SECURITY GUIDE | PUBLIC
Document Version: 7.2 SPS 8 – 2018-12-07

Authorization Concept Guide - SAP Solution Manager 7.2 SPS 8

THE BEST RUN SAP

Content

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: https://help.sap.com/viewer/p/SAP_Solution_Manager ▶ *SAP Components* ▶ *SAP Solution Manager* ▶ *<current release>* ▶.

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

Support Package Stacks (Version)	Date	Description
SP01	2015 / 12 / 11	**General Information** • As of Release 7.2, the security information is published within three separate SAP Solution Manager guides: 1. *Authorization Concept Security Guide* This guide contains all information referring to the general concept of security and authorizations for the complete stack for SAP Solution Manager. 2. *Secure Configuration Security Guide* 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. 3. *Application-Specific Security Guide* This guide contains all information referring to security aspects and authorizations for individual scenarios/applications. **New Process Documentation Functionality** ○ *Obsolete Transactions and Authorizations* 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)*. ○ 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. ○ *Solution Content Activation (Migration) Information* Information on the migration of existing projects and solutions to the new process documentation functionality is given in the *Landscape Setup Guide: Secure Configuration*. **Work Center Role Navigation Concept** ○ All roles SAP_SMWORK_BASIC_* are obsolete, see sections on *Work Center Navigation Roles* and *Authorizations for User Interfaces.*. ○ 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*. **Authorization Object Status** ○ New section describing authorization objects status in role for SAP Solution Manager (Software Component ST) **Critical Authorization Objects** ○ extension of existing sections on SAP_BASIS authorization objects ○ additional section on Solution Manager authorization object SM_SETUP **SAP Fiori User Interface / NWBC**

Support Package Stacks (Version)	Date	Description
		○ 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. ○ Some scenarios, such as `ITPPM`, 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`. **Section: Authorizations and Roles for Infrastructure** ○ Authorization object `AI_LMDB_PS` is obsolete, and only included in roles `SAP_SYSTEM_REPOSITORY_*` with `ACTVT 03` (Display) ○ Information on *Embedded Search* functionality, (used in a number of scenarios) **Dashboard Builder** • New framework for Dashboards delivered and new roles for it, see section Using SAP Solution Manager with Business Warehouse (BW). **i Note** The following role as of release 7.1 is obsolete: ○ `SAP_SM_DASHBOARDS_DISP_ALM`
`SP02`		**SAP Fiori User Interface** • added information in regards to `VSCAN` Documentation for upload of data.

Support Package Stacks (Version)	Date	Description
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** ⚠ Caution 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
SP05	2017 / 05 / 08	**Template Dialog Users and Composite Roles** Template Users are available for all SAP Solution Manager scenarios in application *Solution Manager Users Administration* (SMUA) and *Template Users*, see more information on SMUA in the according section in the *Secure Configuration Guide*. **Dashboard Configuration** Adapted dashboard roles SAP_SM_DSH_* for *Test Suite* **Guided Procedure** Adapted GP roles SAP_SM_GP_* **New: SAP Fiori App Security Guide** For SAP Fiori Apps (ST-UI), an individual guide is published on the SAP Support Portal. All relevant information on SAP Fiori Apps has been moved to this guide.

Support Package Stacks (Version)	Date	Description
SP06	2017 / 10 /31	**Guided Procedure** Adapted GP roles SAP_SM_GP_* with new SM_UPLOAD with value UL **Roles for Infrastructure** Added authorization object S_WDC_P13N to roles SAP_SYSTEM_REPOSITORY_***
SP07	2018 / 05 /14	**Composite Roles** As of SP07, composite roles in SAP Solution Manager are no longer supported. All *business user definitions* with accordingly assigned roles are available with their documentation in application Solution Manager User Administration (SMUA) and in transaction SOLMAN_SETUP. For more information on business users (Use Case IDs), see the according section in this guide. For more information on the application SMUA, see the *Secure Configuration Guide*. **Moved Section on Critical Authorizations** Section *Critical SAP BASIS Authorization Objects* moved to the *Security Optimization Guide*. **Removed Sections** Removed sections on *How to Build Your Own Authorization Concept* and *Creating Configuration User Roles for SAP Solution Manager Using IMG Project*. **New Section** New section on *Social Application Integration Framework*. **Updated Roles** • Adapted Dashboard roles SAP_SM_DSH_* with new Dashboard categories and IDs. • Adapted embedded Fiori role SAP_SM_FIORI_LP_EMBEDDED
SP08	2018 / 12 /03	**Dashboard Roles** Obsolete Dashboard roles set to obsolete in the description tab of the roles: • SAP_SM_DASHBOARDS_DISP_LMDB • SAP_SM_DASHBOARDS_DISP_VBD • SAP_SM_DASHBOARDS_DISP_EEM • SAP_SM_DASHBOARDS_DISP_CIO_BPO • SAP_SM_DASHBOARDS_DISP_SAM **Notifications in Guided Procedure** To allow notifications in GP, you need to assign role SAP_NOTIF_***. See section *Guided Procedure Framework*.

2 Security Guide - General Concepts

Use

> ⚠ Caution
>
> **Usage Rights for SAP Solution Manager**
>
> For usage rights, check the following information in SAP Support Portal at: http://support.sap.com/solution-manager/usage-rights.html

With every Support Package, this Security Guide is updated in SAP Support Portal at: https://help.sap.com/viewer/p/SAP_Solution_Manager.

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: https://help.sap.com/viewer/p/SAP_Solution_Manager.

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 SAP Support Portal at: https://help.sap.com/viewer/p/SAP_Solution_Manager.

What is Your Opinion?

We are always interested in how we can improve our documentation to your needs. In the Support Portal, you can leave your feedback online, which is regularly checked by us.

More Information

For a complete list of the available SAP Security Guides, see SAP Support Portal: https://help.sap.com/viewer/p/SAP_Solution_Manager

3 Introduction

3.1 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.

3.2 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.

4 Authorization Concept for SAP Solution Manager

4.1 User and Roles Concept in SAP Solution Manager

Business 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.

User ID

In transaction `SU01` (User Management), the user receives a User ID.

Use Case ID

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 business user definitions are mapped to **Use Case ID**s in SAP Solution Manager transaction `SOLMAN_SETUP` and application SMUA. Each Use Case ID is assigned a specific set of roles which is specifically designed to allow the defined tasks for this user. SAP has defined a task list/definitions for each Use Case ID, which is documented for each Use Case ID in the system. These tasks/definitions are templates to be used and can easily be modified. In case you modify, you need to adapt authorizations and roles accordingly.

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.

> **i** Note
>
> As of SP07, the composite role concept is obsolete. That means, it is no longer maintained. Transaction `SOLMAN_SETUP`, application SMUA, and the *Application Security Guide for SAP Solution Manager*, each contain all relevant information as to which single roles are required for the according Use Case ID. For additional information, see the *Application Security Guide for SAP Solution Manager* for this function/ scenario.

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 Use Case 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 '*' (asteriks 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. For more information, see the *Secure Configuration Guide*.

- **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 use case ID `SA`, see also section on Solution Manager administration in the application specific guide.

  > **i** Note
  >
  > You can use default user `SOLMAN_ADMIN` also for administration when adding the single roles for Use Case ID SA. Nevertheless, we recommend to have a separate user for administration.

- **End - Users of SAP Solution Manager**
  For each scenario, we deliver business user definitions and according Use Case IDs. There is always a user with *full administration authorization* and a user with *display authorization* delivered (see *section Multilevel Separation*).

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 build 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 Use Case IDs have a number of single roles assigned, which easily allow a further restriction of authorizations for a user. Each single role defines the authorization for one specific function/ module/transaction. This may include roles for work center navigation, work center authorization, `BW` - related authorizations, `CRM` - related authorizations, function - related authorizations, and so on. 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.

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

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*.

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.
>
> 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.

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 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.

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, SOLMANREQU>. 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.

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

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.
>
> 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.
>
> 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 filledwith 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

Overview

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 live, or whether you are already live. 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:
  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 `SAP_SYSTEM_REPOSITORY_*` 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.

- User Management and Role Management: SAP_SM_USER_*
  This role contains both *User Management and Role Management* authorization. It is assigned to every SMC* user and therefore highly security -critical.
- 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.
- 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.

4.6 User Interfaces in SAP Solution Manager

4.6.1 Embedded SAP Fiori Launchpad Role Concept

> **i** Note
>
> As of SP05, preferred User Interface is SAP Fiori Embedded Launchpad.

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.

The navigation role needed for the user to execute tasks, SAP_SMWORK_<WorkCenter>, is assigned automatically in user creation during setup.

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 SAP Support Portal 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*.

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)`.

> ℹ 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 theSAP_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 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.

4.6.2 Authorizations for User Interfaces

In general, *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.

Example

Case 1: activity is independent on other context information

In transaction SOLMAN_SETUP, the button *Edit* allows users to decide on editing mode for the transaction. This button is controlled by authorization object SM_SETUP, and specifically with activity 02 CHANGE. If a user does not have this authorization value, the system does not display the button *Edit* in the User Interface.

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.

> **i Note**
>
> This principle does not yet apply to all applications in SAP Solution Manager.

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

- `ABAP` WebDynpro
- `BSP` based technology (`CRM 7.01 WebClient UI`)
- `ABAP SAPGUI` transactions
- Java WebDynpro (Java stack)

All *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.

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*.

> **i Note**
>
> All delivered roles are updated in this regard from Release 7.1 to Release 7.2.

Restricting Work Center Navigation View Panel - Authorization Object: SM_WC_VIEW

> **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:

1. Choose transaction SM30.
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:

1. Activate BAdI: AGS_WORK_AUTH_SM_WC_VIEW in Enhancement EHN_AGS_WORK_AUTH_UI (activate via transaction SOLMAN_SETUP)
2. Activate BAdI: AGS_WORK_AUTH_F4_TRACE in Enhancement EHN_AGS_WORK_AUTH_TRACE (activate via transaction SPRO).
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
- System and Application Monitoring
- SAP Solution Manager Configuration
- Solution Manager Administration
- Root Cause Analysis
- Data Volume Management

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.

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.
3. On the menu, choose *More*, and *Hide Elements*.
   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

> **Note**
>
> If you want to customize your Work Centers for branding or adapting the Web Dynpro Logon Screen, see SAP Note 1160651.

CRM Web Client User Interface Authorization

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.

Authorization Object C_LL_TGT

Authorization object C_LL_TGT is required within the CRM Web Client User Interface for Links to ITSM Reporting and HTML mail formats.

ABAP SAPGUI Transactions

SAP GUI 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

The following single roles are necessary for any Guided Framework to run:

- SAP_SM_GP_PLUGIN (Guided Procedure SAP Note PlugIn)

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

- SAP_SM_GP_EXE (Guided Procedure execution)
- SAP_SYSTEM_REPOSITORY_DIS (System display access)
- SAP_SUPPDESK_CREATE (Incident creation)

Authorization Object SM_GPACUST

SM_GPACUST is the main authorization object for Guided Procedure.

Authorization Object SM_UPLOAD

SM_UPLOAD allows upload of images to Guided Procedure, for instance SOLMAN_SETUP. The object is deactivated in roles SAP_SM_GP_EXE and SAP_SM_GP_ADMIN.

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.

You Want to Customize Your GP

SAP_SM_GP_ADMIN

If you want to customize your own Guided Procedure, assign SAP_SM_GP_ADMIN. This role contains the critical authorization object S_SYS_RWBO with ACTVT 01, 02, 03 , and the 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.

SAPscript

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

Notifications

Guided Procedure offers the possiblity to send mail reports using the central notification framework. To allow this, you need to assign role SAP_NOTIF_* to your user.

4.8 Social Applications Integration (SAI) Framework

Within the SAI framework, you can create your own OData - Services and configurations to be able to connect Social Media Applications to your application.

SAP Solution Manager Social Application Integrator (SAI) enables you to expose your SAP Solution Manager based self-developed functions to a Social Application platform like *Facebook Messenger*, *Skype*, or *WeChat* (as known as *WeiXin*). Typical usage scenarios:

- you like to be informed by a Social App client which is installed on your mobile, e.g. a Solution Manager alert from *Technical Monitoring* is pushed to the responsible employee's *Facebook Messenger*
- you like to operate functions provided by Solution Manager via a Social App in your mobile, e.g. a Change Manager approves a *Request for Change* in *WeChat*

> **i Note**
>
> It is in your responsibility to use it in a secure way.

User and Their Roles

You can create your own OData service with annotation. The following transactions are available in the roles:

- `SMSAI_ADMIN`: Administration
- `SMSAI_BUILD`: Generation

> **i Note**
>
> As the roles are not assigned by default to one of the Use Case IDs in SAP Solution Manager, all authorization fields which cannot be prefilled by SAP remain empty. You need to maintain authorizations for the roles in transaction `PFCG`.

Administrator

As administrator, you are allowed to access the SAI administration application and the application log to monitor the SAI status. The role `SAP_SM_SAI_ADMIN` contains authorization for administration.

Developer

As developer, you are able to create OData Services in the Solution Manager system, access the *Manifest* tool and create manifest, as well as access the application log for trouble shooting. The role `SAP_SM_SAI_DEV` contains authorization to develop SAI OData - services and their annotations. For the user to be able to use the development environment and transport, additional authorizations must be assigned to the user, such as `S_DEVELOP` and `S_TRANSPRT`.

End-User

The end-user is allowed to display the SAI service configuration. The role `SAP_SM_SAI_READ` contains authorization for display. The end-user is the person who uses the social app and consumes the SAI service which is built by the developer.

> **i Note**
>
> The OData Service that is built is itself protected by the start authorization object `S_SERVICE`.

Technical User Role

If you are using the scenario with a Cloud solution, you require a technical user with role `SAP_SM_SAI_TECH` for connecting.

Authorization Object SM_SAI

The authorization object allows restriction to:

- `ADMIN` define, enable, disable services; map Solution Manager user and social app user; disable/enable user, assign service to users
- `BUILD_SERVICE` it stands for SAI service building related functions, for example the manifest generation tool
- `MONI` monitoring communication data related functions

> **i Note**
>
> Not yet in use with SP07.

Application Log Authorization

The application log is accessed via transaction `SLG1` and object `SAI_LOG`.

S_DEVELOP

For Project Generation, you require to have gateway access and authorization object `S_DEVELOP` for modification purposes. Due to the criticality of the object, you need to maintain it manually.

4.9 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.

> **i** Note
>
> All ABAP roles referring to J2EE security (UME) are shipped in the SAP name space. These roles should not be copied into any other name space, as they connect through their technical name the user management of theABAP stack with the user amangement of the Java stack.

For more information see help for Java Roles https://help.sap.com/saphelp_erp60_sp/helpdata/en/44/0761cea5c610b3e10000000a11466f/frameset.htm

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

4.10.1 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 **three** navigation roles 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`
- `SAP_SM_CRM_UIU_SOLMANDSPTCH`

- SAP_SM_CRM_UIU_SOLMANREQU

In SAP Solution Manager only these roles are required as CRM Business Roles. 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.

4.10.2 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

> **i Note**
>
> This object is usually inactive, see section *Authorization Method*.

- CRM_ORD_OE
- CRM_ORD_OP
- CRM_ORD_PR
- CRM_SEO
- CRM_TXT_ID

> **i Note**
>
> This object is only required if information texts are used.

- B_USERSTAT

> **i Note**
>
> This object defines the change of status executed by the end-user.

- B_USERST_T

> **i 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.

4.11 Using SAP Solution Manager with Business Warehouse (BW)

4.11.1 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*.

4.11.2 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 for instance the following applications:

- Incident Management Reporting
- Test Workbench Reporting

Reporting data extracted from a managed system

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

- End - User Experience Monitoring Reporting
- Process Integration Monitoring Reporting
- Change Reporting
- Alert Reporting
- Early Watch Alert Sessions
- Business Process Monitoring
- Job Monitoring
- Data Base Performance Reporting
- Data Volume Management Reporting

Reporting data extracted from BW systems

The third type is extracting data from the BW-system. BW-system reporting application:

- Monitoring and Alerting

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

> **i Note**
>
> For an easy configuration, minimization of remote accesses and simple user administration, SAP recommends that you set up the BW system component in the current client of your SAP Solution Manager system. This is the Standard Scenario, which is the default setting in the SAP Solution Manager Configuration. Also note that using a separate BW system is no longer supported for a new setup (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*.

Standard Scenario	Remote Scenario	Additional Remarks
Configure BW and Activate Content		
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.		
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 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.	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.	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		

Standard Scenario	Remote Scenario	Additional Remarks
The job EFWK RESOURCE MANAGER is scheduled by user SOLMAN_BTC. SOLMAN_BTC 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		
Extractors in the local system are started by technical user SM_EFWK. Extractors in the managed systems are run by the READ user as the READ RFC destination is used.	Extractors in the local system are started by technical user SM_EFWK. Extractors in the managed systems are run by the READ user as the READ RFC destination is used. Extractors in the BW - system are run by the technical user SM_BW_<SolManSID> via RFC connection SM_BW_<BI_SID>CLNT<BIClient>.	
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		

Standard Scenario	Remote Scenario	Additional Remarks
According to the individual scenarios, users are provided as Use Case IDs. These users include BW - reporting roles (single roles). These users 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, users are provided as Use Case IDs. These users include BW - reporting roles (single roles). These users 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.	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.

4.11.4 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).

4.11.5 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 **assigned automatically in solman_setup**. 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 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.

4.11.6 Dashboard Builder: Using Dashboards for 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.

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.

> **i Note**
>
> The following Dashboards are still supported by the OLD Framework:
>
> - My Dashboard
> - Business Process Operations Dashboard
> - Ici 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.
- `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_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.

Logging

Dashboard application does not supply logging functionality. The application relevant for dashboards provide the log information.

Development Authorization S_DEVELOP

Authorization object S_DEVELOP with ACTVT 03 (display) and DEVCLASS: AI_SOLMAN_SVCP_EXTRACTORS, AGS_SMT_FWK_REPT and AI_DSH_BUILDER is required for dashboards of source type BAdI.

4.12 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.

Name	Remarks
SAP_BC_WDHC_ADMINISTRATOR	Authorization to administer Help Center
SAP_BC_WDHC_POWERUSER	Authorization to use Help Center

Prerequisite

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

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP