Security Guide **PUBLIC**

Document Version: 2.0 – 2017-10-16

Authorization Concept Guide - SAP Solution Manager 7.2 SPS 6

Content

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

This Security Guide is updated in the SAP Service Marketplace at: http://service.sap.com/instguides *SAP Components* *SAP Solution Manager* *<current release>* with every Support Package.

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>*.

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 *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 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 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 *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 four separate guides: ○ *SAP Solution Manager Authorization Concept* This guide contains all information referring to the general concept of security and authorizations for the complete stack for SAP Solution Manager. ○ *SAP Solution Manager Secure Configuration 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. ○ *SAP Solution Manager Application 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). **Note** The following roles as of Release 7.1 are obsolete: ○ `SAP_SM_DASHBOARDS_DISP_ALM` ○ `SAP_SM_DASHBOARDS_DISP_CIO_BPO` ○ `SAP_SM_DASHBOARDS_DISP_EEM` ○ `SAP_SM_DASHBOARDS_DISP_LMDB` ○ `SAP_SM_DASHBOARDS_DISP_SAM` ○ `SAP_SM_DASHBOARDS_DISP_VBD`
`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 Service Marketplace. 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_***

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 '*' (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.

  > **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 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 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, `RFC`s, 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`

- 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.

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.

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

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 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 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:
  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.

  > **Note**
  >
  > If this role (or the corresponding authorization objects) is 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.

Process Documentation

Role	Included Authorization Objects
SAP_SM_SL_DISPLAY	The role contains all relevant authorizations for process documentation in display mode.
SAP_SM_SL_EDIT	The role contains all relevant authorizations for process documentation for editing processes.
SAP_SM_SL_EDIT_BPMN	The role contains all relevant authorizations for process documentation for editing, and maintenance authorization for Business Process Graphics 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.

Authorization Object SM_SDOC

This object is relevant for being able to restrict processes/solutions.

Authorization Object SM_SDOC_ADM

This object restricts solutions on the administrative level.

Authorization Object SM_GAL_GO

This object is specific for role SAP_SM_SL_EDIT_BPMN. It allows for restricting the use of graphical objects for Business Process Operations in Process Documentation.

Document Management and Digital Signature

Role	Included Authorization Objects
SAP_SM_KW_DIS	The role contains all relevant authorizations for Documentation Management in display mode.
SAP_SM_KW_EXE	The role contains all relevant authorizations for Documentation Management for editing documents.
SAP_SM_KW_ALL	The role contains all relevant authorizations for Document Management administration.

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 role SAP_SM_ESH*. You can use role SAP_SM_ESH_ADM to configure the view: Embedded Search. For more information, see section on *View Embedded Search* in the *Secure Configuration Security Guide*. All authorization objects related to Embedded Search have the following naming convention: S_ESH_*.

System Landscape

Role	Included Authorization Objects
SAP_SYSTEM_REPOSITORY_DIS	The role contains all relevant authorizations for systems AI_LMDB_* in display mode, as well as: • SM_CMDB_OB • SM_SETUP manually entered

Role	Included Authorization Objects
SAP_SYSTEM_REPOSITORY_ALL ➡ Recommendation This role is assigned to all SMC* users. After configuration of the required scenarios, either remove this role from your user and replace it with role SAP_SYSTEM_REPOSITORY_DIS, or deactivate the SMC* user.	Additional to all authorization objects for SAP_SYSTEM_REPOSITORY_DIS the role includes as well: • AI_LMDB_AD • AI_LMDB_RE • AI_LMDB_TM ➡ Recommendation As this object is only required in the context for Transport Management, set it inactive if not needed. • S_TCODE; TCD value LMDB
SAP_SYSTEM_REPOSITORY_EDIT	This role allows for editing LMDB specific data in any application. It contains authorization object AI_LMDB_OB in edit mode.

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 roles 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*.

> ℹ 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.

Authorization Object AI_LMDB_RE

This authorization object is relevant for the remote access to the LMDB. It is contained only in role SAP_SYSTEM_REPOSITORY_ALL. If you do not require this object, we recommend to remove it or set it inactive in the role.

Authorization Object AI_LMDB_AD

This authorization object is relevant for the administration of the LMDB. It should only be assigned to the administrator of the LMDB.

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

Role	Included Authorization Objects
SAP_SM_RFC_*	• S_RFC_ADM • S_ADMI_FCD • S_RFC_TT manually added due to its criticality Additionally authorization objects S_TCODE and S_SERVICE

Business Partner

Role	Included Authorization Objects
SAP_SM_BP_*	The role contains all relevant authorizations for business partner and product assignment for POWL queries SMWORK_TSYS_DIAG_REL and SMWORK_DIAG_ALL • B_BUPA_RLT • COM_IL All additional authorization objects for business partners can, but must not necessarily be used.

User and Roles Management

Role	Included Authorization Objects
SAP_SM_USER_*	The role contains all relevant authorizations for User Management and Roles Management • transaction SU01 • transaction PFCG **Recommendation** We strongly recommend to remove this role after configuration from he assigned user.

4.6 User Interfaces in SAP Solution Manager

4.6.1 Work Center Navigation Role Concept

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.

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)`.

> **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 `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.

> **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

> ℹ 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_SW_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
- 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.

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.
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

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)

  > **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)

> **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

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.

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.

> **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.

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 **three** 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`
- `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.

4.9.2 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.

- B_USERSTAT

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

- B_USERST_T

> **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*.

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 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.	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, 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.	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 Dashboard Builder: 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.

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_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.

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)

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

Return Code	Explanation	To Do
0	Invalid logon data (user and client) for the trusting system	Create a corresponding user in the client system for the user in the server system (trusting system)
1	The calling system is not a trusted system, or the system security ID is invalid.	Create the trusted RFC connection again.

Return Code	Explanation	To Do
2	The user has no authorization containing the authorization object `S_RFCACL`, or is logged on as the protected user `DDIC` or `SAP*`.	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`)
3	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.	Synchronize the system times

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.

Usage in Transaction SOLMAN_SETUP

Within transaction `SOLMAN_SETUP`, you can create end-users (template users) for all required scenarios. If the scenario, you want to create users for, requires a mandatory trusted RFC - connection, the system assigns either role `SAP_SM_S_RFCACL` or `SAP_SM_BW_S_RFCACL` (BW-System) are assigned. These roles contain the authorization object.

> **Recommendation**
>
> We recommend to check carefully, whether you require trusted RFC. If you require the authorization object, please maintain it specifically for your purposes, such as correct `System ID, Client`, and `User` in question.

How to Maintain S_RFCACL

> **Recommendation**
>
> How to maintain the object:
>
> - `RFC_SYSID : <System Id of the Solution Manager>`
> - `RFC_CLIENT: <Client of the Solution Manager>`
> - `RFC_USER : ' '`

- `RFC_EQUSER: Y` (for Yes)
- `RFC_TCODE : ' '` (if transaction flag is not active in transaction `SMT1`)
  The SAP Solution Manager managed system setup generates a Trust relationship with an inactive transaction flag. This is the recommended setting for the remote scenario used by the SAP Solution Manager. You can view the transaction flag for a single trust relationship in transaction `SMT1` respective for all trust relationships in transaction `SE16` for table `RFCSYSACL` (field `RFCTCDCHK = X`).

  > **Note**
  >
  > If you another remote scenarios which are based on Trust relationship, then it might be the case that you activate the transaction flag in transaction `SMT1`, for instance in case of the GRC FireFighter application which requires to activate this flag. In this case you should change the value for field `RFC_TCODE` from `' '` to `*`. Despite the fact, that we do not recommend to install the central GRC on the SAP Solution Manager system, you should be aware that this requirement is relevant if you install the central GRC elsewhere, but use GRC FireFighter in local mode.

- `RFC_INFO : <Installation Number of the Solution Manager>`
- `ACTVT : 16`

How to Maintain the Authorization Object for SAP Fiori APPs

> **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, consider the following three areas:

- *Authentification*
  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 TMW 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 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:

Authorization Group	Remarks
`CRMC`	all `CRM` - related customizing views as `CRM` - based scenarios can refer to the same tables; and ICC
`AISU`	all *S-USER* - related tables

Authorization Group	Remarks
BI* (Remodeling, Repartitioning, Warehouse)	all BI - related tables
CHRM	other than CRM - related tables for Change Request Management
SDCO	all other than CRM - related tables for Incident Management
LMDB	all LMDB and SMSY - related tables
SMAN	Implementation and Upgrade - related tables
BPCA	Business Process Change Analyzer - related tables
TSTM	Test Management - related tables
SISE	Solution Manager Basic Configuration (transaction SOLMAN_SETUP) - related tables
DFWK	Dashboard Framework - related tables
SMAL	Monitoring and Alerting (Technical Monitoring) – related tables
SGEN	ES-Reporting and SUGEN - related tables
SARC, BCTA	Data Volume Management
SRCD	Rapid Content Delivery
BCSV	CRM: Status Profile Maintenance
DNO	CRM: Basis Message
SS	RS: SAP Control
DSA	Solution Manager DSA
IVIS	Integration Visibility
SEA	Solution Manager: Scope and Effort Analyzer
SGEN	Solution Manager: SUGEN
SISE	Solution Manager: SOLMAN_SETUP
SMAL	Solution Manager: Monitoring and Alerting
SMAN	Solution Manager: Implementation
SMCM	Solution Manager: Customer Life-Cycle Management
SMSD	Solution Manager: Service Delivery

Authorization Group	Remarks
SMTA	Technical Administration
SMUA	Process Documentation: Administration Data
SMUD	Process Documentation: Instance Data
SMUG	Process Documentation: Authorization Groups
SMUL	Process Documentation: Library
SMUM	Process Documentation: Model Data
TSTM	Solution Manager: Test Management
SMGP	Solution Manager: Guided Procedure
SMRC	Solution Manager: Root Cause Analysis
SMTA	Solution Manager: Technical Administration
SMSD	Solution Manager: Service Delivery
SMDC	Solution Manager: Data Consistency Management (general)
SMDS	Solution Manager: Data Consistency Management (sensitive)
SMCB	Solution Manager: CBTA
SBPO	Solution Manager: Business Process Operations (Monitoring)
STAO	Solution Manager: TAO
USAG	Process Documentation: SMUD Usage

⚠ Caution

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.

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

Recommendation

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.

> ℹ Note
>
> In addition to authorization object `S_START` with SAP Basis 7.40, authorization object `S_USER_STA` is required by a user, if he/she want to add a new Web Dynpro Application in the menu of an authorization role.

Authorization Object S_SERVICE for OData - Services

OData Services have start authorization object `S_SERVICE`.

> ℹ Note
>
> External Services are also protected by authorization object `S_SERVICE`.

4.12.6 User Security: Authorization Object S_SECPOL(_A)

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

Parameter	Description	Default Value
CHECK_PASSWORD_BLACKLIST	Check the Password Blacklist	1
DISABLE_PASSWORD_LOGON	Disable Password Logon	0
DISABLE_TICKET_LOGON	Disable Ticket Logon	0
MAX_FAILED_PASSWORD_LOGON_ATTEMPTS	Maximum Number of Failed Attempts	5
MAX_PASSWORD_IDLE_INITIAL	Validity of Unused Initial Passwords	0
MAX_PASSWORD_IDLE_PRODUCTIVE	Validity of Unused Productive Passwords	0
MIN_PASSWORD_CHANGE_WAITTIME	Minimum Wait Time for Password Change	1
MIN_PASSWORD_DIFFERENCE	No. of Different Chars When Changing	1
MIN_PASSWORD_DIGITS	Minimum Number of Digits	0
MIN_PASSWORD_LENGTH	Minimum Password Length	6
MIN_PASSWORD_LETTERS	Minimum Number of Letters	0
MIN_PASSWORD_LOWERCASE	Minimum Number of Lowercase Letters	0
MIN_PASSWORD_SPECIALS	Minimum Number of Special Characters	0
MIN_PASSWORD_UPPERCASE	Minimum Number of Uppercase Letters	0
PASSWORD_CHANGE_FOR_SSO	Password Change Req. for SSO Logons	1
PASSWORD_CHANGE_INTERVAL	Interval for Regular Password Changes	0
PASSWORD_COMPLIANCE_TO_CURRENT_POLICY	Password Change After Rule Tightening	0

Parameter	Description	Default Value
PASSWORD_HISTORY_SIZE	Size of the Password History	5
PASSWORD_LOCK_EXPIRATION	Automatic Expiration of Password Lock	0

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: **`ZROLE_IMG_MYPROJECT`** and choose button *Single Role*.
   3. Enter a description for your role, for instance: `IMG` project: **`Implementation/Upgrade as of ST SP15`**.
   4. Save your role.

      > **Note**
      >
      > You are asked for a transport request.
3. **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.
   1. To receive all transactions which are contained in the customizing project, choose in the menu: *Utilities* > *Customizing auth.*
   2. In the appearing dialog box, choose button *Add* to attach your customizing project or customizing project view. In our case, we choose the customizing view that was created.
   3. In the various dialog boxes, choose your customizing project or customizing project view, in our case `myproject`.
      The system automatically assigns all relevant transactions and authorization objects for your customizing project or customizing project view.
   4. Confirm your project assignment.
4. **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.
   1. In the *Role Maintenance*, choose tab *Authorizations.*
   2. Choose button *Change*.
   3. Maintain all activity values per authorization object according to your needs, for instance if you want to grant full authorization, always choose all activities.

> ⚠ Caution
>
> All authorization objects need to receive a green traffic light. Beware, that the authorization trace does not trace values for critical authorization objects `S_RFC` and `S_TABU_DIS`.

4. Generate the profile.
5. To assign this profile to a user, choose tab *User*, add your user in the table and execute the user comparison.
6. Save.

Result

You have now created a role for your specific `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.

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: https://help.sap.com/viewer/disclaimer).

go.sap.com/registration/contact.html