authorization check for BW is as follows: If the system does not have any BW - data available, it can not display them. For instance in Business Process Operations for Health Check Analysis, you may select a solution for which no BW - data are present in the system. In this case, the system does not display any solution data.

Display Authorization for Role SAP_BI_E2E

Role SAP_BI_E2E contains activation authorizations for all BI - reporting scenarios as well as batch authorizations. It is not delivered as a display role, as such a use case would be very specific. For instance, if you want to display performance data in the Alerting Framework in work center SAP Solution Manager Administration, you need to add role SAP_BI_E2E as well.

If you want to restrict the role for display purposes, proceed as follows:

1. Copy role SAP_BI_E2E.
2. Restrict the activity field ACTVT for all authorizations to display (usually 03).
3. The authorization objects S_BTCH_* should be set inactive.

4.10.6 Using BI - Dashboards for BI - Reporting

BI - reporting is implemented in several work centers of the SAP Solution Manager. Recently, it became more and more important to aggregate data for several business areas. Dashboards provide an adequate type of display of BI data in a compressed way, filtered for different user groups. Therefore, it is necessary to limit the access to different information for different users.

BI - reporting is implemented for various scenarios, see section BI - Reporting Scenarios. BI - dashboards are based on the BI - reporting function for some of these scenarios.

NEW: Dashboard Builder

The Dashboard Builder integrates dashboards in applications of the Solution Manager, and allows the usage and presentation of data from the Business Warehouse in the Solution Manager. It enables the flexible configuration of dashboards by the help of business apps. The Dashboard Builder is an HTML5-based, coding-free and easy-to-use tool to quickly build a dashboard for visualizing data.

Note

The following Dashboards are still supported by the OLD Framework:

- My Dashboard
- Alert Management Reporting Dashboard
- Business Process Operations Dashboard
- Ici Dashboard
- LMDB Infrastructure Dashboard
- LMDB System Landscape Dashboard

Data Flow and RFC - Connection

1. Call from Software Component ST to ST-BCO, to get the BW query metadata, and execute BW query, using Trusted RFC - Connection SAP_BILO.
2. Call from Software Component ST-BCO to ST, to call the function modules ST or access Business Process Analytics in ST to get the metadata of the dataset or the dataset itself, using Trusted RFC - Connection SAP_DABU (see also SAP Note 2182994).
User Types and Authorization Roles

According to the overall authorization concept of SAP Solution Manager two roles are delivered in software component ST (for SAP Solution Manager) and two roles delivered in software component ST-BCO (for BW-system).

In SAP Solution Manager

- **SAP_SM_DSH_DISP** (Help Text: AUTH_SAP_SM_DSH_DISP)
  You assign this role to a standard dashboard user who is not maintaining the existing dashboards. All necessary roles for displaying dashboards in scenarios are included in the according composite roles for users.

- **SAP_SM_DSH_CONF** (Help Text: AUTH_SAP_SM_DSH_CONF)
  You assign this role to a Dashboard Designer for the Dashboard Builder. The Dashboard Designer is able to quickly and easily create dashboards and provide them to her/his users. The user is allowed to:
  - Create new dashboard categories
  - Modify and delete existing custom dashboard categories
  - Create new dashboards, and assign them to specific dashboard categories
  - Change and delete existing dashboards

**Recommendation**

In case you want to minimize authorizations of role **SAP_SM_DSH_DISP** for specific applications, such as ITPPM, you need to maintain authorization objects **SM_DSHO** and **SM_DSH_CAT** explicitly.

In BW - System

- **SAP_SM_BI_DSH_DISP** (Help Text: AUTH_SAP_SM_BI_DSH_DISP)
  This role is required for end users who want to display dashboards that have been created with the Dashboard Builder. For the underlying DataProviders separate authorization roles are required.

- **SAP_SM_BI_DSH_CONF** (Help Text: AUTH_SAP_SM_BI_DSH_CONF)
  This role is required for users who want to configure dashboards with the Dashboard Builder.

Authorization Concept

**BI** reporting dashboards are integrated in the Dashboard Framework. The following authorization objects are relevant:

- **SM_DSHCAT** is required for restricting Dashboard categories
- **SM_DSHO** is required to control activities within the dashboard according to the category allowed

Authorization Group for Authorization Object S_TABU_DIS

Authorization group **SMSD** is used in SAP Solution Manager to protect according Dashboard Builder tables.
4.11 Using the Help Center

You have the option to use the help center functionality, which resides in SAP Solution Manager as well as in the managed systems.

If you want to maintain/administer the help center you need to have additional authorization. In the following paragraphs we outline, which additional user roles and authorizations you need to assign to your users.

Roles and Authorizations

Roles for Using and Administering Help Center in SAP Solution Manager and Managed Systems

Roles for Help Center in managed systems can also be applied to SAP Solution Manager itself, if you want to maintain the Help Center for SAP Solution Manager.

Table 12:

<table>
<thead>
<tr>
<th>Name</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_BC_WDHC_ADMINISTRATOR</td>
<td>Authorization to administer Help Center</td>
</tr>
<tr>
<td>SAP_BC_WDHC_POWERUSER</td>
<td>Authorization to use Help Center</td>
</tr>
</tbody>
</table>

Prerequisite

On configuring and connecting Help Center of a managed system, see IMG - activity: Information and Configuration Prerequisites (technical name: SOLMAN_HC_INFO)

4.12 Critical SAP BASIS Authorization Objects

4.12.1 Trusted RFC: Authorization Objects S_RFCACL and S_RFC_TT

The Trusted - Trusting Relationship (RFC)

The Trusted - Trusting RFC destination has the Current User settings, and Trust Relationship Yes in transaction SM59.

👉 Recommendation

A trusted relationship in SAP Solution Manager should only be one-sided. We recommend, you only create a trusted relationship between the managed system to SAP Solution Manager, but not SAP Solution Manager to
the managed systems. This means that you should only allow trusted calls from Solution Manager to a managed system but not vice versa.

Authorization errors in the use of an RFC destination flagged as a *Trusted System* cause the following message to be sent: `No Authorization to logon as Trusted System (Trusted RC = #)`.

Every authorization error when using an RFC destination flagged as a *Trusted System*, is a RABAX (ABAP exception). The RABAX contains detailed error information. To analyze the error:

1. Choose transaction ST22 and the selection period.
2. Choose the entry under the user SAPSYS and the program name CALL_FUNCTION_SYSCALL_ONLY. The paragraph *Troubleshooting*, contains the information necessary to correct the error.

**Return Code**

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Explanation</th>
<th>To Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Invalid logon data (user and client) for the trusting system</td>
<td>Create a corresponding user in the client system for the user in the server system (trusting system)</td>
</tr>
<tr>
<td>1</td>
<td>The calling system is not a trusted system, or the system security ID is invalid.</td>
<td>Create the trusted RFC connection again.</td>
</tr>
<tr>
<td>2</td>
<td>The user has no authorization containing the authorization object S_RFCACL, or is logged on as the protected user DDIC or SAP*</td>
<td>Give the user the authorization, or do not use the protected users DDIC or SAP* (see: profile parameter and value: login/no_automatic_user_sapstar = 0)</td>
</tr>
<tr>
<td>3</td>
<td>The timestamp of the logon data is invalid. Check the system time in the client and in the server, and the validity date of the logon data.</td>
<td>Synchronize the system times</td>
</tr>
</tbody>
</table>

**Authorization Object S_RFCACL**

To use an already existing trusted RFC connection, you need to have the authorization object S_RFCACL in the Solution Manager system and in the managed system assigned to your user. This authorization object is not contained in profile SAP_ALL due to its highly critical nature.

**Note**

The roles SAP_SM_S_RFCACL and SAP_SM_BW_S_RFCACL for Template Users created in transaction SOLMAN_SETUP contain the authorization object S_RFCACL, which consists of a number of authorization fields to allow a trusting - trusted relationship between SAP Solution Manager and any managed system.
How to Maintain the Authorization Object

**Caution**
Specifically for all SAP Fiori Applications, make sure you maintain the authorization object with only the required values for the user and the system IDs in question. Do not use any generic values (such as `*`) for `RFC_SYSID`, `RFC_CLIENT`, and `RFC_USER`, see also SAP Note 128447.

Use Transaction Code in S_RFCACL

Trusted RFC connections are only safe if you implement a strong authorization concept concerning authorization object `S_RFCACL` in the managed systems. You can use the authorization field `RFC_TCODE`. This requires, that you make a specific setting for it while creating the trust relationship itself. Whenever you generate a new Trust Relationship, activate the flag *Use Transaction Code* on the tab *Configuration*. This enables the use of the authorization field `RFC_TCODE` of authorization object `S_RFCACL`.

Authorization Object S_RFC_TT

Authorization object `S_RFC_TT` is only required for creating trusted relationships for managed systems in transaction `SMT1`, as of SAP_BASIS_7.02 SP03 and higher, see SAP Note 1734607.

4.12.2 Function Calls: Authorization Object S_RFC and S_DEV_REMO

Authorization Object S_RFC

A remote function call (RFC) calls a function module in another system. Due to the nature of SAP Solution Manager, the number of RFC calls to and from other systems is high. Therefore, a high number of function modules are affected.

In the context of security of RFC calls we have to look at three areas:

- **Authentication**
  Incoming RFC connections must authenticate in the system. For instance, the *READ RFC* call is an incoming RFC call in the managed system. Therefore, a user must be present in the managed system to authenticate the RFC call. Here, user of type *system* is used. From the SAP Solution Manager system's point of view, the *READ RFC* connection is an outgoing RFC. Outgoing RFC connections are maintained in transaction `SM59` in the present system. In the RFC itself, the user is maintained. During the Solution Manager setup of managed systems, most RFCs are automatically created, as well as the user in the managed system, and the assignment of according authorizations for this user. The RFCs are added automatically to transaction `SM59`. For their evaluation and monitoring, RFC traces (transaction `ST05`) can be used as well as the Security Audit Log.

- **System profile parameter**
  The RFC authorization check can be activated / deactivated with the system profile parameter `auth/rfc_authority_check`. This parameter must not be set to the value 0. If you set the value to 9, the
system only accepts the values of `FUNC` (function module) in the authorization object. Make sure, that all roles do only contain `FUNC` (except for function group `SRFC`). For more information, see SAP Note 931252.

- **Authorization objects**
  The authorization object `S_RFC` is used to check, whether the called RFC user is authorized to execute RFC function modules. The authorization object is delivered with dedicated values.

  **Example**
  The SYST function group is needed to call SM59. If it is missing, the remote logon in transaction SM59 causes the RFC_NO_AUTHORITY ABAP runtime error in the target system.

  For `S_RFC` value changes for the technical RFC - users for READ and TM - RFC connection, see SAP Note 1572183.
  Since SAP BASIS 7.02, you can maintain the authorization object for certain function groups but also function modules. Within SAP Solution Manager, you may find the authorization object maintained according to this differentiation.
  Authorization object `S_RFC` can be traced with audit log trace in transaction SM19 and SM20. To protect the deletion of traces, maintain field `ACTVT` with value 36 of authorization object `S_RFC_ADM`.

  **Caution**
  Currently, RFC - function modules in function group `/SSF/INTRFC` have no own authorization checks.

  **Note**
  For more information on RFCs and how to secure them, see [http://scn.sap.com/docs/DOC-60425](http://scn.sap.com/docs/DOC-60425) and SAP Note 14113011.

**Authorization Object S_DEV_REMO**

In managed systems as of SAP BASIS 8.03 and higher, function group `RFC1` is additionally protected by authorization object `S_DEV_REMO`. Therefore, all relevant roles for the setup of managed systems using transaction SOLMAN_SETUP include authorization object `S_DEV_REMO`.

### 4.12.3 Table Maintenance: Authorization Objects S_TABU_DIS, S_TABU_NAM, and S_TABU_CLI

In many scenarios for SAP Solution Manager, the system needs to read table entries. The direct access to tables is limited wherever possible, because a huge number of changes might be executed this way. In some cases, users need to look at data directly. To look at data in a table, users use these transaction codes most frequently: SE16, SE16N, or SE17, SM30, SM34, SM31 or "proxy"-transactions.
Authorization Object S_TABU_DIS

Authorization object S_TABU_DIS is used to control table access. It determines what group of tables using authorization groups someone can look at, when they use any of the transaction codes above. The authorization object S_TABU_DIS controls complete access during standard table maintenance (transaction SM31), advanced table maintenance (transaction SM30) or the Data Browser (transaction SE16). If you need to control access to individual tables instead to groups of tables, you can use authorization object S_TABU_NAM (see section underneath).

You can assign a table to a specified group. Group assignments are defined in table TDDAT (transaction SE54). For Solution Manager, we deliver dedicated authorization groups for specific functions.

The following authorization groups are used in SAP Solution Manager:

<table>
<thead>
<tr>
<th>Authorization Group</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRMC</td>
<td>all CRM-related customizing views as CRM-based scenarios can refer to the same tables; and ICC</td>
</tr>
<tr>
<td>AISU</td>
<td>all S-USER-related tables</td>
</tr>
<tr>
<td>BI* (Remodeling, Repartitioning, Warehouse)</td>
<td>all BI-related tables</td>
</tr>
<tr>
<td>CHRM</td>
<td>other than CRM-related tables for Change Request Management</td>
</tr>
<tr>
<td>SDCO</td>
<td>all other than CRM-related tables for Incident Management</td>
</tr>
<tr>
<td>LMDB</td>
<td>all LMDB and SMSY-related tables</td>
</tr>
<tr>
<td>SMAN</td>
<td>Implementation and Upgrade-related tables</td>
</tr>
<tr>
<td>BPCA</td>
<td>Business Process Change Analyzer-related tables</td>
</tr>
<tr>
<td>TSTM</td>
<td>Test Management-related tables</td>
</tr>
<tr>
<td>SISE</td>
<td>Solution Manager Basic Configuration (transaction SOLMAN_SETUP) - related tables</td>
</tr>
<tr>
<td>DFWK</td>
<td>Dashboard Framework-related tables</td>
</tr>
<tr>
<td>SMAL</td>
<td>Monitoring and Alerting (Technical Monitoring) - related tables</td>
</tr>
<tr>
<td>SGEN</td>
<td>ES-Reporting and SUSEN-related tables</td>
</tr>
<tr>
<td>SARC, BCTA</td>
<td>Data Volume Management</td>
</tr>
<tr>
<td>SRCD</td>
<td>Rapid Content Delivery</td>
</tr>
<tr>
<td>BCSV</td>
<td>CRM: Status Profile Maintenance</td>
</tr>
<tr>
<td>DNO</td>
<td>CRM: Basis Message</td>
</tr>
<tr>
<td>Authorization Group</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SS</td>
<td>RS: SAP Control</td>
</tr>
<tr>
<td>DSA</td>
<td>Solution Manager DSA</td>
</tr>
<tr>
<td>IVIS</td>
<td>Integration Visibility</td>
</tr>
<tr>
<td>SEA</td>
<td>Solution Manager: Scope and Effort Analyzer</td>
</tr>
<tr>
<td>SGEN</td>
<td>Solution Manager: SUGEN</td>
</tr>
<tr>
<td>SISE</td>
<td>Solution Manager: SOLMAN_SETUP</td>
</tr>
<tr>
<td>SMAL</td>
<td>Solution Manager: Monitoring and Alerting</td>
</tr>
<tr>
<td>SMAN</td>
<td>Solution Manager: Implementation</td>
</tr>
<tr>
<td>SMCM</td>
<td>Solution Manager: Customer Life-Cycle Management</td>
</tr>
<tr>
<td>SMID</td>
<td>Solution Manager: Service Delivery</td>
</tr>
<tr>
<td>SMTA</td>
<td>Technical Administration</td>
</tr>
<tr>
<td>SMUA</td>
<td>Process Documentation: Administration Data</td>
</tr>
<tr>
<td>SMUD</td>
<td>Process Documentation: Instance Data</td>
</tr>
<tr>
<td>SMUG</td>
<td>Process Documentation: Authorization Groups</td>
</tr>
<tr>
<td>SMUL</td>
<td>Process Documentation: Library</td>
</tr>
<tr>
<td>SMUM</td>
<td>Process Documentation: Model Data</td>
</tr>
<tr>
<td>TSTM</td>
<td>Solution Manager: Test Management</td>
</tr>
<tr>
<td>SMGP</td>
<td>Solution Manager: Guided Procedure</td>
</tr>
<tr>
<td>SMRC</td>
<td>Solution Manager: Root Cause Analysis</td>
</tr>
<tr>
<td>SMTA</td>
<td>Solution Manager: Technical Administration</td>
</tr>
<tr>
<td>SMGD</td>
<td>Solution Manager: Service Delivery</td>
</tr>
<tr>
<td>SMDC</td>
<td>Solution Manager: Data Consistency Management (general)</td>
</tr>
<tr>
<td>SMDS</td>
<td>Solution Manager: Data Consistency Management (sensitive)</td>
</tr>
<tr>
<td>SMCB</td>
<td>Solution Manager: CBTA</td>
</tr>
<tr>
<td>SBPO</td>
<td>Solution Manager: Business Process Operations (Monitoring)</td>
</tr>
<tr>
<td>STAO</td>
<td>Solution Manager: TAO</td>
</tr>
</tbody>
</table>
### Authorization Group

<table>
<thead>
<tr>
<th>Authorization Group</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>USAG</td>
<td>Process Documentation: SMUD Usage</td>
</tr>
</tbody>
</table>

**Note**

Authorization object S_TABU_DIS is delivered with value asterisk (*) for roles assigned to prominent users in SOLMAN_SETUP such as SOLMAN_ADMIN and SOLMAN_BTC.

The majority of users in a production environment do not need direct access to tables. They view data through transaction codes. However, a few users might need access. When providing direct access to tables, you should use transaction SM30. Extra precautions should be taken for the selected users who require access to transaction SE16, because powerful access to a variety of data might be incorporated. You can make SE16 safer by creating a custom transaction code. With a custom transaction code, the user executes SE16 with a view of the table they require. This means they do not enter the table name, instead the custom transaction code takes them into transaction SE16 and directly into the table.

**Caution**

The combination of the object S_TABU_DIS with other objects can be critical:

- with ACTVT value 02 and S_TABU_CLI (see underneath) for S_TCODE SM30, SM31 allows maintenance of cross-client tables
- with ACTVT value 02 for S_TCODE SM30, SE16 allows unrestricted table maintenance (e.g. SAP_SUPPDESK_CONFIG, see Application - Specific Guide section on Incident Management)

### Authorization Object S_TABU_CLI

Authorization object S_TABU_CLI grants authorization to maintain cross-client tables with the standard table maintenance transaction SM31, extended table maintenance transaction SM30, the Data Browser. It acts as an additional security measure for cross-client tables and enhances the general table maintenance authorization S_TABU_DIS.

**Caution**

A combination of S_TABU_DIS value X, S_TABU_DIS value 02 for field ACTVT, and S_TCODE value SM30, SM31 is critical.

### Authorization Object S_TABU_NAM

The existing SAP table authorization concept is mainly based on the group assignment of tables and the authorization object S_TABU_DIS. But, authorization object S_TABU_DIS might not always be sufficient.
This authorization object contains the fields:

- **ACTVT**: display and change access similar to S_TABU_DIS
- **TABLE**: table name

With this object, the system checks the view names or table names directly, so that an exact authorization check is possible. In the function module `VIEW_AUTHORITY_CHECK`, the system checks S_TABU_NAM only if the authorization check on S_TABU_DIS was unsuccessful.

**Note**

Run report SUSR_TABLES_WITH_AUTH (see SAP Note 1500054) for analyzing table authorizations for a user or a single role. You can use this program to selectively determine the authorizations for the object S_TABU_DIS or S_TABU_NAM with regard to the tables that can be accessed using it. Transaction SU24_S_TABU_NAM reduces the effort required for maintaining authorization default values during the introduction of an authorization concept with S_TABU_NAM.

See also the following SAP Notes:

- [1481950](#) Information on the new authorization check for generic table access
- [1541577](#) Impact of S_TABU_NAM in Risk Analysis and Remediation

### 4.12.4 ABAP Objects: Authorization Object S_DEVELOP

**S_DEVELOP** is the general authorization object for ABAP Workbench objects. You use it to grant access authorizations for all ABAP Workbench components, which include the following:

- ABAP development tools
- ABAP Dictionary and Data Modeler
- Screen Painter and Menu Painter
- Function Builder
- Repository Browser and Info System
- SAP SmartForm

From a production perspective, it is considered critical if authorization object S_DEVELOP is assigned to users. In general, authorization object S_DEVELOP with more than display access (ACTVT 03) is not required by any user in production.

**Note**

The authorization object is assigned for maintaining transaction SNOTE during the SAP Solution Manager basic setup to the SOLMAN_ADMIN user in role SAP_SETUP_BASIC_S_DEVELOP. After implementing all required SAP Notes into the system, you can set the according authorization object inactive. Documentation is given in the Guided Procedure for the automated setup.
Caution

The combination of field values for S_DEVELOP is critical:

- object types STRU (structure), TABL (table), and ACTVT values 07, 40, 41, 42 for S_TCODE SE11 allows maintenance of data dictionary objects.
- object type FUGR (function group) with ACTVT 16 for S_TCODE SE37 allows RFC via function calls.
- object types DEBUG (debugging), PROG (program) with ACTVT value 02, and S_PROGRAM with ACTVT value SUBMIT for S_TCODE SE38 allows replacing and debugging of reports. Note here as well, that S_TCODE SE38 should never be granted to general end-users. In combination with S_TCODE SE80 it allows programming (active in role SAP_DVM_SERVICE (needs access programming tools), see Application - Specific Guide for DVM)
- object type TABLE (table) with ACTVT value 02, and S_TABU_DIS with ACTVT value 02 for S_TCODE SE16, SE16N allows replacing and debugging of tables.
- object type TRAN (table) with ACTVT value 01, 02 for S_TCODE SE93 allows maintenance of transaction codes.

4.12.5 Start Authorization Objects S_START, S_TCODE, and S_SERVICE

Transactions, Web Dynpro Applications, and OData - Services posses so-called start authorization objects. These authorization objects are called when the user calls a transaction, a WebDynpro Application, or an OData - Service.

Authorization Object S_TCODE for Transaction

To be able to run any transaction in any SAP System, authorization object S_TCODE is called by the system and must be assigned to the user running the transaction.

Caution

S_TCODE should only contain the transaction codes that the user is allowed to run.

Authorization Object S_START for Web Dynpro Application

S_START substituting S_SERVICE

Web Dynpro Applications have start authorization object S_START. S_START is delivered with SAP BASIS Release 7.40. This authorization object substitutes authorization object S_SERVICE as the start authorization object.
Authorization Object S_SERVICE for OData - Services

OData Services have start authorization object S_SERVICE.

External Services are also protected by authorization object S_SERVICE.


With Release 7.2 SAP Solution Manager and SAP Basis 7.40, you can define group - specific security policies in regard to Logon and Passwords for your users. For users who should not use the default attributes, you can define individual security policies in transaction SECPOL, and assign it to users in transaction SU01 (transaction SU10 for mass maintenance). For more information, see http://help.sap.com/saphelp_nw70ehp1/helpdata/EN/7f/c52442ad9f5133e10000000a155106/content.htm

Security Policy Parameters to Be Used

Table 15:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECK_PASSWORD_BLACKLIST</td>
<td>Check the Password Blacklist</td>
<td>1</td>
</tr>
<tr>
<td>DISABLE_PASSWORD_LOGON</td>
<td>Disable Password Logon</td>
<td>0</td>
</tr>
<tr>
<td>DISABLE_TICKET_LOGON</td>
<td>Disable Ticket Logon</td>
<td>0</td>
</tr>
<tr>
<td>MAX_FAILED_PASSWORD_LOGON_ATTEMPTS</td>
<td>Maximum Number of Failed Attempts</td>
<td>5</td>
</tr>
<tr>
<td>MAX_PASSWORD_IDLE_INITIAL</td>
<td>Validity of Unused Initial Passwords</td>
<td>0</td>
</tr>
<tr>
<td>MAX_PASSWORD_IDLE_PRODUCTIVE</td>
<td>Validity of Unused Productive Passwords</td>
<td>0</td>
</tr>
<tr>
<td>MIN_PASSWORD_CHANGE_WAITTIME</td>
<td>Minimum Wait Time for Password Change</td>
<td>1</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>MIN_PASSWORD_DIFFERENCE</td>
<td>No. of Different Chars When Changing</td>
<td>1</td>
</tr>
<tr>
<td>MIN_PASSWORD_DIGITS</td>
<td>Minimum Number of Digits</td>
<td>0</td>
</tr>
<tr>
<td>MIN_PASSWORD_LENGTH</td>
<td>Minimum Password Length</td>
<td>6</td>
</tr>
<tr>
<td>MIN_PASSWORD_LETTERS</td>
<td>Minimum Number of Letters</td>
<td>0</td>
</tr>
<tr>
<td>MIN_PASSWORD_LOWERCASE</td>
<td>Minimum Number of Lowercase Letters</td>
<td>0</td>
</tr>
<tr>
<td>MIN_PASSWORD_SPECIALS</td>
<td>Minimum Number of Special Characters</td>
<td>0</td>
</tr>
<tr>
<td>MIN_PASSWORD_UPPERCASE</td>
<td>Minimum Number of Uppercase Letters</td>
<td>0</td>
</tr>
<tr>
<td>PASSWORD_CHANGE_FOR_SSO</td>
<td>Password Change Req. for SSO Log-ons</td>
<td>1</td>
</tr>
<tr>
<td>PASSWORD_CHANGE_INTERVAL</td>
<td>Interval for Regular Password Changes</td>
<td>0</td>
</tr>
<tr>
<td>PASSWORD_COMPLIANCE_TO_CURRENT_POLICY</td>
<td>Password Change After Rule Tightening</td>
<td>0</td>
</tr>
<tr>
<td>PASSWORD_HISTORY_SIZE</td>
<td>Size of the Password History</td>
<td>5</td>
</tr>
<tr>
<td>PASSWORD_LOCK_EXPIRATION</td>
<td>Automatic Expiration of Password Lock</td>
<td>0</td>
</tr>
</tbody>
</table>

**Authorization objects S_SECPOL and S_SECPOL_A**

If you are using security - policies for your users, you need to maintain authorization object S_SECPOL, and if required also authorization object S_SECPOL_A. Authorization object S_SECPOL is delivered in state *Inactive* in role SAP_SM_USER_ADMIN.
4.13 Authorization Object SM_SETUP

Authorization object SM_SETUP allows you to protect the Solution Manager configuration transaction SOLMAN_SETUP. It controls, if a user can access transaction SOLMAN_SETUP. You can restrict access on the following levels:

- Activities
- Scenarios/Procedures
- Steps within a procedure

In case:

- you allow display authorization (ACTVT 03) for any scenario, the user is not allowed to edit any step within the procedure in question.
- your security policy only allows certain users to maintain a specific set of steps within the procedures, you can restrict on procedure and step level.
- a user does not have this authorization object assigned, but still has access to the transaction via authorization object S_TCODE using the work center for SAP Solution Manager configuration (also using WDA: AGS_WORKCENTER), data are not displayed by the system in the User Interface.

4.14 How to Build Your Own Authorization Concept

Use

Since there is no general authorization configuration that fits all possible use scenarios, we recommend that you design an authorization concept tailored to your specific use scenario.

How you maintain authorization objects and bundle them depends on your company’s security concept. You customize/maintain your roles according to your company’s concept. Each company has different priorities, departments and so on. As each business requires a different authorization concept, the template roles delivered by SAP are only templates. Before you grant authorizations to your end users, you must have a clear concept of who is to receive which authorizations, because you need to adjust your authorizations over time due to company changes or extended use of Solution Manager functions. Here is what you should consider when designing your authorization concept.

Note

All the authorization mechanisms must be configured (and configured consistently) to provide appropriate security.

Procedure

1. Identify which functions/capabilities of Solution Manager scenarios you use.
2. Create a menu matrix according to these functions/capabilities.
3. Identify your roles.
4. Populate your menu matrix.
5. Create your roles from SAP template roles. Use a unique naming convention.
6. Maintain your roles.
7. Test your roles.

4.15 Creating Configuration User Roles for SAP Solution Manager Using IMG Project

Use

There are:
- specified roles for the automated basic settings configuration (transaction SOLMAN_SETUP)
- dedicated authorization roles for scenario-specific configuration done in transaction SOLMAN_SETUP
- no dedicated authorization roles for scenario-specific configuration done in transaction SPRO

This section tells you how to create your own roles for the configuration of scenarios.

Note

Configuration of scenario—specific functions can involve configuration of cross-scenario settings. For these functions, additional configuration roles may be needed (if you do not use profiles SAP_ALL and SAP_NEW). They are specified in the IMG activity for cross-scenario functions.

To be able to create authorization roles for scenario—specific configuration, you have created an IMG project in transaction SPRO_ADMIN.

Procedure

Note

This procedure is based on the example customizing project in the How-to document How to Create Customizing Projects and Project IMGs.

1. Create an IMG Project (See section More Information)
   Before you can create a role for scenario-specific configuration, you need to create an IMG project. This project is the basis for role configuration as it contains all transactions you run later on.
2. Create a Role in Transaction PFCG
   1. Choose transaction PFCG.
2. Enter a role name in your name space, for instance: \texttt{ZROLE\_IMG\_MYPROJECT} and choose button \textit{Single Role}.

3. Enter a description for your role, for instance: \texttt{IMG project: Implementation/Upgrade as of ST SP15}.

4. Save your role.

\begin{itemize}
\item \textbf{Note}
\begin{itemize}
\item You are asked for a transport request.
\end{itemize}
\end{itemize}

3. \textbf{Define Configuration Transactions for Your IMG Project}

In role creation, transactions form the basis to easily maintain all necessary authorization objects. When you enter a transaction in the menu tab in your role, the system traces all authorization objects required for this transaction.

\begin{itemize}
\item To receive all transactions which are contained in the customizing project, choose in the menu: \textit{Utilities Customizing auth.}
\item In the appearing dialog box, choose button \textit{Add} to attach your customizing project or customizing project view. In our case, we choose the customizing view that was created.
\item In the various dialog boxes, choose your customizing project or customizing project view, in our case \texttt{myproject}.
\item The system automatically assigns all relevant transactions and authorization objects for your customizing project or customizing project view.
\item Confirm your project assignment.
\end{itemize}

4. \textbf{Maintain Authorization Objects}

Authorization object defaults delivered by SAP contain minimal authorizations. To grant full authorization for the according authorization objects you need to maintain these objects.

\begin{itemize}
\item In the \textit{Role Maintenance}, choose tab \textit{Authorizations}.
\item Choose button \textit{Change}.
\item Maintain all activity values per authorization object according to your needs, for instance if you want to grant full authorization, always choose all activities.
\item \textbf{Caution}
\begin{itemize}
\item All authorization objects need to receive a green traffic light. Beware, that the authorization trace does not trace values for critical authorization objects \texttt{S\_RFC} and \texttt{S\_TABU\_DIS}.
\end{itemize}
\item Generate the profile.
\item To assign this profile to a user, choose tab \textit{User}, add your user in the table and execute the user comparison.
\item Save.
\end{itemize}

**Result**

You have now created a role for your specific \texttt{IMG} configuration project.
Caution

If a project or a project view was assigned to a role, you cannot manually assign any transactions to this role and vice versa. You should therefore only use the role to generate and assign Customizing authorizations.
Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with “you”, or a gender-neutral noun (such as “sales person” or “working days”) is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).
go.sap.com/registration/contact.html