

# Security Guide SAP Solution Manager 7.2

## Application-Specific Guides





# Content

<b>1</b>	<b>Security Guide</b>	<b>7</b>
<b>2</b>	<b>Documentation (Help Text IDs) for Users and Roles</b>	<b>9</b>
<b>3</b>	<b>Administration</b>	<b>10</b>
3.1	Document History	10
3.2	Scenario-Specific Guide: Solution Manager Administration	11
	Users and Authorizations	11
3.3	Scenario-Specific Guide: Technical Administration	14
	Prerequisites	14
	Users and Authorizations	17
	Integration	24
	Traces and Logs	25
<b>4</b>	<b>Root Cause Analysis</b>	<b>26</b>
<b>5</b>	<b>Process Management, and Test Suite</b>	<b>27</b>
5.1	Document History	27
5.2	Getting Started	29
5.3	Scenario-Specific Guide: Process Management	30
	Prerequisites	30
	Scenario Integration	35
	Users and Authorizations	36
	User Roles for Additional Functions	41
	External Integration	48
	Traces and Logs	49
5.4	Scenario-Specific Guide: Business Process Change Analyzer	49
	Prerequisites	50
	CRM Standard Customizing	55
	Scenario Integration	55
	Users and Authorizations	56
	Additional Security Measures	59
5.5	Scenario-Specific Guide: Test Management	60
	Prerequisites	60
	Scenario Integration	64
	Users and Authorizations	65
	Additional User Roles	69
	Partner Integration	77
	Additional Security Measures	80
5.6	Scenario-Specific Guide: Scope and Effort Analyzer (SEA)	80
	Getting Started	81
	Prerequisites	81
	User Descriptions and User Roles	85
	Authorization Objects	86

<b>6</b>	<b>Application Operations and Business Process Operation</b>	<b>87</b>
6.1	Document History	87
6.2	Scenario-Specific Guide: Technical Monitoring	90
	Prerequisites	90
	Scenario Integration	96
	User Descriptions	97
	Early Watch Alert Management Configuration	97
	User Roles for System, Database, Host Monitoring, and Self - Monitoring	98
	User Roles for Process Integration - Monitoring	101
	User Roles for Message Flow Monitoring	102
	User Roles for End-User Experience Monitoring	107
	User Roles for HANA and Business Intelligence Monitoring	110
	User Roles for Interface (Channel) Monitoring	112
	End-User Roles for Job Monitoring	114
	User Roles for Infrastructure Monitoring	116
	Users and Roles for Exception Management	118
	Integration Visibility in Managed Systems	119
	Role for Technical Monitoring Display	121
	Role for Technical Monitoring Support	121
	Main Authorization Objects	121
	Background Jobs	122
6.3	Scenario-Specific Guide: Business Process Operations	123
	Getting Started	123
	Prerequisites	123
	Scenario Integration	129
	Users and Authorizations	130
	User Roles for Additional Functions	136
6.4	Scenario-Specific Guide: Job Management	137
	Prerequisites	137
	Scenario Integration	142
	Users and Authorizations	142
	CRM Standard Customizing for Solution Manager	148
	External Integration	149
<b>7</b>	<b>Change Control and IT Service Management Scenarios</b>	<b>150</b>
7.1	Getting Started	150
7.2	Document History	150
7.3	Scenario-Specific Guide: Quality Gate Management	154
	Prerequisites	154
	CRM Standard Customizing for Solution Manager	158
	Scenario Integration	158
	Users and Authorizations	159
7.4	Scenario-Specific Guide: IT Service Management	163
	Prerequisites	163
	CRM Standard Customizing for Solution Manager	169
	Scenario Integration	170
	Users and Authorizations	171
	External Integration	175
	Integration of SAP Fiori Applications	176
7.5	Scenario-Specific Guide: Change Management	177

	Prerequisites	177
	CRM Standard Customizing for Solution Manager	183
	Scenario Integration	183
	Users and Authorizations	185
	System Recommendations	200
	Integration of SAP Fiori Applications	201
7.6	Scenario-Specific Guide: Configuration Validation	203
	Prerequisites	203
	Users and Authorizations	204
7.7	Additional Security Measures	205
<b>8</b>	<b>Custom Code, DVM, and Value Management Dashboard</b>	<b>207</b>
8.1	Document History	207
8.2	Scenario-Specific Guide: Custom - Code Life Cycle Management	208
	Getting Started	208
	Prerequisites	209
	Users and Authorizations	213
8.3	Scenario-Specific Guide: Data Volume Management	215
	Prerequisites	215
	Scenario Integration	219
	Users and Authorizations	220
8.4	Value Management Dashboard (iCI - Interactive Continuous Improvement)	222
	Getting Started	222
	Prerequisites	223
	Interactive Continuous Improvement (iCI) Dashboard	225
<b>9</b>	<b>Services</b>	<b>228</b>
9.1	Document History	228
9.2	Scenario-Specific Guide: SAP Engagement and Service Delivery	228
	Getting Started	228
	Prerequisites	229
	CRM Standard Customizing for Solution Manager	237
	Scenario Integration	238
	Recommended Users and Authorizations	238
	Security Optimization Service	242
9.3	Early Watch Alert Management and Service Level Reporting	242
9.4	Integration of SAP Fiori Applications	242
<b>A</b>	<b>Reference</b>	<b>244</b>
A.1	The Main SAP Documentation Types	244





# 1 Security Guide

## Caution

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

This guide refers to application specific roles and authorizations. For general information on the authorization concept of Solution Manager or setup security, refer to the according complimentary guides on the SAP Service Marketplace at: [service.sap.com/instguides](https://service.sap.com/instguides) » [SAP Components](#) » [SAP Solution Manager](#) » [<current release>](#) » (updated with every change per Support Package).

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

## To get started

**What is this guide about?** SAP Solution Manager covers a wide range of divers scenarios you can use. As a customer, you might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides per scenario which cover all relevant information for this specific scenario.

## Caution

Before you start using this scenario-specific guide, you must read the core information about security issues in SAP Solution Manager, and the *Landscape Setup Guide*, which refers to all security-relevant information during basic configuration of SAP Solution Manager. Without this information, we do not recommend to set up any specific scenario. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

This guide covers the following topics:

- **Getting Started:** find out about target groups of this guide. Links for any additional components you can find in the Core Guide.
- **Prerequisites:** find out about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other.
- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).
- **Scenario Integration:** according to the life-cycle approach the various scenarios integrate with each other. Here, you can find out about authorizations you need to assign to your users for these cases.

To enable your end-users to work with the application, you need to assign them authorizations in the Solution-Manager-system and in the managed systems.

When you are working in a project to implement new business processes or change existing ones, a number of project members with different tasks are involved. SAP delivers recommended user descriptions on which SAP delivered roles are modelled. These user descriptions and roles can only be regarded as templates for you. You need to first define which tasks the individual members in your company execute, and then adjust the according roles.

### Caution

The roles delivered by SAP can only be regarded as models for adjustment to your company's needs.



Roles for Technical Administration are predefined *Composite Roles* (technical abbreviation: \*\_COMP) for users. These composite roles contain a set of single roles that are relevant for the business tasks.

## Integration


Security topics are relevant for the following phases:

- Configuration
- Operations

### 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: [▶ service.sap.com/instguides](https://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: [service.sap.com/securityguides](https://service.sap.com/securityguides) .



## 2 Documentation (Help Text IDs) for Users and Roles

Within transaction `SOLMAN_SETUP` as well as application `SMUA` (Solution Manager User Administration) users and assigned roles are documented via a link in column *Documentation* within the User Interface screen of the application. When you choose this link, a dialog window appears with the relevant documentation text. The help text is integrated into the system by transaction `SE61`. In the following sections, only the Technical ID of the help text is given for all users and roles that are mentioned in transaction `SOLMAN_SETUP`. For all users and roles that are not integrated in transaction `SOLMAN_SETUP`, you can find the documentation in this guide.

For more information on any specific role or if you want to adapt the original to your own purpose, call transaction `SE61` and proceed as described:

1. Call transaction `SE61`.
2. Choose *Document Class* **General text** (TX).
3. Choose your language.
4. Enter the technical ID of the help text as given in the tables in this guide.
5. Choose button *Display*. The system displays the text, which is also linked in the setup screen.

### **i** Note

- All documents for authorization roles description have the naming convention `AUTH_*`
- All documents for user descriptions have naming conventions either `TP*` or `USER_*`.

# 3 Administration

The **Administration** applications in SAP Solution Manager are the following:

- *SAP Solution Manager Administration*
  - Service Connection
  - Landscape and Infrastructure Management (including CCDB, RFC, and other administration tool access)
  - Self Diagnosis and Self Monitoring
  - Users
- *Technical Administration*
  - IT Task Management and Guided Procedures
  - Service Availability Management
  - IT Calendar
  - Notification Management (including Instant Notification)
  - Work Mode Management

## 3.1 Document History

Here, all changes to the specific scenario guide are listed according to Support Package.

Table 1

Support Package Stacks (Version)	Description
SP01	<p><b>General</b></p> <ul style="list-style-type: none"> <li>• First version</li> </ul> <p><b>Adaptations to Previous Release 7.1 (Due to new Process Documentation functionality)</b></p> <ul style="list-style-type: none"> <li>• Removed role SAP_SMWORK_BASIC* (obsolete)</li> <li>• Substituted roles SAP_SOL_PROJ_ADMIN_* and SAP_SM_SOLUTION_* with SAP_SM_SL_*</li> </ul> <p><b>SAP Fiori Integration</b></p> <ul style="list-style-type: none"> <li>• All users receive Embedded SAP Fiori related authorizations with role SAP_SM_FIORI_LP_EMBEDDED</li> </ul> <p><b>Work Management Mode and EEM Robots</b></p> <ul style="list-style-type: none"> <li>• SAP_SM_DTM_* substituted by SAP_SM_WMM_* in composite role for <i>Service Availability Management</i> and <i>Technical Monitoring</i></li> <li>• new roles for EEM Robots: SAP_SM_EEM_ROBOT_* (substitute DTM roles only for EEM robot part)</li> </ul>
SP03	<p><b>Technical Administration</b></p> <ul style="list-style-type: none"> <li>• adapted role SAP_ITCALENDER</li> </ul>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>adapted role SAP_NOTIF_ADMIN (containing <i>Instant Notification</i>)</li> </ul> <p><b>Redesign of Service Availability Management</b></p> <ul style="list-style-type: none"> <li>substituted authorization objects SM_SAM_MSO and SM_SAM_AST (set inactive) with new authorization objects SM_SAM_DEF, SM_SAM_OUT, SM_SAM_REP in roles SAP_SM_SAM*</li> </ul>

## 3.2 Scenario-Specific Guide: Solution Manager Administration

### 3.2.1 Users and Authorizations

#### ➔ Recommendation

We recommend to add the roles for Solution Manager Administration to the user SOLMAN\_ADMIN, or generate a similar user with roles as mentioned underneath.

The SAP Solution Manager Administration work center is used to manage the SAP Solution Manager system. Therefore, it is primarily used by System Administrators.

The user roles delivered in the composite roles underneath contain all necessary single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the end-user. You can use the delivered composite roles to assign to your users. In case you want to restrict the access and/or the authorizations for a particular user, use the authorization objects SM\_WD\_COMP and SM\_WC\_VIEW.

The table underneath gives you an overview, which single roles are included in the composite roles. An additional column indicates, for which section of the navigation panel the according single role is absolutely necessary. As the [Overview](#) in a work center always contains all links to the relevant sections in the navigation panel, it is not mentioned.

#### i Note

The related links area contains links to other work centers. If you want to allow access to these work centers, you need to check the according scenario - specific section for the relevant scenario.

#### Administrator (Technical Role Name: SAP\_SOLMAN\_ADMIN\_COMP)

Table 2

Single role	Restriction to
SAP_SM_SL_ADMIN	Full access to Project Documentation
SAP_RCA_AGT	Agent Administration authorization

Single role	Restriction to
SAP_RCA_DISP	Display of Root Cause Analysis authorization
SAP_SERVICE_CONNECT	Service Connect authorizations
SAP_SMWORK_SM_ADMIN	Allows access to the Change Management work center.
SAP_SM_SYM_CONF	Configuration authorization for System Database Host Monitoring
SAP_SYSTEM_REPOSITORY_ALL	Full authorization for LMDB  <b>i Note</b> Authorizations for infrastructure are needed in all sections, as this role includes authorizations on systems.
SAP_SM_CMDB_EXE	CMDB Access  <b>i Note</b> Authorizations for notifications are included in roles: SAP_NOTIF_ADMIN
SAP_SM_SMUA_ALL	Access SMUA application
SAP_SM_DASHBOARDS_DISP_LMDB	Access LMDB Dashboard
SAP_SM_BP_ADMIN	Maintain Business Partners
SAP_SM_ROLECMP_ALL	Access to Role Comparison Tool
SAP_SM_FIORI_LP_EMBEDDED	Access to embedded Fiori Launchpad
SAP_SM_RFC_ADMIN	Maintain RFC Connections
SAP_SM_USER_ADMIN	Maintain Users and Roles

### Display User (Technical Role Name: SAP\_SOLMAN\_ADMIN\_DISP\_COMP)

Table 3

Single role	Restriction to
SAP_SM_SL_DISPLAY	Display for Infrastructure
SAP_RCA_DISP	Display to Root Cause Analysis
SAP_SERVICE_CONNECT	Service Connect authorizations  <b>i Note</b> Authorizations for notifications are included in roles: SAP_NOTIF_ADMIN_DISP

Single role	Restriction to
SAP_SMWORK_SM_ADMIN	Allows access to the Change Management work center.
SAP_SM_SYM_LEVEL01	Level one authorization for System, Database Host Monitoring
SAP_SYSTEM_REPOSITORY_DIS	Display authorization for LMDB  <b>i Note</b> Authorizations for infrastructure are needed in all sections, as this role includes authorizations on systems.
SAP_SM_DASHBOARDS_DISP_LMDB	Display LMDB Dashboard
SAP_SM_ROLECMP_DISPLAY	Display Role Comparison Tool
SAP_SM_SMUA_DIS	Display SMUA
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori embedded launchpad
SAP_SM_BP_DISPLAY	Display for RFC Connections
SAP_SM_RFC_DISP	Display for RFC - Connections

## Authorizations for Specific Tools

### Solution Manager User Administration (SMUA)

This tool provides you with the possibility to manage all users that are created in transaction `SOLMAN_SETUP` at once. For more information, see Online Documentation.

The roles `SAP_SM_SMUA_*` are used to access the SMUA tool in view *Users*. Authorization object `SM_SMUA` is contained in this role.

#### **i Note**

The user interface of *SMUA* allows you to display in one table/screen users, roles and RFC-destinations. The system displays the RFC Connection only, if authorization for transaction `SM59` is assigned. The according authorizations are contained in roles `SAP_SM_RFC_*`.

### Segregation of Duty

You can assign the authorization for *SMUA* to a dedicated user who is only allowed to user this application. In this case, you need to additionally assign the following roles to this user:

- `SAP_SMWORK_SM_ADMIN` (Navigation)
- `SAP_SM_USER_ADMIN` (Users and Roles)
- `SAP_SYSTEM_REPOSITORY_ALL` (LMDB Access)

### Archive Log

The role `SAP_SM_ARCHIVE_LOG_ALL` for *Archive Log* contains authorization object `SM_SETUP` with `ACTVT 24` (Archive).

## ➔ Recommendation

We recommend to limit scenario visibility for which the *Archive Log* should be accessible in authorization object SM\_SETUP.

You can assign the authorization for *Archive Log* to a dedicated user. In this case, you need to additionally assign the following roles to your user:

- SAP\_SMWORK\_SM\_ADMIN
- SAP\_SYSTEM\_REPOSITORY\_ALL
- SAP\_SM\_SMUA\_DIS

## Role Comparison Tool: Role Adjust

The role SAP\_SM\_ROLECMP\_\* allows the user to adjust already customized roles with newly shipped values, or value changes, from SAP Standard roles. Access to the application is restricted by authorization object SM\_ROLECMP.

You can assign the authorization for the role comparison tool to a dedicated user. In this case, you need to additionally assign the following roles to your user:

- SAP\_SMWORK\_SM\_ADMIN
- SAP\_SM\_USER\_ADMIN
- SAP\_SM\_SMUA\_DIS
- Authorization object SM\_SETUP with ACTVT 02 (Change) for *User Creation* steps.

## i Note

To remove the *Update* flag in the *Update* column after you have used the *Adjust Role* tool, make sure you choose the button *Refresh* on top of the Users screen.

## 3.3 Scenario-Specific Guide: Technical Administration

### 3.3.1 Prerequisites

#### 3.3.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete Technical Administration scenario. The SAP Solution Manager is connected via *READ - RFC*, and *TRUSTED - RFC* to your managed systems. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

Technical Infrastructure  
 • Technical Administration

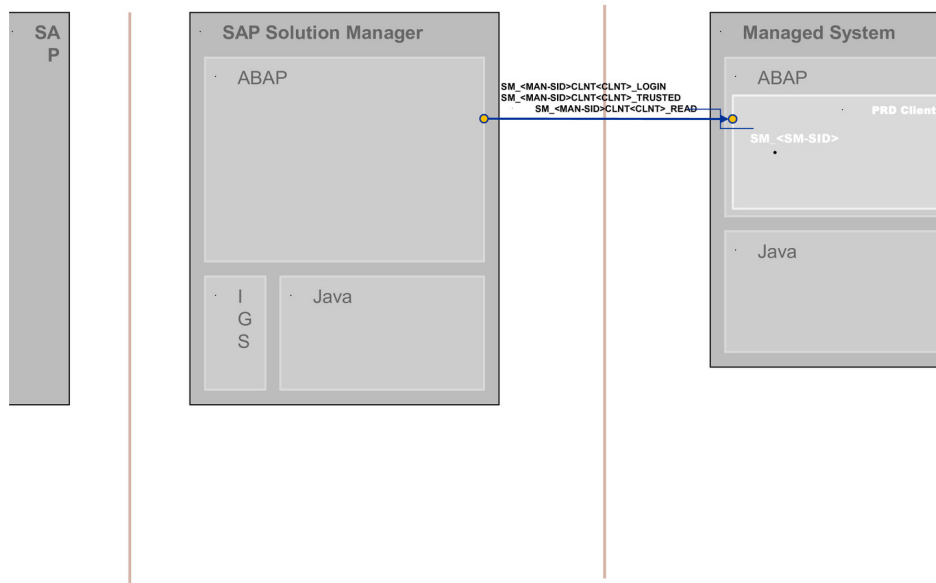


Figure 1: Infrastructure

### 3.3.1.2 Configuration

Technical Administration is subdivided into several *functions*, for instance *Service Availability Management* or *IT Task Inbox*. The configuration users and their authorizations are described in the individual section.

**i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see *Secure Configuration Guide*.

### 3.3.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

#### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels



Table 4

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems	RFC	Reading information from managed systems
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes
Solution Manager to Exchange Server	LDAP	Reading distribution lists
Solution Manager to Mail Server/SMS Sever	HTTP (S) / RFC , SMTP,	For E-mail and SMS

## Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: Managed Systems), see *Secure Configuration Guide*.

Table 5

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	For Notification Management to fetch users and Business Partners

## 3.3.1.4 Technical User

The technical user in the following table is needed for this scenario. It is created automatically during configuration. For more information on individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

## User for READ - access in Managed Systems

Table 6

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>

## 3.3.2 Users and Authorizations

### 3.3.2.1 Technical Administration Users

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for Technical Administration. All users are assigned a composite role, which contains a number of single roles.

#### **i** Note

The composite roles for Technical Administration contain all relevant single roles for all sub-scenarios. As users for Technical Administration are not created within transaction `SOLMAN_SETUP`, you need to maintain them and the according user roles in the classic transactions `SU01` (User Maintenance) and `PFCG` (Role Maintenance).

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization objects `SM_WC_VIEW` and `SM_WD_COMP`.

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

#### Administrator (Technical Role Name: `SAP_TECHNICAL_ADMIN_COMP`)

Table 7

Single Role	Restriction on
<code>SAP_SM_WMM_ALL</code>	Full authorization for <i>Work Mode Management</i>
<code>SAP_SM_EEM_ROBOT_ALL</code>	EEM Robot
<code>SAP_SM_ADMIN_COMPONENT_ALL</code>	MDM <i>Administration Cockpit</i>
<code>SAP_NOTIF_ADMIN</code>	Full authorization for <i>Notification Management</i>
<code>SAP_ITCALENDAR</code>	Full authorization for <i>IT Calendar</i>
<code>SAP_TASK_INBOX_ALL</code>	Full authorization for Task Inbox
<code>SAP_SM_IT_EVENTS_ADMIN</code>	Full authorization for <i>IT Events</i> (launched from IT Calendar)
<code>SAP_SYSTEM_REPOSITORY_ALL</code>	Full authorization for <i>System Repository</i> (LMDB)

Single Role	Restriction on
SAP_SMWORK_SYS_ADMIN	Access to <i>Work Center for Technical Administration</i>
SAP_SM_GP_ADMIN	Run <i>Guided Procedure</i>
SAP_SM_SAM_ALL	Full authorization for SAM integration
SAP_SM_BP_DISPLAY	Allows <i>Business Partner</i> display in IT Task Inbox
SAP_TASK_PLANNING_ALL	Full authorization for <i>Task Planner</i>
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori embedded Launchpad

## Display User (technical role name: SAP\_TECHNICAL\_ADMIN\_DISP\_COMP)

Table 8

Single Role	Remarks
SAP_SM_WMM_DIS	Display authorization for <i>Work Mode Management</i>
SAP_SM_EEM_ROBOT_DIS	Display authorization for <i>Work Mode Management</i>
SAP_SM_ADMIN_COMPONENT_DIS	MDM <i>Administration Cockpit</i>
SAP_NOTIF_DIS	Display authorization for <i>Notification Management</i>
SAP_ITCALENDAR	Authorization for <i>IT Calendar</i>
SAP_SM_IT_EVENTS_DISP	Display authorization for <i>IT Event</i> (launched from IT Calendar)
SAP_TASK_INBOX_DIS	Display authorization for <i>Task Inbox</i>
SAP_SYSTEM_REPOSITORY_DISP	Display authorization for <i>System Repository</i> (LMDB)
SAP_SMWORK_SYS_ADMIN	Access to <i>Work Center for Technical Administration</i>
SAP_SM_GP_DIS	Display <i>Guided Procedure</i>
SAP_SM_SAM_DIS	Display authorization for SAM integration
SAP_SM_BP_DISPLAY	Allows <i>Business Partner</i> display in IT Task Inbox
SAP_TASK_PLANNING_DIS	Display authorization for <i>Task Planner</i>
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori embedded Launchpad

## Notification Management

The role for *Notification Management* SAP\_NOTIF\_ADMIN contains:

- *Global Recipient Notification*
- *Central Notification Management (CNM) - Instant Notification* (as a feature of Gateway services) - enhanced version of *Global Recipient Notification*

## Guided Procedures

This role contains the critical authorization objects `S_SYS_RWBO` with `ACTVT 01, 02, 03` and `S_TRANSPRT` with `ACTVT 01, 02, 03, 07` for Workbench Requests. If you do not want to allow the user to create, change, or display transports, then you need to deactivate these objects in the role `SAP_SM_GP_ADMIN`.

### 3.3.2.2 IT Task Inbox and Guided Procedure

*IT Task Planning* allows you to plan *Guided Procedures*. The new *IT Task Inbox* displays all available tasks which are assigned to a user, to a support organization, or which are planned for certain managed objects. When a user executes a task, the system opens a related Guided Procedure and the task is executed via the steps and activities of the Guided Procedure.

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment.

#### Scenario Configuration

You can configure the *IT Task Management* scenario using transaction `SOLMAN_SETUP`. Template users can be created in the `SOLMAN_SETUP` configuration procedure for this scenario.

The configuration user `SMC_ITTM_<SID>` (Help Text ID: `USER_CONFIG_ITTM`) receives the single roles in transaction `SOLMAN_SETUP` as displayed underneath in the table. The technical role name of the corresponding composite role is: `SAP_ITTM_CONF_COMP`.

Table 9

Single Role	Help Text ID
<code>SAP_SYSTEM_REPOSITORY_ALL</code>	<code>AUTH_SAP_SYSTEM_REP_ALL</code>
<code>SAP_SMWORK_CONFIG</code>	<code>AUTH_SAP_SMWORK_CONFIG</code>
<code>SAP_ITTM_CONF</code>	<code>AUTH_SAP_ITTM_CONF</code>
<code>SAP_SETUP_SYSTEM_PREP</code>	<code>AUTH_SAP_SETUP_SYSTEM_PREP</code>
<code>SAP_SM_ROLECMP_ALL</code>	<code>AUTH_SAP_SM_ROLECMP_ALL</code>
<code>SAP_SM_BP_ADMIN</code>	<code>AUTH_SAP_SM_BP_ADMIN</code>
<code>SAP_SM_USER_ADMIN</code>	<code>AUTH_SAP_SM_USER_ADMIN</code>
<code>SAP_SM_SYM_TRANSPORT</code>	<code>AUTH_SAP_SM_SYM_TRANSPORT</code>

**i Note**

Due to the requirement of copying transaction type `SMOT` into customer name space, a transport request is required for transporting customizing changes. In addition to authorization object `S_TRANSPRT` with authorization for customizing requests, this requires authorization object `S_DATASET` with `ACTVT 34` (write) on file level.

## Work Center Access

Guided Procedure is accessible using the *Work Center for Technical Administration*.

## RFC-Connections

RFc-connections are only used in the case of automated activities that can be used in the self-defined guided procedures. These automated activities always use trusted RFC-connections.

## CRM Authorizations Integration

*IT Task Inbox* requires CRM - integration. Therefore, the transaction type SMOT is used.

### ➔ Recommendation

To avoid loss of data when upgrading your system, always copy transaction types and related objects into your own name space. This requires, that you need to adapt the CRM - specific authorization objects accordingly. For more information on CRM - integration, see the according section in the *Authorization Concept for Solution Manager Guide*.

## Administration User (Technical Name: TP\_ITTM\_ADM)

The technical role name of the corresponding composite role is: SAP\_TASK\_MANAGEMENT\_ALL\_COMP.

Table 10

Single Role	Help Text ID
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_GP_ADMIN	AUTH_SAP_SM_GP_ADMIN
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SM_IT_EVENTS_DISP	AUTH_SAP_SM_IT_EVENTS_DISP
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_TASK_PLANNING_ALL	AUTH_SAP_TASK_PLANNING_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## Authoring User (Technical Name: TP\_ITTM\_AUTH)

The technical role name of the corresponding composite role is: SAP\_GUIDED\_PROCEDURE\_ALL\_COMP.

Table 11

Single Role	Help Text ID
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN

Single Role	Help Text ID
SAP_SM_GP_ADMIN	AUTH_SAP_SM_GP_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBEDDED

### IT Manager (Technical Name: TP\_ITTM\_ITM)

The technical role name of the corresponding composite role is: SAP\_TASK\_PLANNING\_ALL\_COMP.

Table 12

Single Role	Help Text ID
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_TASK_PLANNING_ALL	AUTH_SAP_TASK_PLANNING_ALL
SAP_ITCALENDER_DISP	AUTH_SAP_ITCALENDER_DISP
SAP_TASK_INBOX_DISP	AUTH_SAP_TASK_INBOX_DISP
SAP_SYSTEM_REPOSITORY_DISP	AUTH_SAP_SYSTEM_REP_DISP
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_GP_DISP	AUTH_SAP_SM_GP_DISP
SAP_SM_IT_EVENTS_DISP	AUTH_SAP_SM_IT_EVENTS_DISP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### IT Operator (Technical Name: TP\_ITTM\_ITO)

The technical role name of the corresponding composite role is: SAP\_TASK\_INBOX\_ALL\_COMP.

#### Authorization Roles in the Solution Manager - System

Table 13

Single Role	Help Text ID
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_TASK_INBOX_DISP	AUTH_SAP_TASK_INBOX_DISP
SAP_SYSTEM_REPOSITORY_DISP	AUTH_SAP_SYSTEM_REP_DISP
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_GP_EXE	AUTH_SAP_SM_GP_EXE
SAP_TASK_PLANNING_DISP	AUTH_SAP_TASK_PLANNING_DISP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Display User (Technical Name: TP\_ITTM\_DISP)

The technical role name of the corresponding composite role is: SAP\_TASK\_MANAGEMENT\_DISP\_COMP.

Table 14

Single Role	Help Text ID
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_TASK_PLANNING_DIS	AUTH_SAP_TASK_PLANNING_DIS
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_TASK_INBOX_DIS	AUTH_SAP_TASK_INBOX_DIS
SAP_SYSTEM_REPOSITORY_DISP	AUTH_SAP_SYSTEM_REP_DISP
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_GP_DIS	AUTH_SAP_SM_GP_DIS
SAP_SM_IT_EVENTS_DISP	AUTH_SAP_SM_IT_EVENTS_DISP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### 3.3.2.3 Service Availability Management

*Service Availability Management* (SAM) enables downtime reporting for technical components like servers, technical systems, and other objects. These downtime entries are called “Service Outages” and can be checked and corrected by System Administrators. The final confirmation is done by an IT Manager. These confirmed Service Outages are mapped to “Agreed Service Times” (AST) and reported using Dashboards.

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for SAM. All users are assigned a composite role, which contains a number of single roles.

#### Configuration

The configuration of SAM is executed using transaction SOLMAN\_SETUP. Here, you can also create template users for your application users. The configuration user SMC\_TSAM\_<SID> (Help Text ID: USER\_CONFIG\_TSAM) is assigned the following roles by the system:

#### Single Roles for Configuration User (Technical Role Name: SAP\_SAM\_CONF\_COMP) in the SAP Solution Manager System

Table 15

Role	Help Text-ID
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SMWORK_CONF	AUTH_SAP_SMWORK_CONF
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY



Role	Help Text-ID
SAP_TSAM_CONF	AUTH_SAP_TSAM_CONF
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN

### **i** Note

For conceptual information on *Configuration Users* in SAP Solution Manager, see *Secure Configuration Guide*.

## Work Center Access

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW.

## Administrator (Help Text-ID: TP\_SAM\_ADMIN)

### Single Roles for Administrator (Technical Role Name: SAP\_SAM\_ADMIN\_COMP) in the SAP Solution Manager System

Table 16

Role	Help Text-ID
SAP_SM_SAM_ALL	AUTH_SAP_SM_SAM_ALL
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_WMM_ALL	AUTH_SAP_SM_DTM_ALL
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## Display User (Help Text-ID: TP\_SAM\_DISP)

### Single Roles for Display User (Technical Role Name: SAP\_SAM\_DISPLAY\_COMP) in the SAP Solution Manager System

Table 17

Role	Help Text-ID
SAP_SM_SAM_DIS	AUTH_SAP_SM_SAM_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_WMM_DIS	AUTH_SAP_SM_DTM_DIS
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## Maintenance User (Help Text-ID: TP\_SAM\_AM)

### Single Roles for Maintenance User (Technical Role Name: SAP\_SAM\_EDIT\_COMP) in the SAP Solution Manager System

Table 18

Role	Help Text-ID
SAP_SM_SAM_EDIT	AUTH_SAP_SM_SAM_EDIT
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_WMM_ALL	AUTH_SAP_SM_DTM_ALL
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## Review User (Help Text-ID: TP\_SAM\_CNFM)

### Single Roles for Review User (Technical Role Name: SAP\_SAM\_REVIEW\_COMP) in the SAP Solution Manager System

Table 19

Role	Help Text-ID
SAP_SM_SAM_REVIEW	AUTH_SAP_SM_SAM_REVIEW
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_DTM_DIS	AUTH_SAP_SM_DTM_DIS
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## 3.3.3 Integration

Technical Administration refers to the maintenance of all systems in your system landscape. To run all your systems smoothly, this phase needs to integrate with handling of problems. The following sections describe the integration of technical administration with other scenarios within SAP Solution Manager, and which user roles would be applicable.

### **i** Note

For more detail on each individual scenario, see the according *Scenario—Specific Guide*.

### Work Mode Management

Work mode Application is a planning tool and is used to define the Work Mode of a system. Work Mode can be:

- Planned Downtime

- 
- Maintenance
  - Peak Business Hour
  - Non-Peak Business Hour
  - Non-Business Hour

The Work Mode can be displayed in the following applications:

- IT Calendar
- Monitoring and Alerting
- Reporting (Alert Inbox, PI- Reporting, BP Reporting)
- Monitoring (PI Monitoring and Interface Monitoring)

#### **Authorization Object SM\_WMM\_AUT**

The object restricts activities for Work Mode Management and is contained in role `SAP_SM_WMM_*`, which substitutes role `SAP_SM_DTM_*` (from Release 7.1).

### **3.3.4 Traces and Logs**

Work Mode Management provides the feature to notify users about a system downtime. E-mail addresses can be displayed by the system administrator. Changes are logged.

---

## 4 Root Cause Analysis

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for Root Cause Analysis.

### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WD_COMP`. For more information about user interface authorizations, see *Authorization Concept Security Guide*.

The tables underneath give you a further overview. During automated setup, the user `SAPSUPPORT` automatically receives all relevant roles, see section on `SAPSUPPORT` user. Since the [Overview](#) in a work center always contains all links to the relevant sections in the navigation panel, it is not mentioned.

# 5 Process Management, and Test Suite

## 5.1 Document History

Here, all changes to the specific scenario guide are listed according to Support Package.

Table 20

Support Package Stacks (Version)	Description
SP01	<p><b>General</b></p> <ul style="list-style-type: none"> <li>• First version</li> </ul> <p><b>General Adaptations to Previous Release 7.1 (Due to new Process Documentation functionality)</b></p> <ul style="list-style-type: none"> <li>• Removed roles SAP_SMWORK_BASIC* and SAP_SM_BI_BILO (obsolete)</li> <li>• Substituted roles SAP_SOL_PROJ_ADMIN_*, SAP_SOLAR_* and SAP_SM_SOLUTION_* with SAP_SM_SL_*</li> <li>• Substituted roles SAP_SOL_KW_* with SAP_SM_KW_*</li> </ul> <p><b>Obsolete Authorization Objects</b></p> <ul style="list-style-type: none"> <li>• SM_UA_PRJ</li> <li>• D_SOL_VSBL</li> <li>• D_SOLM_ACT</li> <li>• D_SOL_VIEW</li> <li>• S_PROJECT</li> <li>• S_PROJECTS</li> <li>• S_PROJ_GEN</li> </ul> <p><b>Additional Security Measures in BPCA</b></p> <ul style="list-style-type: none"> <li>• Authorization group BPCA added to all relevant tables and authorization group S_TABU_DIS.</li> <li>• Authorization object S_RFC confined in all relevant roles</li> <li>• Added roles for Business Partners and Test Management Information System</li> </ul> <p><b>Test Management</b></p> <ul style="list-style-type: none"> <li>• New composite roles SAP_TEST_*_COMP</li> <li>• substituted role SAP_SM_SL_EDIT with role SAP_SM_SL_DISPLAY in all composite roles</li> <li>• substituted role SAP_SM_KW_DIS with role SAP_SM_KW_ALL in all composite roles but display role</li> <li>• added SAP_SUPPDESK_CREATE to all composite roles</li> <li>• Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_TEST_MAN has been transferred into roles: SAP_STWB_*, and SAP_STCE_*.</li> </ul>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>To call the old work center, use transaction <code>STWB_OLD</code>. You can restrict the views for both work centers within the authorization field help for authorization object <code>SM_WC_VIEW</code>.</li> </ul> <p><b>SEA</b></p> <ul style="list-style-type: none"> <li>removed Maintenance Optimizer roles</li> </ul> <p><b>Process Documentation</b></p> <ul style="list-style-type: none"> <li>Roadmap authoring environment is obsolete, therefore according roles <code>SAP_RMDEF_RMAUTH_*</code> are obsolete and removed from delivery</li> </ul> <p><b>Project Management (ITPPM)</b></p> <ul style="list-style-type: none"> <li>New template users and configuration user for</li> <li>Specific end - user authorization roles for <code>ITPPM: SAP_SM_ITPPM_*</code></li> <li>Specific configuration role: <code>SAP_ITPPM_CONFIG</code></li> </ul> <p><b>SAP Fiori Integration</b></p> <ul style="list-style-type: none"> <li>All users receive authorization for SAP Fiori embedded launchpad, role: <code>SAP_SM_FIORI_LP_EMBEDDED</code></li> </ul>
SP02	<p><b>BPCA</b></p> <p>All changes within roles are documented in the <i>Menu</i> tab of the respective role:</p> <ul style="list-style-type: none"> <li>adapted single role <code>SAP_BPCA_CONFIG</code></li> </ul> <p><b>Process Management</b></p> <p>All changes within roles are documented in the <i>Menu</i> tab of the respective role:</p> <ul style="list-style-type: none"> <li>adapted single roles <code>SAP_SM_SL_*</code> (additional transaction codes <code>SOLDOC</code> and <code>SOLADM</code>)</li> </ul> <p><b>Test Management</b></p> <p>All changes within roles are documented in the <i>Menu</i> tab of the respective role:</p> <ul style="list-style-type: none"> <li>adapted role <code>SAP_WDA_TST_RFC</code></li> </ul> <p><b>CBTA</b></p> <p>All changes within roles are documented in the <i>Menu</i> tab of the respective role:</p> <ul style="list-style-type: none"> <li>adapted role <code>SAP_CBTA_DIS_COMP</code></li> <li>adapted role <code>SAP_TST_AGENT_RFC</code></li> </ul>
SP03	<p><b>Business Process Graphical Modelling within Process Management</b></p> <ul style="list-style-type: none"> <li>Adapted roles <code>SAP_SM_SL_ADMIN</code> and <code>SAP_SM_SL_DISPLAY</code> with specific BPMN authorization</li> <li>New additional role for Process Management specifically for BPMN maintenance: <code>SAP_SM_SL_EDIT_BPMN</code></li> </ul> <p><b>Process Management</b></p> <p>All changes within roles are documented in the <i>Menu</i> tab of the respective role:</p> <ul style="list-style-type: none"> <li>Adapted single role <code>SAP_SM_SL_ADMIN</code> (additional authorization field value in object <code>SM_SDOCADM - Site</code>)</li> <li>Adapted single roles <code>SAP_SM_SL_ADMIN</code> and <code>SAP_SM_SL_EDIT</code> for <i>Custom Interface Maintenance</i></li> </ul>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>Added single role <code>SAP_SM_DSH_DISP</code> to all standard users (Dashboard)</li> </ul> <p><b>Project Management</b></p> <ul style="list-style-type: none"> <li>Extended section on ITPPM in regards of E2E process integration with <i>Issue Management</i>.</li> <li>Added single role <code>SAP_SM_DSH_DISP</code> to all standard users (Dashboard)</li> <li>Added single role <code>SAP_SMWORK_IMPL</code> to Administrator user</li> </ul> <p><b>Solution Documentation Assistant</b></p> <ul style="list-style-type: none"> <li>section removed</li> </ul> <p><b>Test Management</b></p> <p>All changes within roles are documented in the <i>Menu</i> tab of the respective role:</p> <ul style="list-style-type: none"> <li>According to redesigned BW reports, new BW related role: <code>SAP_BI_E2E_SMT</code></li> <li>new roles for <i>Partner Test Management</i>, see according section</li> <li>removed sections for Partner Test Management products for QC by HP and IBM Rational</li> </ul> <p><b>Business Process Change Analyzer</b></p> <p>All changes within roles are documented in the <i>Menu</i> tab of the respective role:</p> <ul style="list-style-type: none"> <li>added <code>SAP_STWB_WORK_DIS</code> to the display user</li> <li>substituted role <code>SAP_SM_SL_DISPLAY</code> with <code>SAP_SM_SL_EDIT</code> in composite role <code>SAP_BPCA_ECATT_COMP</code></li> <li>new role <code>SAP_SM_BPCA_PTM_INT</code> to integrate Partner Test Management and BPCA for configuration users. They share some steps in their configuration which are optional on both sides. Therefore, this role contains the delta information for these steps.</li> </ul>

## 5.2 Getting Started

**What is this guide about?** SAP Solution Manager covers a wide range of diverse scenarios you can use. As a customer, you might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides per scenario which cover all relevant information for this specific scenario.

The application - specific guide contains the following functions:

- Process/Solution Documentation
  - Process Management
  - Project Management
  - CDMC
  - Customizing Comparison and Distribution
- Business Process Change Analyzer
- Test Suite
  - Test Workbench Workflow



- CBTA
- Test Case Maintenance
- TBOM Maintenance
- Test Plan Maintenance
- Partner Test Management
- Scope and Effort Analyzer
- Business Requirements (see scenario-specific guide for Change Management)

### Caution

Before you start using this scenario-specific section, you must read the information about security issues in SAP Solution Manager, and the *Secure Configuration Guide*, which refers to all security-relevant information during basic configuration of SAP Solution Manager. Without this information, we do not recommend to set up any specific scenario. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

This guide covers the following topics:

- **Getting Started:** find out about target groups of this guide. Links for any additional components you can find in the Core Guide.
- **Prerequisites:** find out about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other.
- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).
- **Scenario Integration:** according to the life-cycle approach the various scenarios integrate with each other. Here, you can find out about authorizations you need to assign to your users for these cases.
- **Background Jobs:** lists all related background jobs

## 5.3 Scenario-Specific Guide: Process Management

### 5.3.1 Prerequisites

#### 5.3.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete implementation and upgrade scenario. The SAP Solution Manager is connected via `READ - RFC`, `TRUSTED - RFC`, `TMW - RFC` to your managed systems, and your managed systems are connected to the SAP Solution Manager via `BACK - RFC`. `TREX` is connected to the `ABAP` stack, as well as `IGS` via specified `RFC` connections. Optionally, you can attach a third party product such as SAP Productivity Pak to the SAP Solution Manager via specified destinations. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

Technical Infrastructure  
 • Implementation and Upgrade

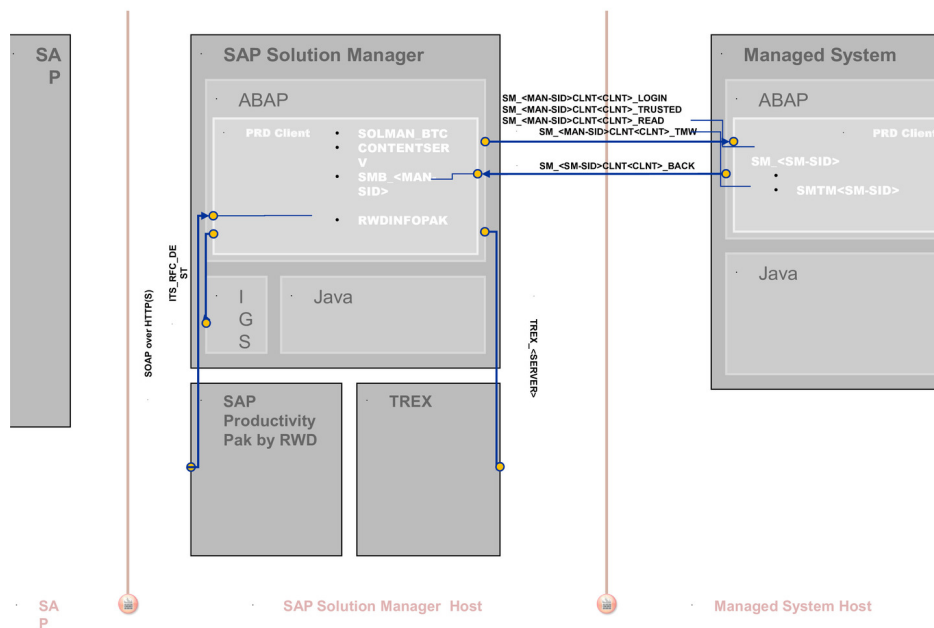


Figure 2: Implementation and Upgrade

### 5.3.1.2 Configuration User

#### Basic Configuration SOLMAN\_SETUP

You can productively use *Process Documentation* after you have executed:

1. Migration of Solutions/ Projects from SAP Solution Manager Release 7.1 to Release 7.2. For more information on the Solution Content Activation Procedure, see according section in the *Secure Configuration Guide*.
2. Configuration procedure for *Process Management* in transaction SOLMAN\_SETUP.

#### Configuration User SMC\_SOLD\_XXX

Composite role (Technical Role Name: SAP\_SOL\_CONFIG\_COMP)

Table 21

Single Role	Help Text
SAP_ESH_CR_ADMIN	<p>No Help Text ID; The roles are required to configure TREX</p> <p><b>i Note</b>  <i>Embedded Search</i> is a main functionality for document search which is also used in other scenarios.</p>
SAP_ESH_TRANSPORT	
SAP_BC_SES_ADMIN	
SAP_SM_ESH_ADMIN	
SAP_SL_CONFIG	AUTH_SAP_SL_CONFIG
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN

Single Role	Help Text
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SMWORK_IMPL	AUTH_SAP_SMWORK_IMPL
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_TREX_ADMIN	AUTH_SAP_SM_TREX_ADMIN

### Authorization Groups for Tables (S\_TABU\_DIS)

The following authorization groups are relevant:

- SMUA: Administrative Data
- SMUD: Instance Data
- SMUG: Authorizations
- SMUL: Library Generation
- SMUM: Model Data
- SLAN: Solution Administration
- USAG: Usage

## 5.3.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 22

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to managed systems and back	RFC	Reading information from managed systems
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes
SAP Productivity Pak by RWD	SOAP over HTTP (S)	External Integration: Document Management

## Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 23

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System		Customer-specific	Customer-specific	
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	To read data of assigned objects; read BC Set activation log;
SM_<SID>CLNT<Client>_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific	Necessary for CDMC, Customizing Synchronization; BC Set content activation;
SM_<SID>CLNT<Client>_TMW (ABAP connection)	Managed System	System-specific	System-specific	Default user: SMTW<SID> of	Used only for the integration of Custom Development Management

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
				Solution Manager system>	Cockpit connection to productive systems (CDMC), see section on Additional Functions

### RFC Connection from Managed System to SAP Solution Manager

Table 24

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	SMB_<managed system ID>	For Help Center Function	Automatically created via transaction SOLMAN_SETUP (view: managed systems)
HELP_CENTER_TO_SOLMAN	Solution Manager System	Customer-specific	Customer-specific	Customer-specific	For write access to Knowledge Warehouse in Solution Manager	Transaction SU01

### Internet Graphics Server (IGS) RFC Connection

Table 25

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

## 5.3.1.4 Technical Users

The Technical Users in the following tables are needed for this scenario. They are created automatically or manually during configuration. Technical Users are of type *System User*, if not otherwise stated. For more information on individual technical users, see *Setup Guide* in section *Technical Users*.

## User for READ - access in Managed Systems

Table 26

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>

## User for SAP RWD Info Pak

Table 27

User Name	User Type	Remarks
RWD <i>InfoPak</i> integration user	Communication User	Technical user for web service; assigned role SAP_RWD_INTERFACE

## User for Access in Managed Systems for CDMC

You use the **TMW RFC** - connection for **CDMC** productive systems for analytics activities. For any other than the productive system such as quality acceptance systems (**QA** systems), development systems (**DEV** systems) or test and upgrade system (sandbox / reference systems) use **Trusted RFC** - connection.

## User for Change Management Connection in managed systems

Table 28

User Name	User ID
<i>TMW - User</i>	SMTM<SID of Solution Manager system>

## 5.3.2 Scenario Integration

Implementation refers to the phase in your product life-cycle when you define and refine your business processes by means of solutions, business processes, and related activities. According to the end-to-end business process life-cycle, this phase needs to integrate with a number of other functions, which come into play in your daily business, such as the handling of problems, and so on. The following sections describe the integration of implementation with other scenarios within SAP Solution Manager, and which user roles would be applicable.

### **i** Note

For more detail on each individual scenario, see the according *Scenario - Specific Guide*.

## Business Process Change Analyzer (BPCA)

Users (for instance the *Application Consultant*) can record **TBOMS** for the *Business Process Change Analysis* (**BPCA**). To be able to do so, you need to assign your user the required **BPCA** - single roles:

**SAP\_SM\_BPCA\_TBOM\_ALL** (generating **TBOMS**), and **SAP\_SM\_BPCA\_RES\_ALL** (analyzing results).

In the managed systems, you need to assign the according application-specific authorizations to your users.

## Incident Management

Users can create *Incidents*.

If you are using specific *Transaction Types* for *Incident Management*, you need to assign the according composite role: **SAP\_SUPPDESK\_\*\_COMP**, see scenario-specific guide for Incident Management.

## Issue Management

In *Process Management*, users can create *Issues* to your user. To be able to do so, you need to assign composite role SAP\_ISSUE\_MANAGEMENT\_EXE\_COMP to your user.

## Job Management

You can also integrate *Job Scheduling*. If you assign Job Scheduling related objects, you need to assign user role SAP\_SM\_SCHEDULER\_EXE to your users, see scenario-specific guide for Job Management

## Test Management

You need to use the according *Test Management* relevant roles in the user roles, see scenario-specific guide for Test Management

## Change Request Management

You can use *Change Request Management* functionality with *Process Management*. You need to assign in addition user role SAP\_SOCM\_REQUESTER, see scenario-specific guide for Change Request Management.

## Scope and Effort Analyzer (SEA)

To use the functionality, use either of the two composite roles (administration authorization or display authorization) relevant for SEA end-users: SAP\_SEA\_\*\_COMP. For more information on SEA, see the scenario-specific guide for Effort and Scope Analyzer.

## 5.3.3 Users and Authorizations

### 5.3.3.1 User Roles in the SAP Solution Manager

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for *Process Management*. All users are assigned a composite role, which contains a number of single roles.

#### Project Manager SOLD\_ADMXXX (Help Text ID: TP\_SOLD\_ADM)

##### Single roles included in composite role (Technical Role Name: SAP\_SOL\_PM\_COMP)

Table 29

Single Role	Help Text ID
SAP_RMMAIN_EXE	AUTH_SAP_RMMAIN_EXE
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SOL_TRAINING_ALL	AUTH_SAP_SOL_TRAINING_ALL
SAP_CPR_USER	AUTH_SAP_CPR_USER
SAP_SMWORK_IMPL	AUTH_SAP_SMWORK_IMPL
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE

Single Role	Help Text ID
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_DSH_DISP	AUTH_SAP_DSH_DISP

### **i** Note

In case you require:

- to maintain transports, assign role SAP\_SOL\_TRANSPORT\_EXE.
- display RFC - Destinations, assign role SAP\_SM\_RFC\_DIS

## Application Consultant (Help Text ID: TP\_SOLD\_EXE)

### Single roles included in composite role (Technical Role Name: SAP\_SOL\_AC\_COMP)

Table 30

Single Role	Help Text ID
SAP_RMMAIN_EXE	AUTH_SAP_RMMAIN_EXE
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SOL_TRAINING_ALL	AUTH_SAP_SOL_TRAINING_ALL
SAP_SMWORK_IMPL	AUTH_SAP_SMWORK_IMPL
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_DSH_DISP	AUTH_SAP_DSH_DISP

### **i** Note

In case you require to display RFC - Destinations, assign role SAP\_SM\_RFC\_DIS.

## Technical Consultant (Technical Role Name: SAP\_SOL\_TC\_COMP)

Technical Consultants plan the technical requirements for a project with the Project Manager and the manager of the technical team and then carry out the required technical tasks in the system. Depending on the scope and complexity of the implementation, Technical Consultants may work in several areas, for example, system administration, database administration, network administration, operating system administration, development of cross-application components, or ABAP development.

### Single roles included in composite role

Table 31

Single Role	Restriction on
SAP_RMMAIN_EXE	<i>Roadmap</i> maintenance
SAP_SM_SL_DISPLAY	Display authorization for <i>Process Documentation</i>



Single Role	Restriction on
SAP_SMWORK_IMPL	Access to the <i>Implementation Work Center</i>
SAP_SYSTEM_REPOSITORY_ALL	Full authorizations for the <i>System Landscape</i> in transaction LMDB
SAP_SM_FIORI_LP_EMBEDDED	Access SAP Fiori launchpad

### **i** Note

In case you require to maintain transports, assign additionally role SAP\_SOL\_TRANSPORT\_EXE.

## **Basis/Development Consultant (Technical Role Name: SAP\_SOL\_BC\_COMP)**

Development Consultants work with the project manager and the application consultant on the planning and organization of the authorization concept. They also perform developmental tasks and customer-specific developments.

### **Single roles included in composite role**

Table 32

Single Role	Restriction on
SAP_RMMAIN_EXE	<i>Roadmap</i> maintenance
SAP_SM_SL_EDIT	Maintenance authorization for <i>Process Documentation</i>
SAP_SM_KW_ALL	Contains full authorization for <i>Document Management</i>
SAP_SMWORK_IMPL	Allows access to the <i>Implementation Work Center</i>
SAP_SUPPDESK_CREATE	Full authorization to create an <i>Incident</i>
SAP_SYSTEM_REPOSITORY_DIS	Display authorizations for the <i>System Landscape</i> in transaction LMDB
SAP_SM_FIORI_LP_EMBEDDED	Access SAP Fiori launchpad

### **i** Note

In case you require to maintain transports, assign additionally role SAP\_SOL\_TRANSPORT\_EXE.

## **Display User (Help Text ID: TP\_SOLD\_DIS)**

### **Single roles included in composite role (Technical Role Name: SAP\_SOL\_RO\_COMP)**

Table 33

Single Role	Help Text ID
SAP_RMMAIN_DIS	AUTH_SAP_RMMAIN_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_SMWORK_IMPL	AUTH_SAP_SMWORK_IMPL

Single Role	Help Text ID
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_DSH_DISP	AUTH_SAP_DSH_DISP

### Read-Only User (According to Document Status) (Technical Role Name: SAP\_SOL\_RE\_COMP)

The read-only user is allowed to read only.

#### **i** Note

In contrast to the display user, the read - user can access documents according to the customizing of the document status.

### Single roles included in composite role

Table 34

Single Role	Restriction on
SAP_RMMAIN_READ	Authorization for <i>Roadmap</i> according to the document status
SAP_SM_SL_DISPLAY	Display authorization for <i>Process Documentation</i>
SAP_SM_KW_DIS	Display authorization for <i>Document Management</i>
SAP_SMWORK_IMPL	Allows access to the <i>Implementation Work Center</i>
SAP_SYSTEM_REPOSITORY_DIS	Display authorizations for the <i>System Landscape</i> in transaction LMDB
SAP_SM_FIORI_LP_EMBEDDED	Access SAP Fiori launchpad

### Integration for Business Process Management (BPM) Objects UI

You can grant access to the BPM Object UI for Process Management by assigning role SAP\_SM\_SL\_EDIT\_BPMN.

The *Graphical Process Modelling* application allows the user to create diagram representations of *Solution Documentation* processes. The application is embedded into Solution Documentation and can only be started from there. The following graphical objects (Global Objects) are specific to the application and need to be saved into the application specific database tables:

- Data Object
- Data Store
- Free Components
- Roles

The data are contained in database table AGSGBC\*. They are solution-specific and can only be accessed from the graphical display.

### Authorization Object SM\_GAL\_GO

This authorization object restricts access to the four global objects.

## User Roles

The main authorization object is added to the following roles for *Solution Documentation*:

- SAP\_SM\_SL\_ADMIN
- SAP\_SM\_SL\_DISPLAY

The object is not included in role SAP\_SM\_SL\_EDIT as this role is provided as maintenance role for several scenarios which would not allow maintenance of global objects. Instead role SAP\_SM\_SL\_EDIT\_BPMN is to be used for maintaining global objects in the graphical display.

In addition to the roles, you require Work Center access role SAP\_SMWORK\_IMP.

## Logging

No specific logging information for the access global objects is available. The entities are graphical only without any reuse.

## Custom Attribute Maintenance

In the Interface Documentation application, you can provide attribute data for the interfaces available in your system landscape, such as technical attributes, communication attributes, functional attributes, as well as custom interface technologies for your own custom content. You can access this function within the Interface Documentation window. Access authorization is given within role SAP\_SM\_SL\_ADMIN as well as SAP\_SM\_SL\_EDIT.

## 5.3.3.2 User Descriptions and User Roles in Managed Systems

In the managed system, you need to assign the according user application-specific authorizations. For more information, see the applicable security guide for the relevant application.

## 5.3.3.3 Main Authorization Objects

### Solution Documentation SM\_SDOC

This object allows to control the Process Documentation maintenance. The object contains field SLAN, which is used to restrict a complete solution. In addition, branches of a solution can be restricted, using field SBRA. To allow only for a set of objects and attributes to be used within a certain solution and branches of this solution, you can use field SMUDAUTHGR. This field allows you to use defined authorization groups to bundle objects and attributes. You can maintain specific authorization groups in view cluster SMUD\_AUTHG using transaction SM34.

### Concept of Authorization Area

Authorization areas can protect sub trees of the solution structure. An administrator can assign an authorization area to a structure element. Then, only users that have authorization for authorization object SM\_SDOC with this authorization area name in the field Authorization Area SMUDAREA are allowed to execute activities for this structure element and its children. Authorization areas are defined solution specific. The solution documentation root element and all elements without assignment have the implicit authorization area assignment 'Default' by definition. When no authorization areas have been assigned to the elements of a solution yet, every element has

authorization area 'Default'. The assignment of a structure element to an authorization area is valid for all branches of a solution in which the assigned elements exist. The authorization area explicitly assigned to a structure element is valid for the whole sub tree rooted by the element, excluding all nested sub trees rooted by elements with own authorization area assignments. Non-structure elements always inherit the authorization area from their structure parents. The authorization area determination is branch specific, since the inheritance hierarchy is branch specific. If an element is moved, it may inherit a new authorization area from the new parent. In this case, the authorization area of an element may differ in different branches.

### Concept of Authorization Group

Authorization Groups are defined solution-dependent. As soon as you assign an object or attribute type to user-created authorization group it is not assigned to the *Default* Authorization Group, because an object or attribute type can only be assigned to one Authorization Group. It is not possible to add the same object or attribute to different Authorization Groups. Authorization Groups must always be disjoint.



#### Example

You want to create a role for users that are allowed to see all objects, but only may maintain test cases. Then, you create an Authorization Group for test cases. You assign *Display* Authorization for the Authorization Group '\*' and *Maintenance* Authorization for the Authorization Group *Test Cases*. For another role, you want to allow users to see and maintain all screen entities, but technical objects. Therefore, you assign *Display* and *Maintenance* Authorization for Authorization Group *Default* and *Test Cases*, and you define a new Authorization Group for the technical objects, which you do not include in the role. Then, technical objects are invisible.

### Solution Documentation Administration SM\_SDOCADM

This object allows restrictions on the administrative level, that is administrative tasks on the process documentation level, the branches level, and logical components. As in SM\_SDOC, solution and branches can be restricted. In addition, the concept of aspect is used to further refine activities.

### Transport System S\_CTS\_ADMI

The authorization object is set inactive in all roles due to its critical nature. If you need to allow changes in transaction SCCA you must activate this authorization object.

### Enterprise Search Categories S\_ESH\_CAT

The authorization object is delivered with the following categories included in field ESH\_CATEG:

- ZSMUD\_ROOT
- ZSMUD\_ELEMENTS
- ZSMUD\_DOCUMENTS

Even though the values are delivered in the roles SAP\_SM\_SL\_\*, they are generated by the system when you run the configuration procedure for Process/Solution Documentation.

## 5.3.4 User Roles for Additional Functions

### 5.3.4.1 User Roles for Activation of Business Functions

Within the Process Management, you have the option to evaluate business functions residing in the managed systems and also activate the business function from within the SAP Solution Manager. To do this, you need to

have implementation authorization as described earlier, and additional authorizations. In the following tables we outline, which additional user roles and authorizations, you need to use the functionality for business functions.

### Authorizations in SAP Solution Manager System

In addition to implementation roles, you need to assign authorization object `S_SWITCH` to the users in both systems, the SAP Solution Manager and the managed system. This authorization allows to activate a business function, and should only be assigned to dedicated users. This authorization object is not included in any of the roles delivered by SAP Solution Manager. Therefore, see section in *How-to Guides* on how-to create your own role for this object.

### Authorizations in the Managed System

If you want to activate business functions in the managed system, you need to assign authorization object `S_SWITCH` to the users in both systems, the SAP Solution Manager and the managed system. This authorization allows to activate a business function, and should only be assigned to dedicated users. This authorization object is not included in any of the roles delivered by SAP Solution Manager. Therefore, see section in *How-to Guides* on how-to create your own role for this object. We would also advise to assign roles for switch framework transactions `SFW*`.

In addition, you must also assign role `SAP_SM_BUSINESS_FUNCTION` to the users. This role contains authorizations to read access necessary function groups as test work bench. objects.

## 5.3.4.2 User Roles for Custom Development Management Cockpit (CDMC)

### Configuration

See SAP Note [1244713](#)

### Users and Authorizations

*Custom Development Management Cockpit* can be accessed from the *Implementation and Upgrade* work centers. It contains two use cases:

- Clearing Analysis
- Upgrade/Change Impact Analysis

#### Note

See use case description in the Application Help for SAP Solution Manager in the Help Portal: [▶ help.sap.com](#)  
[▶ SAP Solution Manager](#)

Both use cases involve several systems. The systems are connected by `RFC`.

You must have `TMW RFC` - connection in place for the connection to the productive systems. For the other projects, like Clearing Analysis or Upgrade Change Impact Analysis, `TRUSTED RFC` - connection is used.

#### Caution

If you use a `TRUSTED RFC` - destination, you need to assign to your user in the managed system user role `SAP_CDMC_MASTER` (with full authorization) or `SAP_CDMC_STAT_SYST` (with restricted authorization).

## Custom Development Management Cockpit

Table 35

Name	Type	Remarks
SAP_CDMC_USER	ABAP	Execution authorization for CDMC
SAP_CDMC_MASTER	ABAP	Administration authorization for CDMC including maintaining global settings and deleting CDMC projects
SAP_CDMC_STAT_SYSTEM	ABAP	Restricted authorization for the statistics system in <i>Clearing Analysis</i> . It contains only the authorizations necessary for the tasks carried out on the statistics system. These tasks are activation of statistics collection, import of the collected statistics to the control center, determination of empty tables, syntax check for source code objects.
SAP_SM_CDMC_INT	ABAP	Integration with <i>BPCA</i> authorization object SM_BPCA.

### **i** Note

To be able to work with the result list, assign an additional role SAP\_CDMC\_CRITICAL\_AUTH which contains all relevant critical authorizations for execution. For more information, see the *Description Tab* in the role in the system (transaction PFCG).

In the Solution Manager, you need also assign the authorization object SM\_BPCA to your roles for the user.

## 5.3.4.3 User Roles for Customizing Comparison and Distribution

You have the option to use the function of *Customizing Distribution*. To use this, you need to have implementation authorization as described earlier, and additional authorizations. For *Customizing Comparison* and distribution SAP delivers composite roles for administrator tasks and display user. These composite roles contain a number of single roles, which are outlined underneath.

### Administrator (Technical Role Name: SAP\_CUSTDIST\_ALL\_COMP)

### **i** Note

This role should be assigned *in addition* to one of the following implementation user roles: SAP\_SOL\_PM\_COMP, SAP\_SOL\_AC\_COMP, or SAP\_SOL\_TC\_COMP.

Table 36

Single Role	Remarks
SAP_SCOUT_ALL	Contains full authorization for customizing scout
SAP_SCDT_ALL	Contains full authorization for customizing distribution (transaction SCDT)
SAP_SCIDM_ALL	Contains full authorization for customizing ID-mapping

### Display User (Technical Role Name: SAP\_CUSTDIST\_DIS\_COMP)

#### **i** Note

This role should be assigned *in addition* to one of the following implementation user roles: SAP\_SOL\_RO\_COMP, or SAP\_SOL\_RE\_COMP.

Table 37

Single Role	Remarks
SAP_SCOUT_DIS	Contains display authorization for customizing scout
SAP_SCDT_DIS	Contains display authorization for customizing distribution (transaction SCDT)
SAP_SCIDM_DIS	Contains display authorization for customizing ID-mapping

### Authorization Objects S\_CD\_SYNC and S\_CD\_SYSAC

Important authorization objects are:

- S\_CD\_SYNC  
authorization for synchronizer and scout
- S\_CD\_SYSAC  
controls system access for customizing distribution


## 5.3.4.4 User Roles for BC-Set Activities

You can activate *BC-Sets* in the SAP Solution Manager system, and in the managed system. To be able to use this function in either system your users need one of the following roles:

### User roles for BC-Set Activities

Table 38

Single Role	Remarks
SAP_BCS_ACTIV	Activate BC-Sets

**i** Note  
see [SAP Note 505603](#)  Activate BC Sets.

Single Role	Remarks
SAP_BCS_CREATE	Create BC-Sets
SAP_BCS_ADMIN	Administration of BC-Sets

### 5.3.4.5 User Roles for Project Management

Project Management (PPM) allows you to plan and manage programs and projects in an IT environment in combination with scenarios which are offered in the SAP Solution Manager, such as Change Request Management and Process Management.

#### Technical System Landscape

PPM is running only in the SAP Solution Manager system.

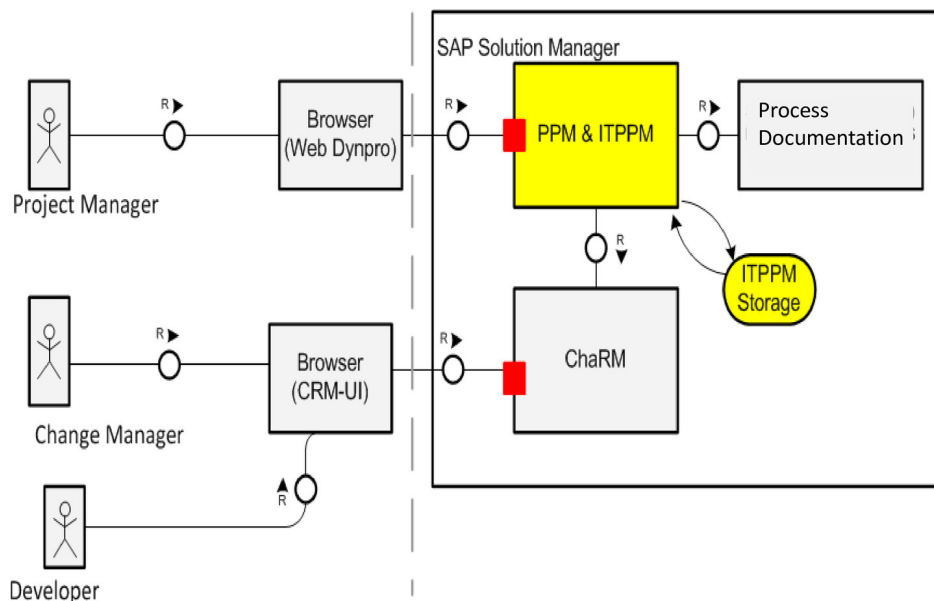


Figure 3: Data Flow

#### Configuration

The configuration is executed by running transaction `SOLMAN_SETUP`.

#### Configuration User

You can either use the suggested configuration user with Standard ID `SMC_PPM_***` (Help Text ID: `USER_SMC_PPM`) or add all required relevant roles to a named user or `SOLMAN_ADMIN`.

In case your security guidelines recommend creating users only in transaction `SU01`, assign composite role `SAP_ITPPM_CON_COMP` to your configuration user.



Table 39

Single Role	Help Text ID
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_ITPPM_CONF	AUTH_SAP_ITPPM_CONF
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP

## End - Users

End-users can be created as template users within the guided procedure for the scenario within transaction SOLMAN\_SETUP.

### **i** Note

The above mentioned roles should be assigned to the Administrator user in addition to composite role SAP\_SOL\_PM\_COMP.

## Project Manager User (Help TXT ID: TP\_ITPPM\_AM)

Analogue Composite Role SAP\_ITPPM\_ADMIN\_COMP

Table 40

Single Role	Help Text ID
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_CPR_PROJECT_ADMINISTRATOR	AUTH_SAP_CPR_PROJECT_ADMINISTRATOR
SAP_CPR_TEMPLATE_ADMINISTRATOR	AUTH_SAP_CPR_TEMPLATE_ADMIN
SAP_CPR_USER	AUTH_SAP_CPR_USER
SAP_BCV_USER2	AUTH_SAP_BCV_USER2
SAP_SM_ITPPM_ALL	AUTH_SAP_SM_ITPPM_ALL
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP
SAP_SMWORK_IMPL	AUTH_SAP_SMWORK_IMPL

## Project Team Member (Help TXT ID: TP\_ITPPM\_TM)

Analogue Composite Role SAP\_ITPPM\_PTM\_COMP

Table 41

Single Role	Help Text ID
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_CPR_USER	AUTH_SAP_CPR_USER
SAP_BCV_USER2	AUTH_SAP_BCV_USER2
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

## Transaction Types

Transaction Type for ITTPM is SMCP.

## Authorization Group for S\_TABU\_DIS

Authorization group for all integration relevant table for ITTPM is SMCP.

## Integration with Change Request Management: Change Manager

In case you use PPM with Change Request Management, you need to additionally assign all roles for the Change Manager user. If you create users via transaction `SOLMAN_SETUP`, the system automatically selects the correct role assignment for this use case. For more information on [Change Request Management](#), see scenario - specific guide for Change Request Management.

## Integration with Change Request Management and Requirement Management: Developer User

In case you use PPM with Change Request Management and Requirement Management, you need to additionally assign all roles for the Developer user from Change Request Management. If you create users via transaction `SOLMAN_SETUP`, the system automatically selects the correct role assignment for this use case. For more information on [Change Request Management](#) or [Requirement Management](#), see scenario - specific guide for Change Request Management or Requirement Management.

## Integration with Requirement Management: Requirement Manager

In case you use PPM with Requirement Management, you need to additionally assign all roles for the Requirement Manager user. If you create users via transaction `SOLMAN_SETUP`, the system automatically selects the correct role assignment for this use case. For more information on [Requirement Management](#), see scenario - specific guide for Requirement Management.

## Issue Management

In case you use ITTPM with [Issue Management](#), you need to additionally assign composite role for the [Issue Management](#) User: `SAP_ISSUE_MANAGEMENT_*_COMP`. For more information on [Issue Management](#), see scenario - specific guide for [Service Delivery and SAP Engagement](#).

## Logging

Authorization of logs is restricted by being able to display the relevant CRM documents in the [Text](#) assignment block of the CRM WebClient UI. There is also a separate logging for PPM (cProject application).

---

## 5.3.5 External Integration

You can integrate with SAP Solution Manager with external products. The term *External Product* refers to either *Third Party Products* or *SAP products*, which can be used to complement a function within SAP Solution Manager.

### 5.3.5.1 Business Process Management Suite

The *Business Process Management Suite* is based on *SAP NetWeaver Composition Environment (CE)*. Integrating this function, allows you to easily model business processes, and document them in your Solution Manager project.

To use this integration, you need to assign in the managed system the User Management (UME) role `SAP_BPM_Solution Manager`. In SAP Solution Manager, your users should be assigned the user roles for implementation as described above.

### 5.3.5.2 Enterprise Service Repository within Process Integration (PI)

*Enterprise Service Repository (ESR)* resides on the SAP product *SAP NW Process Integration (PI)*. It allows you to document the processes, activities, and interfaces in more detail. To use this integration, you need to assign in the managed system the User Management (UME) roles for this environment as described in the according *Process Integration* security guide. In SAP Solution Manager, your users should be assigned the user roles for implementation as described above.

### 5.3.5.3 SAP Productivity Pak application by ANCILE

The *SAP Productivity Pak application by ANCILE* allows you to document in more detail you business processes. To be able to run this integration, you need to create a technical user (type: service user) `RWD_ALIAS` for web service access. This user needs to be assigned role `SAP_RWD_INTERFACE`. Your end-users should be assigned the user roles for implementation as described above.

### 5.3.5.4 Business Process Blueprinting Tool (BPB)

The BPB Tool is supported by an integration between the SAP Solution Manager and the *Solution Composer*. The *Solution Composer* allows data exchange between Solution Manager and Business Process Blueprinting. It synchronizes data between the client and server. SAP Solution Manager stores content of the offered SAP solutions in form of realized business scenarios, business processes and process steps in the Business Process Repository (BPR).

## Additional Information

See the according guides for the *BPB Tool* on the Service Marketplace: ► [service.sap.com/instguides](https://service.sap.com/instguides) ► *SAP Components* ► *SAP Solution Manager* ► *Additional Guides* ►.

## 5.3.6 Traces and Logs

This section provides an overview of the trace and log files that contain, for example, security-relevant information, so that you can reproduce activities if a security breach does occur.

See the *Auditing and Logging* on the Service Marketplace at: ► [help.sap.com](https://help.sap.com) ► *Search Documentation* ►, search for *Auditing and Logging*.

### PANKS (Performance Assistant Note and KBAS Search)

Within the logs of transaction `SOLMAN_SETUP`, the tool allows you to search easily for the relevant SAP Note for an error message within the log.

### Service Connection

If a user has sufficient authorization and is assigned correctly to the appropriate S-user in transaction `AISUSER`, this user can display the same personal contact data (name, phone number) for a system as in SAP Support Portal, as this data is replicated from there to the Solution Manager system. Displaying this data is not logged.

### System Landscape

- Update logs
- RFC logs
- Data save logs

### Customizing Distribution

- Each distribution is logged.
- Each distributed object is logged.

## 5.4 Scenario-Specific Guide: Business Process Change Analyzer

The business process life-cycle stretches via all phases of the life-cycle of a product, the implementation of business processes in a project, their operation as a solution, and the optimization of productive processes in a project. The Business Process Change Analyzer supports this Implementation and Upgrade process within various use cases, for instance:

- Dynamic TBOM (Technical Bill of Material) Recording
- TBOM Creation via 3rd party Test Tool /Test Cases
- Web Services for External Test Tool integration

The function allows you to evaluate the change impact on your changed business processes automatically using trace information.

## 5.4.1 Prerequisites

### 5.4.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete scenario. The SAP Solution Manager is connected via `READ - RFC`, `TRUSTED - RFC` (alternatively `LOGIN`) to your managed systems, and your managed systems are connected to the SAP Solution Manager via `BACK - RFC`. Optionally, you can attach a third party product to the SAP Solution Manager via specified connections. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

#### Technical Infrastructure

- Business Process Change Analyzer

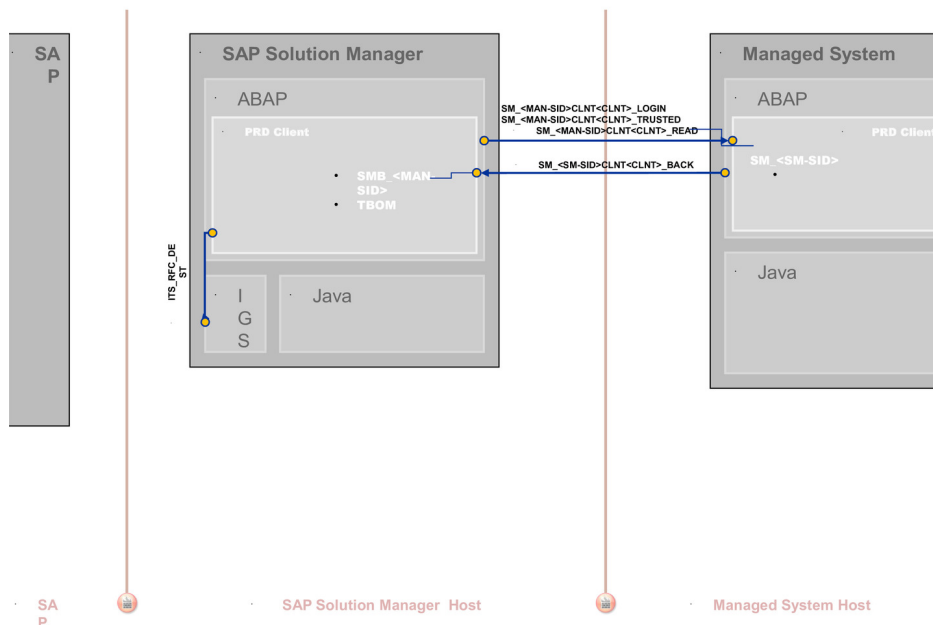


Figure 4: Infrastructure

### 5.4.1.2 Scenario Configuration User

The scenario `BPCA` is configured using transaction `SOLMAN_SETUP`.



#### Creating Configuration User


You can create a specific configuration user (default user name: `SMC_BPCA_<XXXClient>` for `BPCA` (Help Text ID: `USER_CONFIG_BPCA`))

The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

If you create the configuration users manually, the composite roles `SAP_BPCA_CONF_COMP` for `BPCA` contains all single roles, which are automatically assigned to the configuration users. It contains the following single roles:

Table 42

Single Role	Help Text ID
SAP_BPCA_CONFIG	AUTH_SAP_BPCA_CONFIG
SAP_SM_CCM_CONFIG	AUTH_SAP_SM_CCM_CONFIG
SAP_SMUA_ALL	AUTH_SAP_SMUA_ALL
SAP_ROLECMP_ALL	AUTH_SAP_ROLECMP_ALL
SAP_SMWORK_SM_ADMIN	AUTH_SAP_SMWORK_SM_ADMIN
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_BPCA_CRM_INTEGRATION	AUTH_SAP_BPCA_CRM_INTEG
SAP_STWB_2_ALL	AUTH_SAP_STWB_2_ALL
SAP_STWB_WORK_ALL	AUTH_SAP_STWB_WORK_ALL
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SMWORK_CCLM	AUTH_SAP_SMWORK_CCLM
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
 <b>Caution</b> Remove after configuration.	
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SM_BPCA_PTM_INT	AUTH_SAP_SM_BPCA_PTM_INT
 <b>Note</b> PTM and BPCA share some steps in their configuration which are <i>optional</i> on both sides. Therefore, this role contains the delta information for these steps.	

 **Note**

To be able to create users and assign user roles, you need to assign as well role SAP\_SM\_USER\_ADMIN.

## Scenario Configuration Transaction SOLMAN\_SETUP

To configure the *Business Process Change Analyzer* and its *Third Party Integration*, you need to configure it using transaction SOLMAN\_SETUP. During the specific guided configuration, you can create *Standard Template Users*. The system automatically adds all relevant user roles, see according sections on *Users and User Roles*

## 5.4.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Caution

Due to the nature of the use cases in regards to tracing information in managed systems, it is highly recommended to carefully configure SAP Solution Manager and the managed systems, as well as using only SAP recommended roles and authorizations.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 43

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to managed systems and back	RFC	Reading information from managed systems

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

### Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 44

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	Customer-specific	Customer-specific	In case TRUSTED RFC is not used
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	To read data such as business functions, transport requests, Support Packages, repository objects, and so on from the managed systems for BPCA analysis

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific	Optional as Login RFC - Connection can also be used. Needed for TBOM recording of automatic test cases (traces)

### RFC Connection from Managed System to SAP Solution Manager

Table 45

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	SMB_<managed system ID>	For recording of automated test cases to receive trace information about which functions in which managed systems were analyzed	Automatically created via transaction SOLMAN_SETUP (view: managed systems)

### Internet Graphics Server (IGS) RFC Connection

Table 46

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

### Business Warehouse RFC - Connections

Table 47

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	




RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
BI_CLNT<BWclient>if BW is realized in remote BW - scenario system , for content activation and data download	Managed System or Solution Manager System	System-specific	System-specific		in transaction SOLMAN_SETUP
MDX_PARSER (used for the creation of semi-dynamic TBOMs)					

## 5.4.1.4 Technical Users

The technical users in the following tables are needed for this scenario. They are created automatically or manually during configuration. All technical users are of type *System User*. For more information on the individual technical users, see *Secure Configuration Guide* section *Technical Users*

### Users in Managed System


Table 48

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>
Test Automation Framework Technical User	ECATT_ET_USR
 <b>Note</b>	

The technical user ECATT\_ET\_USR is used to log on to SAP Solution Manager from a third party test tool. It is used by the Test Automation Framework in SAP Solution Manager to create TBOMs via automated test cases via a third party tool. The call from SAP Solution Manager to the managed system is made via a trusted RFC destination. This means, that the technical user ECATT\_ET\_USR is also used to log on to the managed system. Therefore, this user must exist with same user ID in both systems, the SAP Solution Manager system and the managed system. It requires the above mentioned authorization for creating TBOMs via a trusted RFC connection.

### User in SAP Solution Manager System

Table 49

User ID	Remarks
User ID and password are customer - specific	User to record TBOM of automatic test cases, assigned role SAP_BPCA_ECATT_COMP.
 <b>Note</b> To use this function, you need to have a trusted RFC - connection authorization in place.	

## 5.4.2 CRM Standard Customizing

An optional use case of the BPCA scenario (TBOM Recording Work Items) is based on CRM, and uses CRM customizing such as Transaction Types, Action Profiles, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects for BPCA. The following table gives you an overview of the Transaction Types used by BPCA.

### Caution

If you copy SAP standard customizing, you need to add the changed values in the according CRM - authorization objects for the scenario. See also:

- on CRM authorizations [Authorization Concept Guide](#)
- on maintenance of authorization objects [How-to Guide on how to maintain authorization objects](#)

### Transaction Types

Table 50

Transaction Type	Usage	Remarks
SMTB	Product Update	The transaction type is delivered with action profile SMTB0001. All actions that are assigned to this action profile have naming convention <SMTB>.

## 5.4.3 Scenario Integration

BPCA refers to the phase in your product life-cycle when you define and refine your business processes by means of projects, business blueprints, and related activities. According to the end-to-end business process life-cycle, this phase needs to integrate with a number of other functions which come into play in your daily business, such as handling of problems, and so on. The following sections describe the integration of BPCA with other scenarios within SAP Solution Manager.

### Note

For more detail on each individual scenario, see the according *Scenario—Specific Guide*.

### Test Management: Create Test Plans

BPCA is used to prepare the test phase. You can create test plans. To be able to create test plans, assign additionally single role SAP\_STWB\_2\_ALL.

### Change Request Management: Request for Change and Change Document

You can run analyses for Requests for Change and Change Documents using BPCA. To see the details of documents, you can jump into the CRM WebUI, directly. In addition to the basic BPCA composite roles, you require composite role SAP\_SM\_CRMWEBUI\_INT\_DIS\_COMP. This composite role contains all relevant roles for this integration:

- SAP\_SM\_CRMUI\_INTEGRATION\_DIS (CRM authorizations)

- SAP\_SM\_CRM\_UIU\_SOLMANPRO (CRM Business Role without authorizations)
- SAP\_SM\_CRM\_UIU\_SOLMANPRO\_CHARM (CHARM - related UIU\_COMP authorizations)
- SAP\_SM\_CRM\_UIU\_FRAMEWORK (General UIU\_COMP authorizations)

For more information, see scenario-specific guide for [Change Request Management](#).

## 5.4.4 Users and Authorizations

### 5.4.4.1 User Descriptions and User Roles

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for BPCA. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. The view *Administration* is only visible for the *Quality Expert*. Here, authorization object S\_TCODE with value SPRO is required. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW. For more information about User Interface authorizations, see [Authorization Concept Guide](#).

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

#### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system must be assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

#### Authorizations in Managed Systems

All users need according application authorization in the managed system and role SAP\_SM\_BPCA\_TBOM for recording activities.

For Business Process Change Analyzer, you need to assign authorizations in the managed system depending on the application you are using in the managed system. In addition, when you are using the trusted RFC - connection, you need to assign authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL) to your user. This authorization object is not included in profile SAP\_ALL and in the composite roles.

#### Quality Expert (Help Text ID: TP\_BPCA\_QE)

##### Technical composite role name SAP\_BPCA\_ALL\_COMP in the Solution Manager system/client

Table 51

Single Roles	Help Text ID
SAP_SM_BPCA_TBOM_ALL	AUTH_SAP_SM_BPCA_TBOM_ALL

Single Roles	Help Text ID
SAP_SM_BPCA_RES_ALL	AUTH_SAP_SM_BPCA_RES_ALL
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_STWB_WORK_ALL	AUTH_SAP_STWB_WORK_ALL
SAP_STWB_2_ALL	AUTH_SAP_STWB_2_ALL
SAP_STWB_INFO_ALL	AUTH_SAP_STWB_INFO_ALL
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_BPCA_CRM_INTEGRATION	AUTH_SAP_BPCA_CRM_INTEGRATION
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

**Technical composite role name: SAP\_SM\_BW\_BPCA\_ADMIN\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 52

Single Roles	Help Text ID
SAP_BI_E2E_BPCA	AUTH_SAP_BI_E2E
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

**Business Process Expert (Help Text ID: TP\_BPCA\_BPE)**

**Technical composite role name SAP\_BPCA\_EXE\_COMP in the Solution Manager system/client**

Table 53

Single Roles	Help Text ID
SAP_SM_BPCA_TBOM_EXE	AUTH_SAP_SM_BPCA_TBOM_EXE
SAP_SM_BPCA_RES_DIS	AUTH_SAP_SM_BPCA_RES_DIS
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_STWB_WORK_ALL	AUTH_SAP_STWB_WORK_ALL
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

**Technical composite role name: SAP\_SM\_BW\_BPCA\_DISPLAY\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 54

Single Roles	Help Text ID
SAP_BI_E2E_BPCA	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Display User (Help Text ID: TP\_BPCA\_DIS)

Technical composite role name SAP\_BPCA\_DIS\_COMP in the Solution Manager system/client

Table 55

Single Roles	Help Text ID
SAP_SM_BPCA_TBOM_DIS	AUTH_SAP_SM_BPCA_TBOM_DIS
SAP_SM_BPCA_RES_DIS	AUTH_SAP_SM_BPCA_RES_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_STWB_INFO_DIS	AUTH_SAP_STWB_INFO_DIS
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_BPCA_CRM_INTEGRATION	AUTH_SAP_BPCA_CRM_INTEGRATION
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_STWB_WORK_DIS	AUTH_SAP_STWB_WORK_DIS

### ECATT user (Help Text ID: TP\_BPCA\_ECATT)

Technical composite role name SAP\_BPCA\_ECATT\_COMP in the Solution Manager system/client

Table 56

Single Roles	Help Text ID
SAP_SM_BPCA_TBOM_ALL	AUTH_SAP_SM_BPCA_TBOM_ALL
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_STWB_WORK_DIS	AUTH_SAP_STWB_WORK_DIS
SAP_STWB_2_ALL	AUTH_SAP_STWB_2_ALL
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## Critical Authorization Objects

### Authorization Object S\_TRANSPRT

BPCA must be able to look at the content of all transport requests in order to analyze it, or in order to perform the obsolescence check for TBOMs. Therefore, the field for transport type is not restricted.

### Authorization Object S\_DEVELOP

BPCA must be able to gather information, such as package, Application Component Hierarchy (ACH), versions, for any development object in a system for TBOM recording, obsolescence check, and BPCA analysis. Therefore, the fields such as package or object type are not restricted.

### Authorization Object S\_ADMI\_FCD

To run TBOM recording, authorization object S\_ADMI\_FCD with value PADM is required. This authorization allows to perform process administration functions like the change of profile parameters. You can remove this authorization in the role, if you set the following required profile parameters in advance (see also SAP Note [2138643](#)):

- `rstr/accept_remote_trace = true`: This parameter should be set on all managed systems that are potentially accessed by RFC from the primary managed system in which the TBOM is recorded.
- `rstr/send_global_trace = true`: This parameter needs to be set only on the primary managed system in which the TBOM recording starts.

## 5.4.5 Additional Security Measures

This section gives you an overview over additional measures to prevent malicious attacks for *BPCA* use cases.

### Restrict Trace File Access

Trace files are stored on the file system of the managed system. The application does not ensure that access to this file is only happening in an authorized way. Ensure that only an administrator on infrastructure level is able to read traces.

### Restrict Data Browser Access (Transaction SE16)

Access to the *Table Data Browser* can allow a user to view sensitive data. If application data with sensitive information is traced, exclude the respective table from SE16 access.

#### ➔ Recommendation

We recommend to trace only configuration information, otherwise critical information from managed systems might be exposed.

### Authorization Group for Tables

Authorization group BPCA is assigned to all relevant tables for BPCA scenario. The authorization group is added as a value in authorization object S\_TABU\_DIS for all relevant roles.

## 5.5 Scenario-Specific Guide: Test Management

### 5.5.1 Prerequisites

#### 5.5.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete *Test Management* scenario. The SAP Solution Manager is connected via `READ - RFC`, `TRUSTED - RFC` (alternatively `LOGIN`) to your managed systems. Optionally, you can attach a third party product to the SAP Solution Manager via specified connections. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

##### Technical Infrastructure

- Test Management

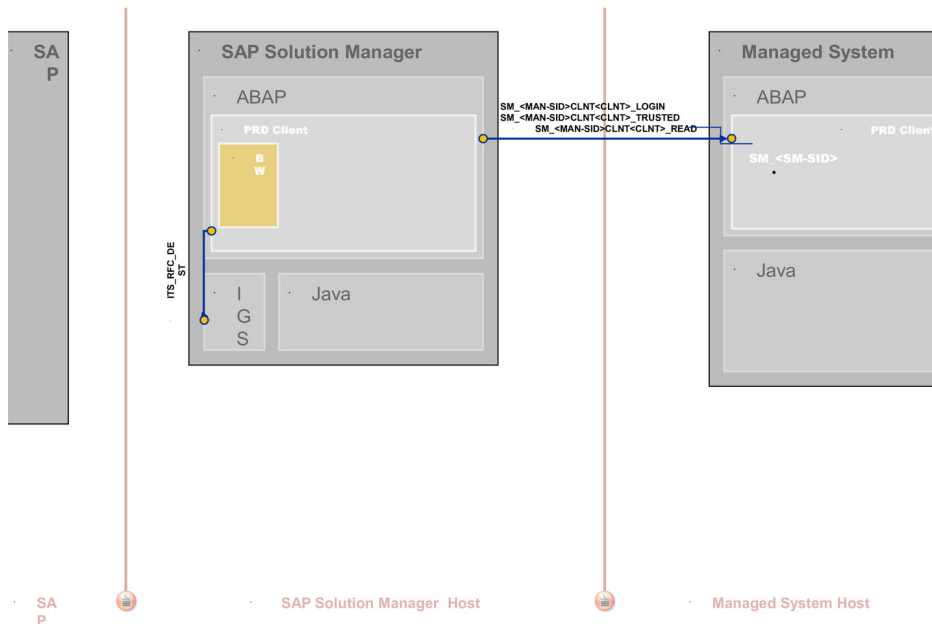


Figure 5: Infrastructure

#### 5.5.1.2 Scenario Configuration

##### **i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see Authorization Concept Guide chapter *Configuration Users*.
- the BW integration concept, see Authorization Concept Guide chapter on BW integration.

## Creating Configuration Users for Running Configuration in Transaction SOLMAN\_SETUP

You have different possibilities of creating the configuration user:

- Use default user SMC\_\*:

When you configure your scenario using the respective automated configuration procedure per scenario via transaction SOLMAN\_SETUP, the system asks you to create a specific configuration user with a default user name:

- **Test Management:** SMC\_TM\_<SystemID> (Help Text ID: USER\_CONFIG\_TM)

Table 57

Single Role	Help Text ID
SAP_TM_CONFIG	AUTH_SAP_TM_CONFIG
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP_ADMIN
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH-SAP_SYSTEM_REPOSITORY_ALL
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN

- Use user SOLMAN\_ADMIN and add additional user roles. Enter the user ID for user SOLMAN\_ADMIN in the pop-up and assign the roles.
- Do not use default user, create your own configuration user in transaction SU01: Set the flag for **Manual Maintenance** in the SOLMAN\_SETUP pop-up, and create your user in transaction SU01.

### ➔ Recommendation

If you want to create the configuration users manually, we recommend to assign:

- the composite role SAP\_TM\_CONF\_COMP which contains all single roles that are automatically assigned to the configuration user for **Test Management** in the SAP Solution Manager system.
- the composite role SAP\_CBTA\_CONF\_COMP which contains all single roles that are automatically assigned to the configuration user for **CBTA** in the SAP Solution Manager system.

### **i** Note

To be able to:

- create users and assign user roles, you need to assign as well role SAP\_SM\_USER\_ADMIN.
- use a trusted RFC connection between the Solution Manager and the managed systems, you need to assign role SAP\_SM\_S\_RFCACL in the Solution Manager system as well as the managed system.

### **i** Note

In the **Test Management work center** view **Administration** you find links for configuration purposes. This view contains links to configuration transactions which are necessary for daily operational use of the work center, such as creating Business Partners or checking RFC Connections. The view can only be accessed using the



administration role for the scenario (see later section on *User Roles*), as the view is restricted by authorization object `S_TCODE` with value `SPRO`.

### 5.5.1.3 Communication Channels and Destinations

The tables below show the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 58

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems and back	RFC	Reading information from managed systems
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes
Solution Manager to/from Quality Center by HP	SOAP over HTTP (S)	Test requirements (send and receive data)
Third - Party Test Tools	SOAP over HTTP (S)	Depends on the individual application

#### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

#### RFC Connections from SAP Solution Manager to Managed Systems

Table 59

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	Customer-specific	Customer-specific	can be used instead of TRUSTED connection

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system> (automatically generated, can be defined by customer via transaction SMSY)	To read data from the managed system
SM_<SID>CLNT<Client>_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	current user	You have the same user ID in the managed system

#### Internet Graphics Server (IGS) RFC Connection

Table 60

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Transaction SM59

#### BW- Reporting RFC Connection

Table 61

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	
BI_CLNT<BWclient>, if BW is realized in remote BW - scenario system, for content activation and data download	Managed System or Solution Manager System	System-specific	System-specific		in transaction SOLMAN_SETUP
<SolutionManagerSID>CLNT<SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client	System-specific	System-specific	BI_CALLBACK (customer specific)	in transaction SOLMAN_SETUP

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
Trusted RFC to remote BW system SAP_BILO	remote BW - system (source: SAP Solution Manager)	System-specific	System-specific	Dialog User	Used to read data from remote BW for BI - Reporting, created during SOLMAN_SETUP

## 5.5.1.4 Technical Users

The technical user in the following table is created automatically during configuration. For more information on the individual technical users, see the *Secure Configuration Guide* in section *Technical Users*.

### User in Managed Systems

Table 62

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>

## 5.5.2 Scenario Integration

*Test Management* refers to the phase in your product life-cycle when you test and validate your business processes by means of projects. According to the end-to-end business process life-cycle, this phase needs to integrate with a number of other functions, which come into play in your daily business, such as handling of problems, and so on. The following sections describe the integration of test management with other scenarios within SAP Solution Manager, and explain which user roles would be applicable.

### **i** Note

For more detail on each individual scenario, see the according *Scenario-Specific Guide*.

### Business Process Change Analyzer (BPCA)

In the process documentation of SAP Solution Manager, users (for instance the Basis Development Consultant) can record TBOMS for the *Business Process Change Analysis*. To be able to do so, you need to assign your user the required BPCA - roles: SAP\_SM\_BPCA\_TBOM\_ALL (generating TBOMS), and SAP\_SM\_BPCA\_RES\_ALL (analyzing results).

In the managed systems, you need to assign the according application-specific authorizations to your users.

## Incident Management

In the process documentation application, users can create Incidents. To be able to do so, you need to assign user role `SAP_SUPPDESK_CREATE`. For processing damaged test case incidents, use composite role `SAP_SUPPDESK_PROCESS_COMP`.

## 5.5.3 Users and Authorizations

### 5.5.3.1 User Descriptions and User Roles

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for *Test Management*. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`.

#### **i** Note

Old Work Center access is available with transaction `STWB_OLD`, which is contained in the Work Center role `SAP_SMWORK_ITEST`.

For more information about User Interface authorizations, see *Authorization Concept Guide*.

#### Authorization for Trusted RFCs between SAP Solution Manager, Managed Systems, and BW - System

Trusted authorizations are needed between SAP Solution Manager and its managed systems, as well as SAP Solution Manager and a remote BW - system.

- In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object `S_RFCACL` (role `SAP_SM_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`). The user in the BW - system is also assigned authorization `S_RFCACL` (role `SAP_SM_BW_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`).
- The user in the managed system receives role `SAP_SM_S_RFCACL` (Help Text ID: `AUTH_SAP_S_SM_RFCACL`) with authorization object `S_RFCACL`.

Both roles are not contained in the respective composite roles, due to their highly security-relevant character.

#### Application - Specific Authorizations in Managed Systems

For *Test Management*, you need to assign authorizations in the managed system depending on the application you are using in the managed system. In addition, when you are using the trusted RFC - connection, you need to assign authorization object `S_RFCACL` to your user. This authorization object is not included in profile `SAP_ALL`.

#### Tester (Help Text ID: TP\_TM\_TM)

Single roles included in composite role (technical role name: `SAP_TEST_TESTER_COMP`)

Table 63

Single Role	Help Text ID
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_STCE_EXE	AUTH_SAP_STCE_EXE
SAP_STWB_INFO_DIS	AUTH_SAP_STWB_INFO_DIS
SAP_STWB_WORK_ALL	AUTH_SAP_STWB_WORK_ALL
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE

### Project Manager/Test Organizer (Help Text ID: TP\_TM\_PM)

#### Single roles included in composite role (technical role name: SAP\_TEST\_PM\_COMP)

In the SAP Solution Manager system

Table 64

Single Role	Help Text ID
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_STWB_2_ALL	AUTH_SAP_STWB_2_ALL
SAP_STWB_INFO_ALL	AUTH_SAP_STWB_INFO_ALL
SAP_STWB_SET_ALL	AUTH_SAP_STWB_SET_ALL
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE

#### **i** Note

If you want to use the Test Management Dashboard, you need to assign additionally single role SAP\_SM\_DASHBOARDS\_DISP\_TW.B.

#### Technical composite role name: SAP\_SOL\_BW\_AC\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same User ID in the BW system.

Table 65

Single Roles	Help Text ID
SAP_BI_E2E_SMT	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Basis Development Consultant (Help Text ID: TP\_TM\_BC)

#### Single roles included in composite role (technical role name: SAP\_TEST\_BC\_COMP)

In the SAP Solution Manager system

Table 66

Single Role	Help Text ID
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SM_CBTA_TRANSPORT	AUTH_SAP_SM_CBTA_TRANSPORT
SAP_STWB_INFO_ALL	AUTH_SAP_STWB_INFO_ALL
SAP_SMWORX_ITEST	AUTH_SAP_SMWORX_ITEST
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_RMMAIN_EXE	AUTH_SAP_RMMAIN_EXE

#### Note

If you want to use the Test Management Dashboard, you need to assign additionally single role SAP\_SM\_DASHBOARDS\_DISP\_TW.

#### Technical composite role name: SAP\_SOL\_BW\_AC\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same User ID in the BW system.

Table 67

Single Roles	Help Text ID
SAP_BI_E2E_SMT	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Display User (Help Text ID: TP\_TM\_RO)

#### Single roles included in composite role (technical role name: SAP\_TEST\_RO\_COMP)

Table 68

Single Role	Help Text ID
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS

Single Role	Help Text ID
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_STWB_INFO_DIS	AUTH_SAP_STWB_INFO_DIS
SAP_STWB_2_DIS	AUTH_SAP_STWB_2_DIS
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### **i** Note

If you want to use the Test Management Dashboard, you need to assign additionally single role SAP\_SM\_DASHBOARDS\_DISP\_TWB.

### Technical composite role name: SAP\_SOL\_BW\_AC\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 69

Single Roles	Help Text ID
SAP_BI_E2E_SMT	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

## Authorization Objects

### SM\_SMT\_TWB

The authorization object allows to access and to manage the Test Management data of the Test Workbench in the Solution Manager layer directly. It substitutes the authorization object S\_TWB in most cases. In all cases when S\_TWB is still used, it is specifically explained.

### SM\_TPCK and SM\_TPLN

The authorization objects allow to access and to manage the Test Packages and Test Plans in the Solution Manager. It is included in roles SAP\_STWB\_2\_\*.

### Authorization Groups for Tables (S\_TABU\_DIS)

Test Management uses authorization group TSTM to protect tables. The group is added to authorization object S\_TABU\_DIS in the relevant roles.

### SM\_WC\_VIEW

Within the new Release 7.2, the work center is redesigned, though you can still call the old work center using transaction STWB\_OLD. You can restrict the views for both work center within the authorization field help. Only assign entries with suffix OLD to the old work center views, and NEW to the new work center views.

## 5.5.4 Additional User Roles

### 5.5.4.1 User Roles for Test Workbench Workflow

The workflow functionality can specify and start actions at specified events in the Test Management process or during testing.

#### User Roles

The user role for Test Workbench Workflow needs to be assigned to the user in addition to the respective composite role.

#### Test Workbench Workflow

Table 70

Role	Restriction on
SAP_STWB_WORKFLOW_ADMIN	Full authorization
SAP_STWB_WORKFLOW_CREATE	Authorization to create actions
SAP_STWB_WORKFLOW_DIS	Display authorization

#### CRM Standard Customizing

The workflow functionality is based on CRM, and uses CRM Customizing such as Transaction Types, Action Profiles, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects for workflow. The following table gives you an overview of the Transaction Types used.

#### Caution

If you copy SAP standard customizing you need to add the changed values in the according CRM - authorization objects for the scenario. See also How-to Guide on how to maintain authorization objects.

#### Transaction Types

Table 71

Transaction Type	Usage	Remarks
TWSQ	Test Sequence Procedure (Test Organizer)	Supported, Status Profile: TWSQ0001 used in authorization object B_USERSTAT and B_USERST_T
TWTP	Test Plan Tester Procedure (Test Organizer)	Supported, Status Profile: TWTP0001 used in authorization object B_USERSTAT and B_USERST_T

#### Authorization Objects

The main CRM - authorization objects are included in the according roles. For details see *Authorization Concept Guide*, section on *CRM integration*.



## 5.5.4.2 User Roles for Extended Capabilities

You use test case work items to assign incorrect or unfinished test cases for further maintenance to a responsible person. This person can display these test cases as so called work items in the inbox.

### User Roles

Table 72

Role	Restriction on
SAP_STWB_WITC_CREATE	Authorization to create or maintain work items
SAP_STWB_WITC_EXE	Authorization to maintain work items as responsible person, but not to create new ones
SAP_STWB_WITC_ADMIN	Administration authorization
SAP_STWB_WITC_DIS	Display authorization

### CRM Standard Customizing

The workflow functionality is based on CRM, and uses CRM Customizing such as transaction types, action profiles, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects for workflow. The following table gives you an overview of the transaction types used.

#### Caution

If you copy SAP standard customizing you need to add the changed values in the according CRM - authorization objects for the scenario. See also *How-to Guide* on how to maintain authorization objects.

### Transaction Types

Table 73

Transaction Type	Usage	Remarks
TWTC	Test case maintenance	Supported, Status profile: TWTC0001 used in authorization object B_USERSTAT and B_USERST_T

### Authorization Objects

#### CRM - Authorization Objects

The standard CRM - authorization objects are used. For details, see [Authorization Concept Guide](#), section on CRM integration

#### Authorization object SM\_TSTMGNT

This authorization object controls, if a Test Case work item can be created or changed.

## 5.5.4.3 User Roles for CBTA (Component-Based Test Automation)

*Component Based Test Automation* is an optional SAP Software Component which can be installed on SAP Solution Manager. It allows creation, usage and maintenance of automated tests. Such tests can be executed on various (Systems under Test) SUT. CBTA supports the following SUT:

- SAP SUT based on ABAP technology, such as SAP GUI, CRM Web UI, Web Dynpro ABAP, and so on.
- SAP SUT running non-ABAP technology, such as Web Dynpro Java, BSP, and so on.
- SAP SUT running a mix of ABAP and non-ABAP technology, such as Java-ABAP double Stacks, Portal, and so on.
- Non-SAP SUT, such as 3rd party servers running Web technology, and so on.

You use: CBTA use cases:

- without TBOM creation (BPCA integration)
- with TBOM creation

### Configuration

#### Configuration Procedure

You can configure CBTA in transaction SOLMAN\_SETUP. .

#### **i** Note

The Systems Under Test must not be a productive system.

### Configuration User

The configuration can be executed using user SMC\_CBTA\_>SID>, which you can create when calling the CBTA configuration procedure in transaction SOLMAN\_SETUP.

Composite role SAP\_CBTA\_CONFIG\_COMP

Table 74

Single Role	Help Text ID
SAP_SM_CBTA_CONFIG	AUTH_SAP_SM_CBTA_CONFIG
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH-SAP_SYSTEM_REPOSITORY_DIS
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_FIORI_LP_EMBEDDED	SAP_SM_FIORI_LP_EMBED

## Caution

Role `SAP_SM_CBTA_CONFIG` contains transaction `SM30` with authorization object `S_TABU_DIS` value `&NC&` (no authorization group). The table that is maintained is `ECCUST_ET`, which is used for registering the CBTA tool. See SAP NOTE [1976897](#) to maintain a specific authorization group for the table.

## Used RFC - Connections and Users

### Note

For detailed information, see SAP Note [1763697](#).

In general, the scenario is using the RFCs as defined in `SOLMAN_SETUP`, see transaction `SOLMAN_SETUP`.

In order to enable automated testing, information needs to be persisted on SAP Solution Manager in order to enable the CBTA application to communicate with the SUT. For this purpose, the SUT Management Application allows to define:

1. System Under Test which is subject of the test.
  - The SUT based on ABAP technology: RFC- destination (with technical user)
  - SUT not based on ABAP technology: URL is to be provided in order to identify the SUT
2. User ID for the scenario execution
  - SUT based on ABAP technology: the provision is mandatory
  - SUT not based on ABAP technology: the provision is optional

User credentials are persisted in the Secure Password Storage.

Disregarding of which scenario you use, between your SAP Solution Manager system (TCE) and your managed system (SUT), the following RFC connections are in place:

- READ RFC: `SM_<SID>_CLNT<Client>_READ` with technical user `SM_<SID>`
- RFC: `TST_<SUTSID>_CLNT<Client>` with technical user `TST_SUT_<SolutionManagerSID>`
- Trusted (can also be Login) RFC destination as defined in the Target System of the SDC
- BACK RFC with `BACK RFC` user

## Data Flow Information

### Creation / Maintenance of Test Profiles (Design Time) - User: Test Coordinator/Administrator

1. Selection of the System Data Container (SDC) to be used
2. Import of chosen SDC definition into SUT Management Application.  
This creates an enhanceable structure *SDC – SDC Target Systems – System Roles*.
3. Definition of SDC Enhancements in SUT Management per available System Role.

### Usage of Test Profiles in Test Scripts (Runtime)

1. Creation of tests in Test Composition Environment (TCE).
  - Selection of underlying SDC and Target System
  - Selection of appropriate Test Profile
  - Execution of Recording Wizard  
(records the business scenario processed on the SUT, creates automatically the Test Script components out of the recorded scenario, persists in the Test Repository)

2. Execution of previously created tests from within TCE.
3. Maintenance of previously created tests from within TCE.

**i Note**

For both recording- and execution scenarios, the opening of sessions on the SUT is necessary. For this session opening, data from tables of SUT Management Application are retrieved. Execution authorization is required for accessing that data at runtime.

**Technical System User on the Managed System: TST\_<SolutionManagerSID>**

To be able to work with CBTA, you need to have a system user TST\_<SolutionManagerSID> in place for the respective RFC TST\_<SUTSID>\_CLNT<Client>. This user needs the following roles:

**Technical User Roles**

Table 75

Role	Help Text ID
SAP_TST_AGENT_RFC	AUTH_SAP_TST_AGENT_RFC
SAP_CRM_TST_RFC (optional)	AUTH_SAP_CRM_TST_RFC
<p><b>i Note</b></p> <p>If your managed system is a CRM-based system, you need to add role SAP_CRM_TST_RFC. Download this role from your SAP Solution Manager system onto your PC, then upload it in your CRM system. You need to maintain the authorization objects, generate the profile, and execute the user comparison.</p>	
SAP_WDA_TST_RFC	AUTH_SAP_WDA_TST_RFC
<p><b>i Note</b></p> <p>If your managed system is a WD-ABAP-based system</p>	

**Authorization for Trusted RFC between SAP Solution Manager and Managed System (SUT)**

In case of BPCA integration, the end-user on the Solution Manager system and in the managed system are assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

**Test Engineer Standard ID: CBA\_TE\_>SID> (Help Text ID: TP\_CBTA\_TE)**

**User Roles in the SAP Solution Manager System**

Composite role technical name: SAP\_CBTA\_EXE\_COMP

Table 76

Role	Help Text ID
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_SUTMAN_EDIT	AUTH_SAP_SM_SUTMAN_EDIT
SAP_SM_CBTA_EDIT	AUTH_SAP_SM_CBTA_EDIT
SAP_SM_CBTA_TRANSPORT	AUTH_SAP_SM_CBTA_TRANSPORT
SAP_STCE_ALL	AUTH_SAP_STCE_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Test Coordinator Standard ID: CBA\_TC\_<SID> (Help Text ID: TP\_CBTA\_TC)

#### User Roles in the SAP Solution Manager System

Composite role technical name: SAP\_CBTA\_ADMIN\_COMP

Table 77

Role	Help Text ID
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_SUTMAN_ADMIN	AUTH_SAP_SM_SUTMAN_ADMIN
SAP_SM_CBTA_ADMIN	AUTH_SAP_SM_CBTA_ADMIN
SAP_SM_CBTA_TRANSPORT	AUTH_SAP_SM_CBTA_TRANSPORT
SAP_STCE_ALL	AUTH_SAP_STCE_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Test Engineer Standard ID: CBA\_DIS\_<SID> (Help Text ID: TP\_CBTA\_DIS)

#### User Roles in the SAP Solution Manager System

Composite role technical name: SAP\_CBTA\_DIS\_COMP

Table 78

Role	Help Text ID
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_SUTMAN_DIS	AUTH_SAP_SM_SUTMAN_DIS
SAP_SM_CBTA_DIS	AUTH_SAP_SM_CBTA_DIS
SAP_STCE_DIS	AUTH_SAP_STCE_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## SUT Management Role for Managed System Users

### User Roles in the Managed Systems (SUT)

Table 79

Role	Help Text ID
Business Relevant Application Role	

### **i** Note

If you integrate CBTA with BPCA due to TBOMS, assign the user roles for BPCA (SAP\_SM\_BPCA\_TBOM) to your users, see scenario-specific guide for *Business Process Change Analyzer* in this document chapter *User Description and User Roles*.

## Run Library Manager (RTL) Integration

The role SAP\_SM\_TST\_RTL\_DEV can be assigned to the Test Engineer user who is allowed to use the RTL Management.

The RTL Manager is a client side tool that allows customizing the VB script libraries that CBTA uses at runtime when recording and executing test scripts. The CBTA runtime library is stored centrally in the MIME repository of the SAP Solution Manager system. The folder SAP/PUBLIC/CBTA in transaction SE80 (MIME Repository) contains the official runtime library (CBASE.zip) that SAP delivers. Additional files are stored at that location when submitting the customizing.

The RTL Manager provides the ability to write additional custom functions that the test scripts may need when automating the test of some business scenarios where the common approach (based on default components) is not sufficient. When executing a CBTA test script, the VB script coding corresponding to the test is sent from SAP Solution Manager MIME repository to the client computer and executed using the VB script interpreter. The Runtime Library is a set of VB scripts providing helper classes, functions and procedures that are necessary to simulate actions that are normally performed by a regular user. Default Components are components performing atomic operations against User Interface elements. The Runtime Library (RTL) is delivered with default components for all the User Interface Technologies that CBTA supports. With the help of the RTL Manager, the following is possible:

- The developer can check out the Runtime Library to his local file system with the purpose to modify it. He/she can add custom code at the specified locations.
- When he/she has finalized the custom code, then he/she can save the modifications back to SAP Solution Manager MIME Repository. This allows, that the libraries are available for other testers.
- By transporting the changes, the libraries can be updated as well on additional Solution Manager Systems in the landscape.

## BPCA TBOM Integration

If you integrate CBTA with BPCA due to TBOMS, assign the user roles for BPCA (SAP\_SM\_BPCA\_TBOM and SAP\_SM\_SL\_DISPLAY) to your users, see security guide for *Business Process Change Analyzer* in this document chapter *User Description and User Roles*.

## CRM Standard Customizing

The workflow functionality is based on CRM and uses CRM Customizing such as Transaction Types, Action Profiles, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects for workflow. The following table gives you an overview of the Transaction Types used.

## Caution

If you copy SAP standard customizing you need to add the changed values in the according CRM - authorization objects for the scenario. See also *How-to Guide* on how to maintain authorization objects.

## Transaction Types

Table 80

Transaction Type	Usage	Remarks
TWTC	Test case maintenance	supported, status profile: TWTC0001 used in authorization objects B_USERSTAT and B_USERST_T

## Critical Authorization Objects

### S\_TABU\_NAM

Authorization object S\_TABU\_NAM allows display of table RFC\_READ\_TABLE (in configuration role for configuration user). This table is used to determine which scenarios are relevant in the setup.

### SM\_SUTMNGT

This authorization object controls access and execution for SUT Management. The activities are checked for SUT Management definitions for the explicitly listed System Data Containers:

- Execute: usage of SUT Management Test Profiles and the defined user credentials in test cases.
- Maintain: creation, modification and deletion of definitions in SUT Management
- Check: verification of definitions in SUT Management (credentials, technical destination)
- Import: enables all SDC import activities into SUT Management.

The activities do not have dependencies and can be granted independently.

## Scenario Integration

SUT Management is integrated with CBTA capability of SAP Solution Manager, and CBTA is integrated with Test Management as external tool. It can be invoked via:

- Test Composition Environment
- Transaction STCE
- Transaction SECATT
- Process Management
- Test Packages in Test Plans

## Note

CBTA is also strongly connected to scenario BPCA in regards to TBOM. For more information, see scenario-specific guide for BPCA.

## Additional Security Related Information

### SSL Communication Security

To make sure that downloading and uploading of the RTL files is protected, make sure that the SSL option is selected in the *Communication Security*. Mark the check box *User ID/Password* in the *Transport Channel Authentication* section.

## 5.5.5 Partner Integration

### 5.5.5.1 Tool with BC – ECATT- Integration

You can integrate an external test tool with eCatt.

#### Roles for eCatt - Integration

Table 81

Role	Remarks
SAP_ECET	Authorization for saving and loading of test scripts with eCatt. This role is automatically assigned during technical user generation, see IMG - activity <i>Generate User</i> (technical name: SOLMAN_ETEST_USER), assigned to technical user of type <i>Service</i> , for instance SM_ECATT
SAP_SM_ECET	Authorization to use Test Automation Framework (TAF), must be assigned manually to technical user of type <i>Service</i> , for instance SM_ECATT

#### **i** Note

Both roles are assigned to the generated user, for instance SM\_ECATT.

### 5.5.5.2 Partner Test Management

Business Processes are defined in the SAP Solution Manager in application *Process Documentation*. In case, you use a Partner Test Management Tool for testing the process documentations, you can send the process documentation from the SAP Solution Manager system to the Partner Test Management (PTM) tool. When the Business Blueprint is transferred to the PTM tool, the testers carry out the manual/ automated testing and create the defects in the PTM tool. As soon as the testing cycle is completed in PTM, the test results and the created defects are transferred back to the SAP Solution Manager system.

#### Configuration

The configuration is executed by running transaction SOLMAN\_SETUP.

#### Configuration User

You can either use the suggested configuration user with Standard ID SMC\_PTM\_\*\*\* (Help Text ID: USER\_CONFIG\_PTM) or add all required relevant roles to a named user or SOLMAN\_ADMIN.



In case your security guidelines recommend creating users only in transaction SU01, assign composite role SAP\_PTM\_CONF\_COMP to your configuration user.

**⚠ Caution**

If you require *Switch Framework* authorization (for instance for transaction SFW5), you need to add the transaction (authorization object S\_TCODE) and the according authorization object S\_SWITCH. The authorization is not included in the role due to security reasons.

**Analogues Composite Role SAP\_PTM\_CONF\_COMP**

Table 82

Single Role	Help Text ID
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_PTM_CONF	AUTH_SAP_PTM_CONF
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_BPCA_PTM_INT	AUTH_SAP_SM_BPCA_PTM_INT

**i Note**

PTM and BPCA share some steps in their configuration which are optional on both sides. Therefore, this role contains the delta information for these steps.

**End - Users**

End-users can be created as template users within the guided procedure for the scenario within transaction SOLMAN\_SETUP.

**Administration User (Help TXT ID: TP\_PTM\_ADM)**

**Analogues Composite Role SAP\_PTM\_ADMIN\_COMP**

Table 83

Single Role	Help Text ID
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Single Role	Help Text ID
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_TMT_ADMIN	AUTH_SAP_TMT_ADMIN
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS

### Maintenance User (Help TXT ID: TP\_PTM\_EXE)

Analogue Composite Role SAP\_PTM\_EXE\_COMP

Table 84

Single Role	Help Text ID
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SMWORk_ITEST	AUTH_SAP_SMWORk_ITEST
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_TMT_EXE	AUTH_SAP_TMT_EXE
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS

### Display User (Help TXT ID: TP\_PTM\_DIS)

Analogue Composite Role SAP\_PTM\_DIS\_COMP

Table 85

Single Role	Help Text ID
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_SMWORk_ITEST	AUTH_SAP_SMWORk_ITEST
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_TMT_DISP	AUTH_SAP_TMT_DISP
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS

## Technical User

### SAML2 Technical User (Technical Name: SM\_HPCOM)

#### Technical User Roles

Table 86

Roles	Help Text ID
SAP_SUPPDESK_INTERFAC E	AUTH_SAP_SUPPDESK_TMT_INTER
SAP_TMT_INTERFACE	AUTH_SAP_SUPPDESK_TMT_INTER
SAP_SUPPDESK_ADMIN	AUTH_SAP_SUPPDESK_ADMIN

### Test Management Alias User (Technical Name: TMT\_ALIAS)

#### Technical User Roles

Table 87

Roles	Help Text ID
SAP_TMT_WSDL_ACCESS	AUTH_SAP_TMT_WSDL_ACCESS

#### Additional Information

##### Authorization Group for S\_TABU\_DIS

PTM shares with Service Desk Configuration authorization group SDCD.

## 5.5.6 Additional Security Measures

### Application Log

A user can access the application log in transaction SLG1. The according object is SMT\_TWB and the sub-object is DEFAULT.

## 5.6 Scenario-Specific Guide: Scope and Effort Analyzer (SEA)

The business process lifecycle stretches via all phases of the lifecycle of a product, the implementation of business processes in a project, their operation as a solution, and the optimization of productive processes in a project. These phases are realized in the SAP Solution Manager system using such units as projects (for implementation and optimization) and solutions (for productive operations). The *Scope and Effort Analyzer* supports the Test Management process.

The Scope and Effort Analyzer (SEA) allows you to analyze the impact of a Support Package or Enhancement Package without installing the corresponding software. The analysis capability relies on the functions Business Process Change Analyzer (BPCA) and Custom Code Management (CCM) to calculate the impact, see scenario-specific guides for both scenarios.

A SEA analysis is defined via a guided activity that is used to collect all necessary input for such an analysis. Afterwards, the analysis runs in the background. As soon as the analysis is finished, you can display the analysis result.

This guide gives you an overview over all relevant security-related issues for the scenario.

## 5.6.1 Getting Started

**What is this guide about?** SAP Solution Manager covers a wide range of diverse scenarios you can use. You might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides per scenario which cover all relevant information for this specific scenario.

### Caution

Before you start using this scenario-specific guide, you must read the core information about security issues in SAP Solution Manager, and the *Secure Configuration Guide*, which refers to all security-relevant information during basic configuration of SAP Solution Manager. Without this information, we do not recommend to set up any specific scenario. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

This guide covers the following topics:

- **Getting Started:** find out about target groups of this guide. Links for any additional components can be found in the Core Guide.
- **Prerequisites:** find out about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other.
- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).
- **Scenario Integration:** according to the life-cycle approach the various scenarios integrate with each other. Here, you can find out about authorizations you need to assign to your users for these cases.

## 5.6.2 Prerequisites

### 5.6.2.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete scenario.

In general, Scope and Effort Analyzer (SEA) is based on the technical system landscape as explained in scenarios BPCA and CCM as it is based on their infrastructure.

Within SEA functionality the following system types are used:

1. Update System (system for planned update)
2. Custom Code System (system to read custom developments and modifications)
3. Statistic System (system to read usage statistics)
4. Test System (system used for test scope optimization activities)
5. Solution Manager System
6. BW-System

## 5.6.2.2 Scenario Configuration User

The scenario relies heavily on the integration to the following scenarios:

- Custom Code Management
- Business Process Change Analyzer

At least Custom Code Management should be configured to run SEA successfully. For configuration information and users, see the respective scenario-specific guides for both scenarios. Both scenarios are configured using transaction `SOLMAN_SETUP`.

### SICF Report Group

The SICF-report group to activate all relevant SICF-services is `SM_SEA`. For more information on SICF-report groups in SAP Solution Manager, see section on ICF Services in this guide.

## 5.6.2.3 Communication Channels and Destinations

During the guided activity for SEA analysis, systems are selected which are used during the analysis run. For these systems RFC-connections are needed as well as access to a BW-system.

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 88

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to managed systems and back	RFC	Reading information from managed systems

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 89

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	Customer-specific	Customer-specific	In case TRUSTED RFC is not used
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID of Solution Manager system>	To read data such as business functions, transport requests, Support Packages, repository objects, and so on from the managed systems for BPCA analysis
SM_<SID>CLNT<Client>_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific	Optional as Login RFC - Connection can also be used. Needed for TBOM recording of automatic test cases (traces)

### RFC Connection from Managed System to SAP Solution Manager

Table 90

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	SMB_<managed system ID>	For recording of automated test cases to receive trace information about which functions in which managed systems were analyzed	Automatically created via transaction SOLMAN_SETUP (view: managed systems)

### Internet Graphics Server (IGS) RFC Connection

Table 91

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

### Business Warehouse RFC - Connections

Table 92

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	
BI_CLNT<BWclient>if BW is realized in remote BW - scenario system , for content activation and data download	Managed System or Solution Manager System	System-specific	System-specific		In transaction SOLMAN_SETUP
MDX_PARSERfor ODBO BAPI					Used for the creation of semi-dynamic TBOMs)

## 5.6.2.4 Technical Users

The technical users in the following tables are created automatically or manually during configuration. For more information on the individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

### **i** Note

This scenario relies on BPCA - relevant configuration. For information on BPCA, see *Scenario - Specific Guide for BPCA*.

### User in Managed Systems

Table 93

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>

## 5.6.3 User Descriptions and User Roles

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for SEA. All users are assigned a composite role, which contains a number of single roles.

### Work Center

The Work Center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW. For more information about User Interface authorizations, see [Authorization Concept Guide](#).

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system must be assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

### Administrator

#### Technical composite role name SAP\_SEA\_ALL\_COMP in the Solution Manager system/client

Table 94

Single Roles	Restriction on
SAP_SEA_ALL	Run SEA functionality
SAP_SM_BPCA_RES_ALL	BPCA result analysis
SAP_SM_BPCA_TBOM_EXE	BPCA TBOM
SAP_SM_SL_EDIT	Process Documentation maintenance
SAP_SM_KW_ALL	KW full authorization
SAP_SMWORK_ITEST	Work Center access
SAP_BPCA_CRM_INTEGRATION	BPCA CRM integration
SAP_SYSTEM_REPOSITORY_DIS	System Landscape display
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori Launchpad

#### Technical composite role name: SAP\_SM\_BW\_CCM\_ADMIN\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same User ID and Password in the BW system.

Table 95

Single Roles	Remarks
SAP_BI_E2E_CCM	BI data download for CCM



Single Roles	Remarks
SAP_SM_BI_ADMIN	BI administration

## Display User

### Technical composite role name SAP\_SEA\_DIS\_COMP in the Solution Manager system/client

Table 96

Single Roles	Restriction on
SAP_SM_BPCA_TBOM_DIS	Display of BPCA TBOM
SAP_SM_BPCA_RES_DIS	BPCA result analysis display
SAP_SEA_DISPLAY	SEA display
SAP_SM_SL_DISPLAY	Process Documentation display
SAP_SM_KW_DIS	KW display
SAP_SMWORK_ITEST	Access to WC
SAP_SYSTEM_REPOSITORY_DIS	System Landscape display
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori Launchpad

### Technical composite role name: SAP\_SM\_BW\_CCM\_DISPLAY\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same User ID and Password in the BW system.

Table 97

Single Roles	Remarks
SAP_BI_E2E_CCM	BI data download CCM
SAP_SM_BI_DISP	BI display

## 5.6.4 Authorization Objects

### S\_TABU\_DIS

All tables and views start with prefix AGSSEA\_\* and are assigned to authorization group SEA.

### SM\_SEA

The field ACTVT of authorization object SM\_SEA can have the following values:

- 01 – Create, execute and restart an analysis
- 02 – Change an analysis
- 03 – Display an analysis
- 06 – Delete an analysis

# 6 Application Operations and Business Process Operation

This application-specific guide contains the following functions:

- Application Operations
  - System Monitoring
  - Exception Management
  - Data Readiness Management
  - Process Integration Monitoring
  - Message Flow Monitoring
  - End-User Experience Monitoring
  - Hana and BI-Monitoring
  - Interface and Connection Monitoring
  - Job Monitoring
  - Self Monitoring
  - IT Infrastructure Monitoring
  - Integration Visibility
- Business Process Operations
  - CDC
- Job Management

## 6.1 Document History

Here, all changes to the specific scenario guide are listed according to Support Package.

Table 98

Support Package Stacks (Version)	Description
SP01	<b>Adaptations with Release 7.2 Relevant for all Subscenarios</b> <ul style="list-style-type: none"><li>• Roles <code>SAP_SMWORK_BASIC_*</code> and <code>SAP_SM_BI_BILO</code> obsolete</li><li>• All roles for <i>Technical Monitoring</i> have been adapted to <code>SAP_BASIS 7.40</code>.</li><li>• Authorization object <code>SM_WC_VIEW</code> from role <code>SAP_SMWORK_BASIC_*</code> has been transferred into Core Roles.</li><li>• Added to all L2 users role <code>SAP_SM_MAI_REPORTING</code></li><li>• Removed from all L2 users role <code>SAP_SM_BI_BILO</code></li></ul>

Support Package Stacks (Version)	Description
	<p><b>Adaptations Business Process Operations</b></p> <ul style="list-style-type: none"> <li>• Role SAP_SMWORK_BPM obsolete</li> <li>• Roles SAP_SM_SOLUTION_* and SAP_SOLMAN_DIRECTORY_* are removed from user roles, substituted by new roles SAP_SM_SL_* accordingly, see section on <i>Users and Authorizations</i>.</li> <li>• Removed section on <i>Solution Maintenance</i></li> <li>• Added new authorization objects according to Software Components SAP BASIS and ST</li> <li>• Deleted roles SAP_CDC_ADMIN and SAP_CDC_DIS</li> <li>• Additional role assignment for integration with Job Monitoring and Interface Channel Monitoring for template users.</li> </ul> <p><b>Adaptations Job Management</b></p> <ul style="list-style-type: none"> <li>• Role SAP_SM_SOLUTION_* is removed from user roles, substituted by new roles SAP_SM_SL_* accordingly, see section on <i>Users and Authorizations</i>.</li> <li>• Substituted role SAP_BPMJSM_BW_ALL_REPORTING with role SAP_SM_BPMON_REPORTING</li> <li>• All core roles SAP_SM_SCHEDULER_* and role SAP_SMWORK_JOB_MAN adapted</li> <li>• Removed section on <i>Solution Maintenance</i></li> <li>• New authorization objects added from SAP_BASIS</li> <li>• Substituted authorization object SM_JSM_SCH with SM_JSM_SDL</li> </ul> <p><b>Adaptations System Monitoring</b></p> <ul style="list-style-type: none"> <li>• Work Center for System Monitoring is obsolete, according Work Center role SAP_SMWORK_SYS_MON is not delivered anymore.</li> </ul> <p><b>Adaptations Interface Channel Monitoring</b></p> <ul style="list-style-type: none"> <li>• Added role SAP_SM_SYM_LEVEL01 to Level 2 user.</li> </ul> <p><b>SAP Fiori Integration</b></p> <ul style="list-style-type: none"> <li>• All users receive SAP Fiori Embedded Launchpad authorizations, role SAP_SM_FIORI_LP_EMBEDDED</li> </ul>
SP02	<p><b>Business Process Operations</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>• Adapted role SAP_BP_OPERATIONS_ADMIN_COMP</li> </ul> <p><b>System Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>• Adapted role SAP_SM_SYM_LEVEL*</li> <li>• Added role SAP_DBA_DISP to composite role SAP_SM_L2_COMP</li> </ul> <p><b>Interface Channel Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>• Adapted role SAP_SM_IC_CONF</li> <li>• Added BW authorizations to Level 1 User: SAP_BI_E2E_SM, SAP_SM_BI_DISP</li> </ul> <p><b>PI Monitoring</b></p>

Support Package Stacks (Version)	Description
	<p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Adapted roles SAP_SM_PIM_LEVEL*</li> </ul> <p><b>End-User Experience Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Adapted role SAP_SM_EEM_LEVEL02</li> </ul>
SP03	<p><b>BI - Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Adapted roles SAP_SM_BIM_LEVEL*</li> <li>Adapted role SAP_SM_BIM_CONF</li> <li>Additional section on <i>Data Readiness Monitoring</i> (DRM)</li> </ul> <p><b>Job Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Adapted roles SAP_SM_JMON_LEVEL*</li> </ul> <p><b>End - User Experience Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Adapted roles SAP_SM_EEM_LEVEL*</li> <li>Adapted role SAP_SM_EEM_CONF</li> <li>Adapted technical names of User IDs from &lt;EEM&gt; to &lt;UXM&gt;</li> <li>Integration of new SAP Fiori App, see separate section</li> </ul> <p><b>PI Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Adapted role SAP_SM_PIM_CONF</li> <li>Adapted roles SAP_SM_PIM_LEVEL*</li> </ul> <p><b>BP Operations</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Adapted role SAP_SMWORK_BPO and added Fiori Catalogue for <i>Data Consistency Management</i></li> <li>New roles SAP_SM_BPOIMP_* for <i>Business Process Improvement</i>, see according new section</li> </ul> <p><b>CDC</b></p> <p>Adaptations of terminology for roles.</p> <p><b>Message Flow Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>Delivered new roles for SAP Fiori App: Message Flow Monitoring, see new section</li> <li>Adapted roles SAP_SM_MFM_LEVEL*</li> </ul> <p><b>Interface Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>• Adapted roles SAP_SM_IC_LEVEL*</li> <li>• Adapted role SAP_SM_IC_CONF</li> </ul> <p><b>System Monitoring</b></p> <p>Adaptations of authorization objects in roles are described in <i>Menu</i> tab of the respective role</p> <ul style="list-style-type: none"> <li>• Adapted roles SAP_SM_SYM_LEVEL*</li> </ul> <p><b>Exception Management</b></p> <ul style="list-style-type: none"> <li>• new section for scenario <i>Exception Management</i>.</li> </ul>

## 6.2 Scenario-Specific Guide: Technical Monitoring

### 6.2.1 Prerequisites

#### 6.2.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete Technical Monitoring. The SAP Solution Manager is connected via `READ - RFC`, `Trusted - RFC` (alternatively `LOGIN`) to your managed systems, and your managed systems are connected to the SAP Solution Manager via `BACK - RFC`. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

Technical Infrastructure  
 • Technical Monitoring

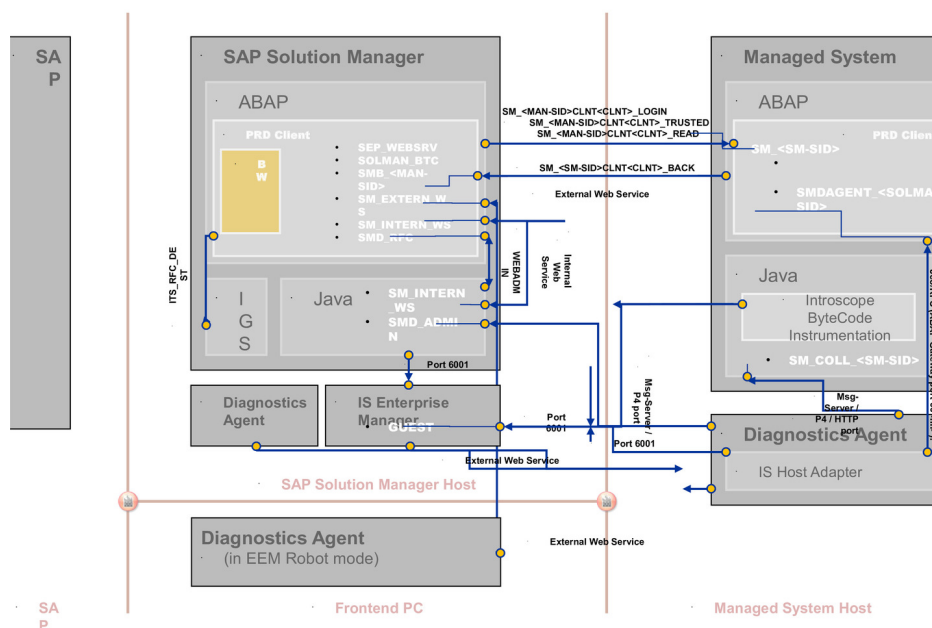


Figure 6: Infrastructure

**i** Note

The PI Monitoring depends on the version of the PI-system used. It is currently only available as of PI 7.11 Support Package 6, and PI 7.30.

## 6.2.1.2 Scenario Configuration Users

**i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see *Authorization Concept Guide* chapter *Configuration Users*.
- the BW integration concept, see *Authorization Concept Guide* chapter on BW integration.

You configure the technical monitoring scenarios using the automated guided procedure in the SAP Solution Manager Configuration work center or the transaction `SOLMAN_SETUP`.

To configure the scenarios, proceed as follows:

### Creating Configuration User in Transaction `SOLMAN_SETUP`

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic functions.

When you configure your scenario using automated configuration, the system asks you to create a specific configuration user (default technical user name: `SMC_<sub-scenario>_<XXXclient>`) for the individual sub-scenarios:

- System Monitoring including SolMan Self-Monitoring, Connection Monitoring, and Interface Monitoring (default user name: SMC\_SM\_<SMclient>)
- End-User Experience (default user name: SMC\_EEM\_<SMclient>)
- PI Monitoring (default user name: SMC\_PI\_<SMclient>)
- HANA and BI Monitoring (default user name: SMC\_BIMN\_<SMclient>)
- IC Monitoring (default user name: SMC\_IC\_<SMclient>)

### **i** Note

If access to the application is required, add user authorization for Level 02 Template users.

- Message Flow Monitoring (default user name: SMC\_MFM\_<SMclient>)
- Infrastructure Monitoring including SAP IT Infrastructure Management (default user name: USER\_SMC\_ITMO and USER\_SMC\_ITMA)

### **i** Note

To be able to use Infrastructure Monitoring, you need to configure:

1. SAP IT Infrastructure Management
2. Infrastructure Monitoring

As a prerequisite you need to have applied the according Add-On.

- Early Watch Alert Management (default user SOLMAN\_ADMIN)
- Self Monitoring (default user SOLMAN\_ADMIN)

The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration. You have different possibilities of creating configuration users for configuration purposes:

- Use *default user* SMC\_\*: Create the default user via pop-up.
- Use *user* SOLMAN\_ADMIN and add additional user roles: Enter user ID for user SOLMAN\_ADMIN in the pop-up and assign the roles.
- Do *not use default user*, create your own configuration user in transaction SU01: Set the flag for Manual Maintenance in the SOLMAN\_SETUP pop-up. and create your user in transaction SU01.

### **➔** Recommendation

If you want to create the configuration users manually, you need to assign:

- the composite roles SAP\_<sub-scenario>\_CONF\_COMP which contain all single roles that are automatically assigned to the configuration users in the SAP Solution Manager system.

### **i** Note

To be able to:

- create users and assign user roles, you need to assign as well role SAP\_SM\_USER\_ADMIN.
- use a trusted RFC connection between the Solution Manager and the managed systems, you need to assign role SAP\_SM\_S\_RFCACL in the Solution Manager system as well as the managed system.

- the composite role `SAP_SM_BW_<sub-scenario>_CONF_COMP` which contains all single roles that are automatically assigned to the configuration user in the BW system.

**i Note**

To be able to use a trusted RFC connection between the Solution Manager and the BW-system, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system and role `SAP_SM_BW_S_RFCACL` in the BW-system.

### Scenario Configuration transaction SOLMAN\_SETUP

To configure the individual scenarios, you need to configure it using transaction `SOLMAN_SETUP`.

During the specific guided configurations you can create Standard template users. The system automatically adds all relevant user roles, see according sections on *Users and User Roles*.

## 6.2.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager for all technical Monitoring scenarios.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 99

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems and back	RFC	Reading information from managed systems
Solution Manager to remote BW - system	RFC	
Solution Manager to managed systems	HTTP	
Solution Manager to managed systems	Web Service	
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes



## Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 100

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system> Customer-specific	To read data from the managed system (pullmetrics: availability, exceptions, performance, configuration → visible in the Repository Tool

### RFC Connection from Managed System to SAP Solution Manager

Table 101

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	Default user: SMB_<managed system ID> (Customer-specific)	pushmetrics : visible in the Repository Tool	Automatically created via transaction <code>SOLMAN_SETUP</code> (view: managed systems)

### BW- Reporting RFC Connection

Table 102

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	
BI_CLNT<BWclient> if BW is realized in remote BW - scenario system , for content activation	Managed System or Solution	System-specific	System-specific		In transaction <code>SOLMAN_SETUP</code>

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
	Manager System				
<SolutionManagerSID>CLNT<SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client	System-specific	System-specific	BI_CALLBACK (customer specific)	In transaction SOLMAN_SETUP
Trusted RFC to remote BW systemSAP_BILO	remote BW - system (source: SAP Solution Manager)	System-specific	System-specific	Dialog User	Used to read data from remote BW for BI - Reporting . created during SOLMAN_SETUP

#### Internet Graphics Server (IGS) RFC Connection

Table 103

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

#### CCMSPing RFC Connection

Table 104

RFC Destination Name	Activation Type	Logon User (Password)	Use (Scenario)	Remarks
CCMSPING.<server> <SystemNr.>	Registered Server Program (program ccmsping.00)	CSMREG (customer-specific)	Service Level Reporting with CCMSPING; system availability overview in System Monitoring work center; IT Performance Reporting	User created during configuration of Central Monitoring (CCMS),

## 6.2.1.4 Technical Users

The technical users in the following tables are created automatically or manually during configuration. All technical users are of type System Users, except for the Java stack user. For more information on the individual technical users, see *Landscape Setup Guide* in section *Technical Users*.

## User in Managed Systems

Table 105

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>
Java data collector user	SM_COLL_<SID of SolMan>



### Caution

- If your managed system runs on SAP\_BASIS 7.31 or higher, you need to add the following authorization object to your READ user for PI Monitoring purposes (in particular for PI Message Alerting): S\_XMB\_ALERT with activity ACTVT:33 and CONSUMER\_ID: full authorization.
- The *PI Consumer* should be set to full authorization to allow it for all Solution Manager systems. You can restrict it also to specific consumers. The consumer - ID is usually: SOLMAN\_<SID of SolMan>.

## 6.2.2 Scenario Integration

Technical Monitoring refers to the phase in your product life-cycle when you operate your systems, and you have to monitor them. According to the end-to-end business process life-cycle, this phase needs to integrate with a number of other functions which come into play in your daily business, such as handling of problems and so on. The following sections describe the integration of technical monitoring with other scenarios within SAP Solution Manager, and which user roles are applicable.



### Note

For more detail on each individual scenarios, see the according *Scenario-Specific Guide*.

### Incident Management

In Technical Monitoring users can create Incidents for an alert. The according user role SAP\_SUPPDESK\_CREATE is included in the L user composite roles. If you want your users to also check for their Incident messages, you should assign composite role SAP\_SUPPDESK\_PROCESS\_COMP.



### Note

- A key user can only display his/her own messages, when the key user is the reporter.
- For a key user to see messages created by other users, see SAP Note [1256661](#) (1. Substitution).

### Root Cause Analysis

Technical Monitoring is highly integrated with Root Cause Analysis. The according role SAP\_RCA\_DISP is included in the user roles.

### Notification Management (Technical Administration)

You can create notifications. The according role SAP\_NOTIF\_ADMIN is included in the user roles. You can create notifications from Alert Inbox and Connection Monitoring

## EarlyWatch Alert / Service Report Generated Documents

To view generated documents for *EarlyWatch* Alert, you need to assign role `SAP_OP_DSWE_EWA` to your user.

### 6.2.3 User Descriptions

To enable your users to work with the application, you need to assign them authorizations in the Solution Manager system and in the managed systems.

When you are operating the SAP Solution Manager and its managed system, you need to monitor your system landscape. We deliver recommended user descriptions on which SAP delivered roles are modeled. In general, Technical Monitoring distinguishes three different types of users for all scenarios.

The according user descriptions and roles can only be regarded as templates for you. You need to first define which tasks the individual members in your company execute, and then adjust the according roles.

#### Caution

The roles delivered by SAP can only be regarded as models for adjustment to your company's needs.

#### Level 1 Users

Level 1 users assigned to a level 1 role have access to all display activities, and are able to distribute incoming events and alerts to other users. The assigned users are not allowed to do central or local Root Cause Analysis, or to change the configuration of the different monitoring capabilities. These users are also not allowed to confirm alerts.

#### Level 2 Users

Level 2 users assigned to a level 2 role can be considered as a second level for a particular topic. They have all authorizations as level 1 users for a this topic. In addition, they have access to all end-to-end Root Cause Analysis capabilities provided by SAP Solution Manager as well as to all local Root Cause Analysis capabilities provided by the managed systems. The assigned users are not allowed to change the configuration of the different monitoring capabilities.

#### Configuration Users

Configuration users assigned to a configuration role can be considered as a kind of third level for a particular topic. They have all authorizations for configuration purposes. In case they need authorization as level 1 users and level 2 users for a certain topic, add these authorizations to the user. In addition, they have access to setup and configuration capabilities of the different monitoring capabilities. Setup and configuration of Technical Monitoring capabilities is available in SAP Solution Manager Configuration Work Center.

### 6.2.4 Early Watch Alert Management Configuration

In this paragraph, the *Guided Procedure* for the *Early Watch Management Configuration* is explained in more detail in regards to authorization objects and values. These authorizations reflect authorization objects which are included in roles `SAP_SETUP_MANAGED` and `SAP_SETUP_MANAGED_DISP`. This Guided Procedure is run by user `SOLMAN_ADMIN` due to the nature of Early Watch Alert as mandatory feature for all SAP customers.

## **i** Note

To run *Early Watch Management Configuration* successfully on itself, you need to assign additionally the following roles in the Solution Manager system:

- SAP\_SYSTEM\_REPOSITORY\_ALL
- SAP\_RCA\_ADT\_ADM
- SAP\_RCA\_CONF\_ADMIN
- SAP\_SDCCN\_ALL (optional)

in the managed system:

- SAP\_SM\_USER\_ADMIN
- SAP\_RCA\_CONF\_ADMIN
- SAP\_J2EE\_ADMIN
- SAP\_SDCCN\_ALL (optional)

## 6.2.5 User Roles for System, Database, Host Monitoring, and Self - Monitoring

### 6.2.5.1 First Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

#### First Level User (Help Text ID: TP\_SM\_L1)

Technical composite role SAP\_SM\_L1\_COMP in SAP Solution Manager system

Table 106

Single Roles	Help Text ID
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SM_LEVEL01
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### 6.2.5.2 Second Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

## Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

### Second Level User (Help Text ID: TP\_SM\_L2)

#### Technical composite role SAP\_SM\_L2\_COMP in SAP Solution Manager system

Table 107

Single Roles	Help Text ID
SAP_SM_SYM_LEVEL02	AUTH_SAP_SM_SYM_LEVEL02
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARD_ALM
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_BP_DISPLAY	SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_DBA_DISP	AUTH_SAP_DBA_DISP

#### Technical composite role name: SAP\_SM\_BW\_SM\_L2\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system. For more information on BW user concept, see section on BW configuration in section Prerequisites.

Table 108

Single Roles	Help Text ID
SAP_BI_E2E_SM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

## 6.2.5.3 Integration of SAP Fiori Applications

Here, you find specific information on the individually delivered applications that can be used on a central Fiori Hub.

## **i** Note

General configuration and role information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the security guide for the Authorization Concept for Solution Manager.

### **APP: System Monitoring (Use Case)**

System Monitoring proactively monitors the status of the systems, hosts, and databases in the SAP Solution Manager system landscape. The end user can analyze the status of various metrics, events, and alerts generated. Users can do the following:

- Get a status overview of all technical systems, including instances, databases, and hosts.
- Drill down from status overview information to single metrics and events.
- Display the details of metrics and events, including their thresholds and current rating or value
- Access landscape information.

### **Authorizations in the Back-end SAP Solution Manager**

- The relevant Odata - Service is added to the core role `SAP_SM_SYM_LEVEL01` for System Monitoring.
- In the back-end SAP Solution Manager system assign the relevant composite role `SAP_SM_LEVEL01_COMP` to the user or create the template user via transaction `SOLMAN_SETUP`. Due to the nature of the application, as a subset of the complete functionality of System Monitoring, not all authorizations for the user in this role are required. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SM_SYM_LEVEL01` role accordingly. Remove in authorization object `SM_MOAL_TC` `ACTVT` `PO` (postpone).
- To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S RFC` and `S RFCACL` authorization.

## **i** Note

As you can modify SAP Fiori Apps to your own purpose, we do not deliver any specifically predefined roles for them.

### **Authorizations in the Frond-end**

The following two roles are delivered for front-end usage for the application (Software Component ST-UI):

- `SAP_STUI_APPOPS_TCR`  
This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_APPOPS_AUTH`  
This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, do the following:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

## 6.2.6 User Roles for Process Integration - Monitoring

### 6.2.6.1 First Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

The views EEM or System Monitoring are visible, because Interactive Reporting can also be called via these views. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see [Authorization Concept Guide](#).

#### First Level User (Help Text ID: TP\_PIM\_L1)

Technical composite role SAP\_PIM\_L1\_COMP in SAP Solution Manager system

Table 109

Single Roles	Help Text ID
SAP_SM_PIM_LEVEL01	AUTH_SAP_SM_PIM_LEVEL01
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### 6.2.6.2 Second Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

The views EEM or System Monitoring are visible, because Interactive Reporting can also be called via these views. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

#### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object S RFCACL (role SAP\_SM\_S RFCACL; Help Text ID: AUTH\_SAP\_S\_SM RFCACL). The user in the BW - system is also assigned authorization S RFCACL (role SAP\_SM\_BW\_S RFCACL; Help Text ID: AUTH\_SAP\_S\_SM RFCACL).

#### Second Level User (Help Text ID: TP\_PIM\_L2)

Technical composite role name SAP\_PIM\_L2\_COMP in SAP Solution Manager system



Table 110

Single Roles	Help Text ID
SAP_SM_PIM_LEVEL02	AUTH_SAP_SM_PIM_LEVEL02
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARD_ALM
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

#### Technical composite role name: SAP\_SM\_BW\_PIM\_L2\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 111

Single Roles	Help Text ID
SAP_BI_E2E_PIM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

#### Roles in the PI managed system

Table 112

UME role/group	Remarks
SAP_XI_RWB_SERV_USER	Used for adapter engine PING and self-test DC
SAP_XI_RWB_SERV_USER_MAIN	
XI_AF_CHANNEL_ADMIN	Used for channel status DC

## 6.2.7 User Roles for Message Flow Monitoring

### 6.2.7.1 Technical System Landscape

The technical system landscape of Message Flow Monitoring MFM is oriented on the overall technical system landscape of Technical Monitoring, specifically PI Monitoring. Nevertheless, some functions offered have an impact on the managed system:

- Restart or cancel of PI Message
- Process or delete Idoc

Since these functions are changing data in the managed system, it is required to use a specific user for data collection, which is not the standard user for it. This is achieved by using Trusted RFC-destinations or, in case of Web Service communication, logical ports with ticket based authentication.

RFC-communication is used between SAP Solution Manager (ABAP stack) and managed system of type ABAP. Web Service communication is used between SAP Solution Manager (ABAP stack) and managed system of type Java. All connections are created during the managed system configuration. They have usually the following names:

- RFC: SM\_<SIDofMgmtSys>CLNT<Client>\_TRUSTED
- Logical Port: E2E\_SOLMAN\_<SIDofMgmtSys>DIALOG

## 6.2.7.2 First Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

The views EEM or System Monitoring are visible, because Interactive Reporting can also be called via these views. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

### First Level User (Help Text ID: TP\_MFM\_L1)

Technical composite role SAP\_MFM\_L1\_COMP in SAP Solution Manager system

Table 113

Single Roles	Remarks
SAP_SM_MFM_LEVEL01	AUTH_SAP_SM_MFM_LEVEL01
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Authorizations in the Managed System

If the current user is used to logon to managed system via Trusted RFC or assertion ticket (Web Service call), the following authorizations are required for this user in the managed system:

- S\_RFCACL (trusted)
- S\_XMB\_MONI, S\_XMB\_AUTH, S\_XMB\_DSP (PI message handling) with ACTVT 03 (display), 16 (execute), and A3 (read)
- S\_IDOCCTRL (Idoc handling) with ACTVT 10

## 6.2.7.3 Second Level Roles in SAP Solution Manager

The table underneath gives you a further overview, which single roles are included in the composite role.

The views EEM or System Monitoring are visible, because Interactive Reporting can also be called via these views. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

### Authorizations in the Managed System

If the current user is used to logon to managed system via trusted RFC or assertion ticket (Web Service call), the following authorizations are required for this user in the managed system:

- S\_RFCACL (trusted)
- S\_XMB\_MONI, S\_XMB\_AUTH, S\_XMB\_DSP (PI message handling) with ACTVT 03 (display), 16 (execute), and A3 (read)
- S\_IDOCCTRL (Idoc handling) with ACTVT 10

### Second Level User (Help Text ID: TP\_MFM\_L2)

#### Technical composite role name SAP\_MFM\_L2\_COMP in SAP Solution Manager system

Table 114

Single Roles	Help Text ID
SAP_SM_MFM_LEVEL02	AUTH_SAP_SM_MFM_LEVEL02
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARD_ALM
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

#### Technical composite role name: SAP\_SM\_BW\_PIM\_L2\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 115

Single Roles	Help Text ID
SAP_BI_E2E_PIM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Roles in the PI managed system

Table 116

UME role/group	Remarks
SAP_XI_RWB_SERV_USER	Used for adapter engine PING and self-test DC
SAP_XI_RWB_SERV_USER_MAIN	
XI_AF_CHANNEL_ADMIN	Used for channel status DC

## 6.2.7.4 Authorization Objects

### Flow Groups

Authorizations for MFM are based on restricting access to flow groups. A flow group corresponds to a technical scenario.

### SM\_MFM\_FG

This authorization object restricts the display of flow groups for users.

### Payload Display in MFM and PI-Monitoring

#### MFM: SM\_MFM\_PYL

This authorization object controls if the payload information for a flow group is visible or not.

#### Caution

The object is **security-critical** and shipped with status *active* for user L2 for Message Flow Monitoring.

In this context, payload information refers to User Defined Search (UDS) attributes. The business user can decide which values from Payload should also be UDS attributes. These are typically 1-10 attributes from Payload. Therefore, payload in Solution Manager displays the self-defined attributes of Payload. Per default the system does not display any UDS attributes. UDS attributes can only be displayed when the features is activated in the PI-system.

### Central User-Defined Search

In PI-Monitoring, SAP Solution Manager displays the Central User-Defined Search (cUDS). With this function, you can centrally choose a search criteria in Solution Manager, and thus trigger a UDS in your PI-System. The result is displayed in Solution Manager. The user is able to navigate from here into the according PI-system to view the individual messages. The search function itself is started centrally on the SAP Solution Manager. It runs directly on the various selected PI-systems. The RFC-destination used in these cases is Trusted or a logical port for Web Service (Java). This supports the concept that a named user is running the search. The system searches only for the Payload Data previously defined by customizing or set to being sensitive in the individual PI-system. The

search result is not saved within the SAP Solution Manager. Within MFM, UDS attributes are saved nevertheless, but this function is secured by the authorization object.

### PI Message Handling: S\_XMB\*

Authorization objects S\_XMB\_MONI, S\_XMB\_AUTH, and S\_XMB\_DSP are required.

### Idoc Handling: S\_IDOCCTRL

To handle Idocs this authorization object is required with ACTVT 10.

## 6.2.7.5 Function Integration

Within the *Message Flow Monitoring*, you can create Incidents and Notifications. You can also use Guided Procedures. For each integration authorization check the individual function information:

- Incidents: Scenario-specific guide for IT Service Management
- Notification and Guided Procedure: Scenario-specific guide for Technical Administration

## 6.2.7.6 Integration of SAP Fiori Applications

Here, you find specific information on the individually delivered applications that can be used on a central SAP Fiori Hub.

### **i** Note

General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central SAP Fiori Hub, you can find in the *Security Guide for the Authorization Concept* for Solution Manager.

### APP: Message Flow Monitoring (Use Case)

Message Flow Monitoring is used to monitor the flow and view details of each flow instance. The App displays the statistical data of flow instances. Users can do the following:

- display the statistical data at various levels: flow group, flow type and flow instance (SM\_MFM\_FG)
- search for specific flow instances using various attributes
- save the searches for future use
- edit and delete searches
- cancel and restart PI messages

### Authorizations in the Back-End SAP Solution Manager (ST Component)

### **i** Note

As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, assign the relevant composite role `SAP_MFM_LEVEL01_COMP` to the user or create the template user for Level 1 via transaction `SOLMAN_SETUP`. The relevant Odata - Service is delivered per default in the core role for Message Flow Monitoring `SAP_SM_MFM_LEVEL01`.

Due to the nature of the application as a subset of the complete functionality **not all authorizations for the Level 1 user in these roles are required to run the application**. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SM_MFM_LEVEL01` roles accordingly. In this case, remove the following authorization objects:

- `S_TCODE`
- `SM_WC_VIEW`

Modify authorization object `SM_MOAL_TC`: Remove `ACTVT 78` (Assign), `ACTVT PO` (Postpone), and `ACTVT 71` (Create analysis report)

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

### Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- `SAP_STUI_MFMON_TCR`

This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.

- `SAP_STUI_MFMON_AUTH`

This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:

1. Copy the Odata service into your name space.
2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

## 6.2.8 User Roles for End-User Experience Monitoring

### 6.2.8.1 First Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

The view System Monitoring is visible, because `EEM Monitoring` can also be called via this view. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`, and the authorizations for the `URL` framework. For more information about user interface authorizations, see core security guide.

#### First Level User `UXM_L1_XXX` (Help Text ID: `TP_EEM_L1`)

Technical composite role name `SAP_EEM_L1_COMP` in SAP Solution Manager system

Table 117

Single Roles	Help Text ID
SAP_SM_EEM_LEVEL01	AUTH_SAP_SM_EEM_LEVEL01
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_EEM_ROBOT_DIS	AUTH_SAP_SM_EEM_ROBOT_DIS

## 6.2.8.2 Second Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

The view System Monitoring is visible, because EEM Monitoring can also be called via this view. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

### Second Level User UXM\_L2\_XXX (Help Text ID: TP\_EEM\_L2)

Technical composite role SAP\_EEM\_L2\_COMP in SAP Solution Manager system

Table 118

Single Role	Remarks
SAP_SM_EEM_LEVEL02	AUTH_SAP_SM_EEM_LEVEL02
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN

Single Role	Remarks
SAP_SM_DASHBOARDS_DISP_EEM	AUTH_SAP_SM_DASHBOARD_EEM
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARD_ALM
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_EEM_ROBOT_ALL	AUTH_SAP_SM_EEM_ROBOT_ALL

**Technical composite role name: SAP\_SM\_BW\_EEM\_L2\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 119

Single Roles	Help Text ID
SAP_BI_E2E_EEM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### 6.2.8.3 Integration of SAP Fiori Applications

Here, you find specific information on the individually delivered applications that can be used on a central SAP Fiori Hub.

**i Note**

General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central SAP Fiori Hub, you can find in the *Security Guide for the Authorization Concept* for Solution Manager.

**APP: User Experience Monitoring (Use Case)**

This application gives the possibility to list the User Experience (UX) Monitoring scripts with their last execution metrics, availability and performance. From the script list, users have the possibility to drill down to the list of robots running a particular script, then to the list of the last executions for the selected script on the selected robot, and finally to the steps of the selected execution. It also provides a robot oriented view to drill down through a robot perspective from the list of UX Monitoring robots down to the scripts steps.

**Authorizations in the Back-End SAP Solution Manager (ST Component)**

**i Note**

As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.



In the back-end SAP Solution Manager system, assign the relevant composite role `SAP_EEM_LEVEL01_COMP` to the user or create the template user for Level 1 via transaction `SOLMAN_SETUP`. The relevant Odata - Service is delivered per default in the core role for User Experience Monitoring `SAP_SM_EEM_LEVEL01`.

Due to the nature of the application as a subset of the complete functionality **not all authorizations for Level 1 user in these roles are required to run the application**. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SM_EEM_LEVEL01` roles accordingly. In this case, remove the following authorization objects:

- `S_TCODE`
- `SM_WC_VIEW`

Modify authorization object `SM_MOAL_TC`: Remove `ACTVT 78` (Assign), `ACTVT PO` (Postpone), and `ACTVT 71` (Create analysis report)

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

### Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- `SAP_STUI_UXM_TCR`

This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.

- `SAP_STUI_UXM_AUTH`

This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:

1. Copy the Odata service into your name space.
2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

## 6.2.9 User Roles for HANA and Business Intelligence Monitoring

### 6.2.9.1 First Level User Role

The table underneath gives you an overview, which single roles are included in the composite role.

The view System Monitoring is visible, because `BI Monitoring` can also be called via this view. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`, and the authorizations for the `URL` framework. For more information about user interface authorizations, see core security guide.

#### First Level User (Help Text ID: `TP_BIM_L1`)

Technical composite role name `SAP_BIM_L1_COMP` in the SAP Solution Manager system/client

Table 120

Single Roles	HELP Text ID
SAP_SM_BIM_LEVEL01	AUTH_SAP_SM_BIM_LEVEL01
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_CENTRAL_JOB_OVERVIEW	AUTH_SAP_SM_CENTRAL_JOB

## 6.2.9.2 Second Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

The view System Monitoring is visible, because BI Monitoring can also be called via this view. Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

### Second Level User (Help Text ID: TP\_BIM\_L2)

Technical composite role SAP\_BIM\_L2\_COMP in SAP Solution Manager system

Table 121

Single Role	Re
SAP_SM_BIM_LEVEL02	AUTH_SAP_SM_BIM_LEVEL02
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REPOSITORY_DISP
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN

Single Role	Re
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARDS_DISP_ALM
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_CENTRAL_JOB_OVERVIEW	AUTH_SAP_SM_CENTRAL_JOB

**Technical composite role name: SAP\_SM\_BW\_BIM\_L2\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 122

Single Roles	Help Text ID
SAP_BI_E2E_EEM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

## 6.2.9.3 Data Readiness Monitoring

*Data Readiness Monitoring* (DRM) enables the user to determine whether the data is up to date at a special point in time. This is ensured by checking the last successful run in relation to a provided point in time that defines whether all data is considered as ready or not. DRM extends the application HANA and BI Monitoring. Therefore, the authorization concept is same, with the additional access allowance for the DRM service.

## 6.2.10 User Roles for Interface (Channel) Monitoring

### 6.2.10.1 First Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

**First Level User (Help Text ID: IC\_L1\_XXX)**

Technical composite role SAP\_IC\_L1\_COMP in SAP Solution Manager system

Table 123

Single Roles	Help TXT ID
SAP_EM_DISPLAY	AUTH_SAP_EM_DISPLAY
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON

Single Roles	Help TXT ID
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_IC_LEVEL01	AUTH_SAP_SM_IC_LEVEL01
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

**Technical composite role name: SAP\_SM\_BW\_SM\_L2\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 124

Single Roles	Help Text ID
SAP_BI_E2E_SM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

## 6.2.10.2 Second Level User Roles

The table underneath gives you a further overview, which single roles are included in the composite role.

Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

### Second Level User (Help Text ID: IC\_L2\_XXX)

Technical composite role SAP\_IC\_L2\_COMP in SAP Solution Manager system

Table 125

Single Roles	Help TXT ID
SAP_EM_DISPLAY	AUTH_SAP_EM_DISPLAY
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG

Single Roles	Help TXT ID
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARD_ALM
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_IC_LEVEL02	AUTH_SAP_SM_IC_LEVEL01
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SYM_LEVEL01

**Technical composite role name: SAP\_SM\_BW\_SM\_L2\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 126

Single Roles	Help Text ID
SAP_BI_E2E_SM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

## 6.2.11 End-User Roles for Job Monitoring

### 6.2.11.1 First Level User Role

The table underneath gives you an overview, which single roles are included in the composite role.

Access in the navigation panel is restricted by using the authorization object SM\_WC\_VIEW, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

**First Level User (Help Text ID: TP\_JMON\_L1)**

Technical composite role name SAP\_JMON\_L1\_COMP in the SAP Solution Manager system/client

Table 127

Single Roles	HELP Text ID
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE

Single Roles	HELP Text ID
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_CENTRAL_JOB_OVERVIEW	AUTH_SAP_SM_CENTRAL_JOB

## 6.2.11.2 Second Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`, and the authorizations for the URL framework. For more information about user interface authorizations, see core security guide.

### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object `S_RFCACL` (role `SAP_SM_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`). The user in the BW - system is also assigned authorization `S_RFCACL` (role `SAP_SM_BW_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`).

### Second Level User (Help Text ID: TP\_JMON\_L2)

Technical composite role `SAP_JMON_L2_COMP` in SAP Solution Manager system

Table 128

Single Role	Remarks
SAP_SM_JMON_LEVEL02	AUTH_SAP_SM_JMON_LEVEL02
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SYSTEM_REPOSITORY_DISP	AUTH_SAP_SYSTEM_REP_DISP
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARDS_DISP_ALM
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_SCHEDULER_BPO	AUTH_SAP_SM_SCHEDULER_BPO
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Single Role	Remarks
SAP_SM_CENTRAL_JOB_OVERVIEW	AUTH_SAP_SM_CENTRAL_JOB

**Technical composite role name: SAP\_SM\_BW\_JMON\_L2\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 129

Single Roles	Help Text ID
SAP_BI_E2E_JMON	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### 6.2.11.3 Central Applications in Technical Monitoring

#### Central Job Overview

The application *Central Job Overview* is included in Job Monitoring as well as HANA and BI-Monitoring. Therefore, role SAP\_SM\_CENTRAL\_JOB\_OVERVIEW is added to the respective composite roles. In addition, the application can be run stand-alone. If you use the application stand-alone, you need to assign the following roles to your user:

- SAP\_SM\_CENTRAL\_JOB\_OVERVIEW
- SAP\_SM\_RFC\_DISP (specifically authorization object S\_RFC\_ADM)
- SAP\_SYSTEM\_REPOSITORY\_DIS (specifically authorization object AI\_LMDB\_OB)
- SAP\_SMWORK\_TECH\_MON
- SAP\_SM\_FIORI\_LP\_EMBEDDED

#### Alert Inbox

The *Alert Inbox* can be called from any of the sub-scenarios. The main authorization object for this application is SM\_MOAL\_TC.

### 6.2.12 User Roles for Infrastructure Monitoring

To be able to use *IT Infrastructure Management* and *Infrastructure Monitoring* you have to:

1. deploy the required Add-On.
2. check if the following authorization values are contained in the mentioned roles:
  - in role SAP\_SM\_ITMA\_CONF in authorization object SM\_SETUP (value: CMDB\_INF\_MAN)
  - in role SAP\_SM\_ITMO\_CONF in authorization object SM\_SETUP (value: E2E\_MAI\_SETUP5)

Before you are able to configure *Infrastructure Monitoring*, you need to configure *IT Infrastructure Management*.

## 6.2.12.1 First Level User Role

The table underneath gives you a further overview, which single roles are included in the composite role.

### First Level User (Help Text ID: TP\_IT\_L1)

Technical composite role SAP\_IT\_L1\_COMP in SAP Solution Manager system

Table 130

Included Single Roles	Help Text ID
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SYM_LEVEL01
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## 6.2.12.2 Second Level User Role

The table underneath gives you an overview, which single roles are included in the composite role.

### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object S\_RFCACL (role SAP\_SM\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL). The user in the BW - system is also assigned authorization S\_RFCACL (role SAP\_SM\_BW\_S\_RFCACL; Help Text ID: AUTH\_SAP\_S\_SM\_RFCACL).

### Second Level User (Help Text ID: TP\_IT\_L2)

Technical composite role SAP\_IT\_L2\_COMP in SAP Solution Manager system

Table 131

Single Roles	Help Text ID
SAP_SM_SYM_LEVEL02	AUTH_SAP_SM_SYM_LEVEL02
SAP_SMWORK_TECH_MON	AUTH_SAP_SMWORK_TECH_MON
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_SUPPDESK_CREATE



Single Roles	Help Text ID
SAP_SM_DASHBOARDS_DISP_ALM	AUTH_SAP_SM_DASHBOARD_ALM
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

**Technical composite role name: SAP\_SM\_BW\_SM\_L2\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 132

Single Roles	Help Text ID
SAP_BI_E2E_SM	AUTH_SAP_BI_E2E
SAP_SM_BI_DIS	AUTH_SAP_SM_BI_DIS

## 6.2.13 Users and Roles for Exception Management

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for *Exception Management*.

### Configuration

#### Transaction SOLMAN\_SETUP

You can configure the scenario using transaction SOLMAN\_SETUP. When you call the procedure view *Exception Management*, the system asks you to create a specific configuration user. You can create this user SMC\_EXM\_\*\*\*, or you can add the suggested user roles to another user.

#### Configuration User SMC\_EXM\_\*\*\* (Help TXT: USER\_CONFIG\_EM)

##### Single Roles (technical composite role name: SAP\_EM\_CONF\_COMP)

Table 133

Role	Help Text-ID
SAP_EM_CONFIG	AUTH_SAP_EM_CONF
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP_DISP
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## Cockpit User: EXM\_EXE\_<SID> (Help TXT: TP\_EM\_EXE)

Single Roles (technical composite role name: SAP\_EM\_COCKPIT\_COMP)

Table 134

Role	Help Text-ID
SAP_EM_COCKPIT	AUTH_SAP_EM_COCKPIT
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBEDDED

## Display User: SAPSUPPORT

For more information on the user SAPSUPPORT, see Secure Configuration Security Guide.

## Authorization Objects

### SM\_EM

This authorization object restricts the access to Exception Management within the scenario Root Cause Analysis. It is contained in roles SAP\_EM\*, and differentiates between the following activities ACTVT:

- 02 Change Configuration
- 03 Display Configuration, Overview over exceptions
- 27 Display total records payload

## Scenario Integration

- Notification Management
- Incident Management
- Alert Inbox
- Guided Procedure Browser
- EFWK Log Viewer

## 6.2.14 Integration Visibility in Managed Systems

*Integration Visibility* is a technical foundation that discovers message flows and enables consumer applications to subscribe and consume monitoring events for a selected set of discovered message flows in PI. This includes all A2A and B2B in the monitored landscape. It can be used with SAP Solution Manager. Then, Solution Manager is used as User Interface to correlate the data collected from different sources.

## **i** Note

This documentation only describes the necessary roles if you use Integration Validation with SAP Solution Manager. For more information on the scenario and the UME roles for it, see the online documentation for *Integration Visibility* in PI.

## User Roles

In the overall Integration Visibility landscape proposed roles are needed for following positions:

Table 135

Single Role	User Type	Remarks
SAP_IV_DC_SUBSCRIBE	System User	position 3 in the data flow graphic: distribute flow subscriptions and message filter criteria. It is used for subscription and query handling, when request arrives from Subscription Manager.
SAP_IV_EVENT_CONSUMER		position 5 in the data flow graphic: In terms of Solution Manager: Integration Visibility Consumer acts as Managing system
SAP_IV_DC_EXECUTE		It is used to run the data collector, generate, and persist events
SAP_IV_DC_CONFIG	Dialog User	Corresponds to Integration Architect and is used to manage data collector configuration. Users assigned to this role will be able to: <ul style="list-style-type: none"><li>• configure IV Discovery settings and to manage flow definitions</li><li>• navigate to whole "Integration Visibility" User Interface</li><li>• configure Data Collector execution</li></ul>
SAP_IV_DC_SUPPORTER		Corresponds to Technical Supporter. Users assigned to this role, will be able to: <ul style="list-style-type: none"><li>• read data from all Integration Visibility tables in NWA Open SQL Data Browser (without BC_IV_DC_EVENT – contains business sensitive information)</li><li>• navigate to whole "Integration Visibility" User Interface with read-only rights</li><li>• have full access to: WS Navigator/ Log Viewer/Log Configurator/ WS Log Viewer/ WS Log Configurator/ GET operations from all IV web services</li></ul>
SAP_IV_DC_ADMIN		Composite role. Includes: <ul style="list-style-type: none"><li>• SAP_IV_DC_SUBSCRIBE</li><li>• SAP_IV_DC_EXECUTE</li><li>• SAP_IV_EVENT_CONSUMER</li><li>• SAP_IV_DC_CONFIG</li></ul>

## 6.2.15 Role for Technical Monitoring Display

For display usage of Technical Monitoring, composite role `SAP_TECHMON_DISPLAY_COMP` is delivered. The role contains authorization for displaying the complete technical monitoring applications.

## 6.2.16 Role for Technical Monitoring Support

For the support of Technical Monitoring, the single role `SAP_SM_TECH_MON_TOOL` is delivered. The role contains authorization object `SM_SP_TOOL` for access to various support tools.

## 6.2.17 Main Authorization Objects

The following section describes the main authorization object for Technical Monitoring. For more detail, see the SDN Wiki on Authorizations.

### Authorization Object `SM_MOAL_TC`

This authorization object defines on the application level which contexts the user is allowed to work in, for instance *Problem Context Configuration* should be possible for Level 2 and configuration users.

The authorizations for the object are maintained differently for all user roles for the Technical Monitoring sub-scenarios. For instance, activity 02 (change) allows for start, stop, ping (button: *Manage*) in Channel Monitoring for configuration user, and Level 2 user in PI Monitoring roles.

### Authorization Object `SM_MOAL_OC`

This authorization object controls whether a user is allowed to create, delete, display, change, copy, generate, activate, and deactivate objects relevant in the Business Process Operations. It is used in:

- Job Monitoring
- Business Process Operations
- HANA and BI - Monitoring

### Authorization Object `SM_SETUP`

This authorization object restricts the access to the configuration for the technical monitoring scenario. Only the configuration users are allowed to access this transaction.

In this case, the configuration user is allowed to access the edit mode for the setup of technical monitoring data.

### Authorization Object `S_TRANSPRT`

Authorization object `S_TRANSPRT` is only relevant and maintained in the configuration user roles for the scenarios as the configuration application requests creating, changing, releasing a transport and request.

### Authorization Object `SM_CMDB_OB`

The authorization object is relevant for Infrastructure Monitoring.

## Content Delivery Synchronization: CSU\_\*

### CSU\_PACK

This object controls if the user is allowed to create and maintain registration details, as well as create content packages and maintain content packages related information. *Change* authorization refers to the following activities:

- Create a new Delivery Package type in Content Delivery tool.
- Edit Delivery Package related information like Service Marketplace Place Link, Notification Status type in Content Delivery tool.
- Download a "local" Delivery Package.
- Send Notification to the SAP Backend on the availability of a new content package.
- Create or register a new content type in Content Delivery tool.
- Edit and delete a content type related detail in Content Delivery tool.

### CSU\_UNPACK

This object controls if the user is allowed to download and install content packages on SAP Solution Manager. *Change* authorization refers to the following activities:

- Maintain configuration details like Service Market Place user information, SAP Backend user information, frequency to check for content updates and the user to be notified.
- Download content package from Service Market Place into local store.
- Install content in case of framework delivery type.

## Table Authorization: S\_TABU\_DIS

The following authorization groups are relevant:

- SMAL : Monitoring and Alerting, Self-Diagnosis
- SRCD : Rapid Content Delivery

## UXM Authorization: AI\_EEM

ACTVT : DL allows upload of UXM scripts on the robots.

## 6.2.18 Background Jobs

The following background jobs run:

- SAP\_ALERT\_CALCULATION\_ENGINE
- SAP\_ALERT\_HOUSEKEEPING
- SAP\_METRIC\_STORE\_CLEANUP

All jobs run with system user SOLMAN\_BTC.

Details on the jobs can be found in work center Solution Manager Administration in view Self-Monitoring (Description).

## 6.3 Scenario-Specific Guide: Business Process Operations

### 6.3.1 Getting Started

**What is this guide about?** SAP Solution Manager covers a wide range of diverse scenarios you can use. As a customer, you might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides per scenario which cover all relevant information for this specific scenario.

#### Caution

Before you start using this scenario-specific guide, you must read the core information about security issues in SAP Solution Manager, and the *Landscape Setup Guide*, which refers to all security-relevant information during basic configuration of SAP Solution Manager. Without this information, we do not recommend to set up any specific scenario. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

This guide covers the following topics:

- **Getting Started:** find out about target groups of this guide. Links for any additional components can be found in the Core Guide.
- **Prerequisites:** find out about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other.
- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).
- **User Roles for Additional Functions:** find out about additional authorization for the work center.
- **Scenario Integration:** according to the life-cycle approach the various scenarios integrate with each other. Here, you can find out about authorizations you need to assign to your users for these cases.

### 6.3.2 Prerequisites

#### 6.3.2.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete business process operations scenario. The SAP Solution Manager is connected via `TMW - RFC`, and `TRUSTED - RFC` to your managed systems. `IGS` is connected via a specified `RFC` connection. In addition, a local `RFC` destination is in place from your productive client to the `000` client. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

## Technical Infrastructure

- Business Process Operations

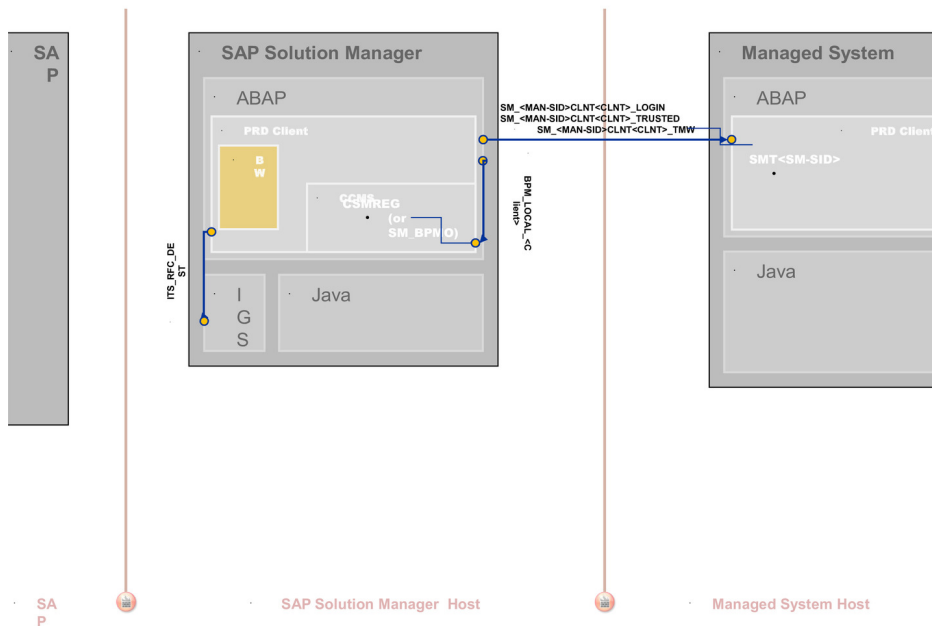


Figure 7: Infrastructure

### 6.3.2.2 Scenario Configuration User

The scenario *BPO* is configured using transaction `SOLMAN_SETUP`.

To configure the scenario proceed as follows:

#### Creating Configuration User in Basic Configuration Transaction `SOLMAN_SETUP`

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic functions.

During basic automated configuration, you can create a specific configuration user (default technical user name: `SMC_BPO_<XXXXClient>` for *BPO* (Help Text ID: `USER_CONFIG_BPO`). The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

Table 136

Single Roles	Help Text ID
SAP_CDC_ADMIN	AUTH_SAP_CDC_ADMIN
SAP_SOLMAN_DIRECTORY_EDIT	AUTH_SAP_SOLMAN_DIRECTORY
SAP_BPO_CONFIG	AUTH_SAP_BPO_CONFIG
SAP_SM_SOLUTION_ALL	AUTH_SAP_SM_SOLUTION_ALL
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL

Single Roles	Help Text ID
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_BPOANA_ALL	AUTH_SAP_SM_BPOANA_ALL
SAP_OP_DSWP_BPM_DIS	AUTH_SAP_OP_DSWP_BPM_DIS
SAP_SMWORK_BPO	AUTH_SAP_SMWORK_BPO
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBEDDED
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP

If you want to create the configuration user manually, you need to assign:

- the composite role `SAP_BPO_CONF_COMP` which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

### **i** Note

To be able to:

- create users and assign user roles, you need to assign as well role `SAP_SM_USER_ADMIN`.
- use a trusted RFC connection between the Solution Manager and the managed systems, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system as well as the managed system.

- the composite role `SAP_BW_BP_OPERATION_ADMIN_COMP` which contains all single roles that are automatically assigned to the configuration user in the BW-system.

### **i** Note

To be able to use a trusted RFC connection between the Solution Manager and the BW-system, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system and role `SAP_SM_BW_S_RFCACL` in the BW-system.

## Scenario Configuration Transaction `SOLMAN_SETUP`

To run Business Process Operations, you need to configure it using transaction `SOLMAN_SETUP`.

During the specific guided configuration you can create Standard template users. The system automatically adds all relevant user roles, see according sections on [Users and User Roles](#).



## 6.3.2.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 137

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems	RFC	Exchange data
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 138

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	Customer-specific	Customer-specific	to be used instead of trusted RFC
SM_<SID>CLNT<Client>_TMW (ABAP connection)	Managed System	System-specific	System-specific	Default user: SMT<SID> of Solution Manager system>	Used to read data from the managed systems such as job lists, sales organization data, IDocs, selection help, and so on, and run batch jobs

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
					<p><b>i Note</b></p> <p>Specific data collectors write log information and details list information into table /SSA/PTAB in the managed system.</p> <p>Batch Jobs BPM_DATA_COLLECTION_1 and BPM_DATA_COLLECTION_2 are scheduled in the managed systems. The jobs allow an asynchronous execution of the data collectors in a managed system. Instead of executing the data collection in a synchronous call from the SAP Solution Manager, the task to execute the data collectors is given to a background job. The result of the data collection is buffered in a dedicated persistency on the managed system. In another step these results are fetched to the SAP Solution Manager system and removed from the database of the managed system. The asynchronous data collection is recommended for unfrequent long lasting data collections.</p> <p>Data collection for monitoring objects that are scheduled to be collected asynchronously will not work. This may result in problems for lasting data collections.</p>
SM_<SID>CLNT<Client>_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific	<ul style="list-style-type: none"> <li>• Mandatory for CDC functionality setup, due to necessity of code generation in managed system;</li> <li>• Mandatory for Business Process Monitoring to use according value help from</li> </ul>

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
					managed systems. Login RFC can be used instead, but then the value help must be maintained manually.

### Internet Graphics Server (IGS) RFC Connection

Table 139

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

### Local Connections

Table 140

Destination Name	Target Host Name	System Number	Log on Client	Logon User (Password)	Remarks
BPM_LOCAL_<Client>	Managing system	System-specific	000	SM_BPMO(customer-specific)	RFC is created during Business Process Operations setup session.

### BW- Reporting RFC Connection

Table 141

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	
BI_CLNT<BWclient>, if BW is realized in remote BW - scenario system, for content activation	Managed System or Solution Manager System	System-specific	System-specific		in transaction SOLMAN_SETUP
<SolutionManagerSID>CLNT<SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client	System-specific	System-specific	BI_CALLBACK (customer-specific)	in transaction SOLMAN_SETUP

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
Trusted RFC to remote BW system SAP_BILO	remote BW - system (source: SAP Solution Manager)	System-specific	System-specific	Dialog User	Used to read data from remote BW for BI - Reporting, created during SOLMAN_SETUP

### 6.3.2.4 Technical Users

The technical users in the following tables are created manually during configuration. All technical users are of type *System User*, except for user SM\_BPMO (Service User). For more information on individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

#### User in Managed Systems

Table 142

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>

#### User in Solution Manager System

Table 143

User Name	User ID
<i>BPMO - User</i>	SM_BPMO; Assigned role SAP_SM_BPMO_COMP

### 6.3.3 Scenario Integration

*Business Process Operation* refers to the phase in your product life-cycle when you define and refine your business processes by means of projects, business blueprints and related activities. According to the end-to-end business process life-cycle, this phase needs to integrate with a number of other functions which come into play in your daily business, such as handling of problems and so on:

- CDC
- BP-Analytics (including BP-Improvement)
- BP-Reporting
- BP-Monitoring

The following sections describe the integration of business process operations with other scenarios within SAP Solution Manager, and which user roles would be applicable.

## **i** Note

For more detail on each individual scenario, see the according *Scenario-Specific Guide*.

### **Incident Management**

Users can create Incident messages. To be able to do so, you need to assign user role `SAP_SUPPDESK_CREATE`.

### **Job Monitoring**

Users can monitor jobs. To be able to do so, you need to assign user role `SAP_SM_JMON_*`..

### **System Monitoring**

Users can monitor jobs. To be able to do so, you need to assign user role `SAP_SM_SYM_*`..

### **Job Scheduling**

For more information, see scenario - specific guide for Job Scheduling Management.

## **6.3.4 Users and Authorizations**

### **6.3.4.1 User Roles**

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for business process operations. All users are assigned a composite role, which contains a number of single roles.

#### **Work Center**

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information about User Interface authorizations, see *Authorization Concept Guide*.

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

#### **Authorization for Trusted RFCs between SAP Solution Manager, Managed Systems, and BW - System**

Trusted authorizations are needed between SAP Solution Manager and its managed systems, as well as SAP Solution Manager and a remote BW - system.

- In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object `S_RFCACL` (role `SAP_SM_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`). The user in the BW - system is also assigned authorization `S_RFCACL` (role `SAP_SM_BW_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`).
- The user in the managed system receives role `SAP_SM_S_RFCACL` (Help Text ID: `AUTH_SAP_S_SM_RFCACL`) with authorization object `S_RFCACL`.

Both roles are not contained in the respective composite roles, due to their highly security-relevant character.

## Authorization in Managed System

In the managed system, you need to assign the according user application-specific authorizations. For more information, see the applicable security guide for the relevant application.

### Administrator/Manager User (Help Text ID: TP\_BPO\_ADMIN)

Technical composite role name: SAP\_BP\_OPERATIONS\_ADMIN\_COMP in the SAP Solution Manager system

Table 144

Single Roles	Help Text ID
SAP_BC_FDT_ADMINISTRATOR	This role gives access to the <i>BRFplus Workbench</i> which is the User interface for creating rule objects (like expressions or data objects) for modeling and testing. The Business Rule Framework plus (BRFplus) is an ABAP-based business rules modeling system that can be used by all applications that are built upon the Netweaver ABAP stack.
SAP_SM_GP_ADMIN	AUTH_SAP_SM_GP_ADMIN
SAP_OP_DSWP_BPM	AUTH_SAP_OP_DSWP_BPM
SAP_SETUP_DSWP_BPM	AUTH_SAP_SETUP_DSWP_BPM
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORT
SAP_SM_BPOANA_ALL	AUTH_SAP_SM_BPOANA_ALL
SAP_SMWORk_BPO	AUTH_SAP_SMWORk_BPO
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SYM_LEVEL01
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SM_SCHEDULER_BPO	AUTH_SAP_SM_SCHEDULER_BPO
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SM_IC_LEVEL02	AUTH_SAP_SM_IC_LEVEL02
SAP_CDC_OBJECT_MODELER	AUTH_SAP_CDC_INSTANCE
SAP_CDC_INSTANCE_CREATOR	AUTH_SAP_CDC_INSTANCE

Single Roles	Help Text ID
SAP_CDC_INSTANCE_EXECUTER	AUTH_SAP_CDC_INSTANCE
SAP_CDC_INSTANCE_ANALYZER	AUTH_SAP_CDC_INSTANCE

### **i** Note

The scenarios Business Process Monitoring, Job Monitoring, and Interface Channel Monitoring are integrated in their monitoring application. Native Job Monitoring applications and Interface Channel Monitoring applications can be called for a set of objects and referenced to a business process or business process step. Therefore, the according core roles for Job Monitoring and Interface Channel Monitoring are assigned per default.

### **Technical composite role name: SAP\_BW\_BP\_OPERATIONS\_ADMIN\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same *User ID* in the BW system. For more information on BW user concept, see section on BW configuration in section *Prerequisites*.

Table 145

Single Roles	Help Text ID
SAP_BI_E2E_BPO	AUTH_SAP_BI_E2E
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

### **i** Note

For more information on *Process Chain Monitoring* of an external BW system, see SAP Note [1411885](#).

### **Role in the Managed System**

The role must be assigned to the user with the same *User ID* in the managed system.

Table 146

Assigned Role	Help Text-ID
SAP_MANAGED_BPOANA_ALL	AUTH_SAP_MANAGED_BPOANA_ALL

### **Analytics/Reporting User (Help Text ID: USER\_TP\_BPO\_REP)**

### **Technical composite role name: SAP\_BP\_OPERATIONS\_REPORT\_COMP in the SAP Solution Manager system**

Table 147

Single Roles	Help Text ID
SAP_SM_GP_EXE	AUTH_SAP_SM_GP_EXE
SAP_OP_DSWP_BPM	AUTH_SAP_OP_DSWP_BPM
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_BPOANA_DIS	AUTH_SAP_SM_BPOANA_DISP
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORT
SAP_SMWORK_BPO	AUTH_SAP_SMWORK_BPO

Single Roles	Help Text ID
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

**Technical composite role name: SAP\_BW\_BP\_OPERATIONS\_ADMIN\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same *User ID* in the BW system. For more information on BW user concept, see section on BW configuration in section *Prerequisites*.

Table 148

Single Roles	Help Text ID
SAP_BI_E2E_BPO	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Note

For more information on *Process Chain Monitoring* of an external BW system, see SAP Note [1411885](#).

### Role in the Managed System

The role must be assigned to the user with the same *User ID* in the managed system.

Table 149

Assigned Role	Help Text-ID
SAP_MANAGED_BPOANA_DISP	AUTH_SAP_MANAGED_BPOANA_DISP

### Alert User (Help Text ID: USER\_TP\_BPO\_ALERT)

**Technical composite role name: SAP\_BP\_OPERATIONS\_ALERT\_COMP in the SAP Solution Manager system**

Table 150

Single Roles	Remarks
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SYM_LEVEL01
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SM_GP_EXE	AUTH_SAP_SM_GP_EXE
SAP_OP_DSWP_BPM	AUTH_SAP_OP_DSWP_BPM
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_BPO	AUTH_SAP_SMWORK_BPO
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE



Single Roles	Remarks
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORT
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_IC_LEVEL02	AUTH_SAP_SM_IC_LEVEL02

### **i** Note

The scenarios Business Process Monitoring, Job Monitoring, and Interface Channel Monitoring are integrated in their monitoring application. Native Job Monitoring applications and Interface Channel Monitoring applications can be called for a set of objects and referenced to a business process or business process step. Therefore, the according core roles for Job Monitoring and for Interface Channel Monitoring are assigned per default.

## **CDC User (Help Text ID: USER\_TP\_BPO\_CDC)**

**Technical composite role name: SAP\_BP\_OPERATIONS\_CDC\_COMP) in the SAP Solution Manager system**

Table 151

Single Roles	Remarks
SAP_CDC_DISPLAY	AUTH_SAP_CDC_DISPLAY
SAP_SM_GP_EXE	AUTH_SAP_SM_GP_EXE
SAP_OP_DSWP_BPM	AUTH_SAP_OP_DSWP_BPM
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_BPO	AUTH_SAP_SMWORK_BPO
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT

## **Display User (technical role name: SAP\_BP\_OPERATIONS\_DIS\_COMP)**

Table 152

Single Roles	Remarks
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SYM_LEVEL01
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SM_GP_DIS	AUTH_SAP_SM_GP_DIS

Single Roles	Remarks
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_BPOANA_DIS	AUTH_SAP_SM_BPOANA_DISP
SAP_SMWORK_BPO	AUTH_SAP_SMWORK_BPO
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

## Project-Based Delivery

To be able to use the function of project-based delivery, the following roles must be added additionally to the according user:

- SAP\_BPR\_PPM (SAP NWBC navigation role, does not need to be copied into customer name space)
- SAP\_CPR\_PROJECT\_ADMINISTRATOR
- SAP\_CPR\_USER
- SAP\_XRPM\_ADMINISTRATOR

### Note

Check as well SAP Note [1346050](#) .

## Main Authorization Objects

### SM\_MOAL\_OC

This authorization object restricts access to configuration of Monitoring Objects, divided by application:

- Business Process Operations
- Job Monitoring
- IC Monitoring

The object is contained in BPO role SAP\_SETUP\_DSWP\_BPM, Job Monitoring roles, and Interface Channel Monitoring roles.

### SM\_MOAL\_TC

This authorization object restricts access to call Monitoring Objects, divided by application:

- Business Process Operations
- Job Monitoring
- IC Monitoring

The object is contained in BPO role SAP\_SETUP\_DSWP\_BPM, Job Monitoring roles, and Interface Channel Monitoring roles. If you require change authorization (ACTVT 02) for IC Monitoring or Job Monitoring, you need to add it manually.

### SM\_OCC\_REP

This authorization object restricts the transparency of user names (transparency) in reporting for OCC Alerts. In OCC Alert Reporting, you can report on the number of alerts per Processor or Confirmer. The user data are

security - sensitive. As per default, the user information is therefore anonymous. The authorization object is contained in an inactive version in role `SAP_SM_BPMON_REPORTING`. In case the user should be made visible within the report, the object must be activated in the role by your Administrator.

## 6.3.5 User Roles for Additional Functions

### 6.3.5.1 End-User Roles for CDC

You can use these additional CDC authorization roles, which allow:

- better segregation of duties by supporting different CDC tasks
- each role has full authorization to create/change the respective task, but display-only authorization in the other areas
- no need to change the existing authorization objects `SM_CDC_OBJ` and `SM_CDC_INS`
- `SAP_CDC_INSTANCE_ANALYZER` for result analysis
- `SAP_CDC_INSTANCE_EXECUTER` for scheduling
- `SAP_CDC_INSTANCE_CREATOR` for administration
- `SAP_CDC_OBJECT_MODELER` for development

New Role	Authorization object SM_CDC_OBJ "CDC: Comparison Object"	Authorization object SM_CDC_INS "CDC: Comparison Instance"
<b>SAP_CDC_OBJECT_MODELER</b> "Cross-Database Comparison (Object Modeler)"	01 Create or generate 02 Change 03 Display 06 Delete 07 Activate, generate	03 Display
<b>SAP_CDC_INSTANCE_CREATOR</b> "Cross-Database Comparison (Instance Creator)"	03 Display 36 Extended maintenance	01 Create or generate 02 Change 03 Display 06 Delete
<b>SAP_CDC_INSTANCE_EXECUTER</b> "Cross-Database Comparison (Instance Executer)"	03 Display	03 Display 16 Execute 65 Reorganize
<b>SAP_CDC_INSTANCE_ANALYZER</b> "Cross-Database Comparison (Instance Analyzer)"	03 Display	03 Display 35 Output

Figure 8: CDC - Authorizations Overview

### 6.3.5.2 Business Process Improvement

The Business Process Analytics *Improvement* Application is the enhanced version of the Business Process Analytics Application. Users can select a key figure from a list of all available Application Monitors of a managed system via the KPI-Cloud catalogues, and execute it directly.

#### Data Flow

1. Analytics Application is started by the user via Browser information (Fiori Launchpad Tile access)
2. Key figure is selected by the user.
3. Data retrieval is executed by the system and displayed on the screen.
4. Analysis functions can be executed on data by the user.

## User Roles

The following roles are required in addition to the general BPO roles.

- Administrator User: `SAP_SM_BPOIMP_ALL`
- Analytics User: `SAP_SM_BPOIMP_EDIT`
- Display User: `SAP_SM_BPOIMP_DIS`

Access to Fiori Launchpad is granted by roles `SAP_SMWORK_BPO` (groups and catalogue) and `SAP_SM_FIORI_LP_EMBEDDED` (relevant UI authorizations).

## Main Authorization Objects

### SM\_BPA\_OBJ

The object restricts access to specific tile information (BPA objects).

### SM\_BPA\_KYF

#### Caution

Key Figures are highly security - critical.

This object restricts the access to key figures. You can organize the access to key figure data in different levels for each system/client combination:

- Key Figure Groups: Key figures are collected by the system in customer-specified Key Figure Groups (defined via Application Area, Business Goals, Processes).
- Authorization Groups: All key figures contain specific characteristics with a Semantic-ID as identifier.

## 6.4 Scenario-Specific Guide: Job Management

### 6.4.1 Prerequisites

#### 6.4.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete Job Management scenario. The SAP Solution Manager is connected via `READ - RFC` to your managed systems. `IGS` is connected via a specified `RFC` connection. Optionally, you can attach a third party product such as `SAP CPS` to the SAP Solution Manager via specified connections. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

Technical Infrastructure  
 • Job Management

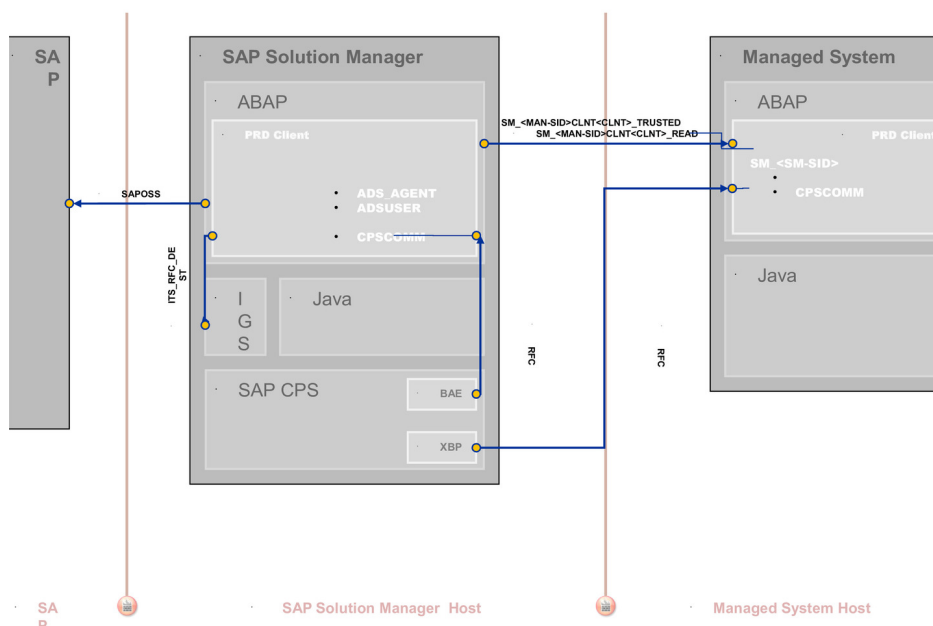


Figure 9: Infrastructure

## 6.4.1.2 Scenario Configuration User

**i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see *Authorization Concept Guide* chapter *Configuration Users*.
- the BW integration concept, see *Authorization Concept Guide* chapter on *BW Integration*.

The scenario is configured using transaction SOLMAN\_SETUP.

To configure the scenario proceed as follows:

### Creating Configuration User (Transaction SOLMAN\_SETUP)

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic function to send an Incident message to SAP. For more information, see *Secure Configuration Guide*.

When you configure your scenario using basic automated configuration, the system asks you to create a specific configuration user (default technical user name: SMC\_JMON\_<XXXClient>) for Job Management (Help Text ID: USER\_CONFIG\_JMON) when you call the configuration procedure. This user is a dialog user. The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

Table 153

Single Roles	Help Text ID
SAP_SM_SCHEDULER_CONFIG	AUTH_SAP_SM_SCHEDULER_CONFIG
SAP_SM_JMON_CONF	AUTH_SAP_SM_JMON_CONF
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_SOLMANPRO_ADMIN
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_SOLMANPRO_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_SOLMANPRO_CHARM
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP

You have different possibilities of creating configuration users for configuration purposes:

- Use default user SMC\_\*\*\*: Create the default user via pop-up.
- Use user SOLMAN\_ADMIN and add additional user roles: Enter user ID for user SOLMAN\_ADMIN in the pop-up and assign the roles.
- Do not use default user, create your own configuration user in transaction SU01: Set the flag for *Manual Maintenance* in the SOLMAN\_SETUP pop-up, and create your user in transaction SU01.

### ➔ Recommendation

If you want to create the configuration user manually, we recommend to assign:

- the composite role SAP\_JOBMAN\_CONF\_COMP which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

### **i** Note

To be able to:

- create users and assign user roles, you need to assign as well role SAP\_SM\_USER\_ADMIN.

- use a trusted RFC connection between the Solution Manager and the managed systems, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system as well as the managed system.
- the composite role `SAP_BW_JOBMAN_ADMIN_COMP` which contains all single roles that are automatically assigned to the configuration user in the BW-system.

### **i** Note

To be able to use a trusted RFC connection between the Solution Manager and the BW-system, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system and role `SAP_SM_BW_S_RFCACL` in the BW-system.

## 6.4.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 154

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems	RFC	Reading information from managed systems
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes
SAP CPS	RFC	See SAP Note <a href="#">1037903</a>

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

### **i** Note

All mentioned RFC - destinations are automatically created via transaction SOLMAN\_SETUP (view: managed systems), see *Secure Configuration Guide*.

Table 155

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	Necessary for all functions in implementation and upgrade

### Internet Graphics Server (IGS) RFC Connection

Table 156

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

## 6.4.1.4 Technical User

The technical users in the following tables are created automatically or manually during configuration. All technical users are of type *System User*, except for user CPSCOMM (Communication User). For more information on individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

### User in Managed Systems

Table 157

User Name	User ID
<i>Read - User</i>	SM_<SID> of Solution Manager system>

### User in SAP Solution Manager System

Table 158

User Name	User ID
CPS user	CPSCOMM

**i** Note

for communication between SAP CPS and SAP Solution Manager, assigned roles SAP\_SM\_REDWOOD\_COMMUNICATION and SAP\_BC\_REDWOOD\_COMM\_EXT\_SDL



## 6.4.2 Scenario Integration

The following sections describe the integration of *Job Scheduling Management* with other scenarios within SAP Solution Manager, and which user roles would be applicable.

### Incident Management

You can integrate *Incident Management* with Job Scheduling by configuring the Integration for IT Service Management (Incident Management) in transaction `SOLMAN_SETUP`.

### Change Request Management

You can integrate *Change Request Management* with Job Scheduling by configuring the Integration with Change Request Management scenario in transaction `SOLMAN_SETUP`.

### Business Process Operations

You can integrate Business Process Operations with Job Scheduling.

### IT Task Inbox

You can integrate IT Task Inbox.

## 6.4.3 Users and Authorizations

### 6.4.3.1 User Roles

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for *Job Scheduling*. You can create Template users in transaction `SOLMAN_SETUP`. In analogy, composite roles exist which contain a number of single roles.

#### Administrator (Technical User Name: `JM_ADM_XXX`)

The technical name of the according composite role is `SAP_JOBMAN_ALL_COMP`.

Table 159

Single Role	Help Text ID
<code>SAP_BC_BATCH_ADMIN_REDWOOD</code>	<code>AUTH_SAP_BC_REDWOOD</code>
<code>SAP_BC_REDWOOD_COMM_EXT_SDL</code>	<code>AUTH_SAP_BC_REDWOOD</code>
<b>i</b> Note Both roles are only needed for managing external schedulers.	
<code>SAP_SM_BPMON_REPORTING</code>	<code>AUTH_SAP_SM_BPMON_REPORTING</code>
<code>SAP_CM_SMAN_CHANGE_MANAGER</code>	<code>AUTH_SAP_CM_SMAN_CHANGE_MANAGER</code>
<code>SAP_CM_SMAN_DEVELOPER</code>	<code>AUTH_SAP_CM_SMAN_DEVELOPER</code>

Single Role	Help Text ID
SAP_SOCM_CHANGE_MANAGER	AUTH_SAP_SOCM_CHANGE_MANAGER
SAP_SOCM_DEVELOPER	AUTH_SAP_SOCM_DEVELOPER
SAP_SM_SCHEDULER_ADMIN	AUTH_SAP_SM_SCHED_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SM_JMON_LEVEL02	AUTH_SAP_SM_JMON_LEVEL02
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
<p><b>i Note</b> The administration user receives role SAP_SM_RFC_ADMIN due to administration tasks. If this is not required, assign SAP_SM_RFC_DISP instead.</p>	
SAP_SUPPDESK_PROCESS	AUTH_SAP_SUPPDESK_PROCESS
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_SOCM_REQUESTER	AUTH_SAP_SOCM_REQUESTER
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### In the BW - System

The technical name of the according composite role is SAP\_SM\_BW\_JSCHED\_ADMIN\_COMP.

Table 160


Single Role	Help Text ID
SAP_BI_E2E_JSM	AUTH_SAP_BI_E2E
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

### Technical Operator (Technical User Name: JM\_TOP\_XXX)

The technical name of the according composite role is SAP\_JOBMAN\_TOP\_COMP.

Table 161

Single Role	Help Text ID
SAP_BC_BATCH_ADMIN_REDWOOD	AUTH_SAP_BC_REDWOOD

Single Role	Help Text ID
SAP_BC_REDWOOD_COMM_EXT_SDL	AUTH_SAP_BC_REDWOOD
 <b>Note</b> Both roles are only needed for managing external schedulers.	
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING
SAP_CM_SMAN_DEVELOPER	AUTH_SAP_CM_SMAN_DEVELOPER
SAP_SOCCM_DEVELOPER	AUTH_SAP_SOCCM_DEVELOPER
SAP_SM_SCHEDULER_TOP	AUTH_SAP_SM_SCHED_TOP
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SM_RFC_DISP	AUTH_SAP_SM_RFC_DISP
SAP_SUPPDESK_PROCESS	AUTH_SAP_SUPPDESK_PROCESS
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### In the BW - System

The technical name of the according composite role is SAP\_SM\_BW\_JSCHED\_DIS\_COMP.

Table 162

Single Role	Help Text ID
SAP_BI_E2E_JSM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Business Process Operation (Technical User Name: JM\_BPO\_XXX)

#### In the Solution Manager

The technical name of the according composite role is SAP\_JOBMAN\_BPO\_COMP.

Table 163

Single Role	Help Text ID
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING

Single Role	Help Text ID
SAP_CM_SMAN_CHANGE_MANAGER	AUTH_SAP_CM_SMAN_CHANGE_MANAGER
SAP_SOCM_CHANGE_MANAGER	AUTH_SAP_SOCM_CHANGE_MANAGER
SAP_SM_SCHEDULER_BPO	AUTH_SAP_SM_SCHED_BPO
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SM_RFC_DISP	AUTH_SAP_SM_RFC_DISP
SAP_SUPPDESK_PROCESS	AUTH_SAP_SUPPDESK_PROCESS
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### In the BW - System

The technical name of the according composite role is SAP\_SM\_BW\_JSCHED\_DIS\_COMP.

Table 164

Single Role	Help Text ID
SAP_BI_E2E_JSM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Application Manager (technical user name: JM\_AM\_XXX)

#### In the Solution Manager

The technical name of the according composite role is SAP\_JOBMAN\_AM\_COMP.

Table 165

Single Role	Help Text ID
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING
SAP_SOCM_REQUESTER	AUTH_SAP_SOCM_REQUESTER
SAP_SM_SCHEDULER_AM	AUTH_SAP_SM_SCHED_AM
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL

Single Role	Help Text ID
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SM_JMON_LEVEL02	AUTH_SAP_SM_JMON_LEVEL02
SAP_SM_RFC_DISP	AUTH_SAP_SM_RFC_DISP
SAP_SUPPDESK_DISPLAY	AUTH_SAP_SUPPDESK_DISPLAY
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### In the BW - System

The technical name of the according composite role is `SAP_SM_BW_JSCHED_DIS_COMP`.

Table 166

Single Role	Help Text ID
SAP_BI_E2E_JSM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Level 2 User (Technical User Name: JM\_L2\_XXX )

The technical name of the according composite role is `SAP_JOBMAN_L2_COMP`.

Table 167

Single Role	Help Text ID
SAP_SOCM_REQUESTER	AUTH_SAP_SOCM_REQUESTER
SAP_SM_SCHEDULER_L2	AUTH_SAP_SM_SCHED_L2
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REPOSIORY_DIS
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SM_RFC_DISP	AUTH_SAP_SM_RFC_DISP

Single Role	Help Text ID
SAP_SUPPDESK_PROCESS	AUTH_SAP_SUPPDESK_PROCESS
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Level 1 User (Technical User Name: JM\_L1\_XXX)

The technical name of the according composite role is SAP\_JOBMAN\_L1\_COMP.

Table 168

Single Role	Help Text ID
SAP_SOCM_REQUESTER	AUTH_SAP_SOCM_REQUESTER
SAP_SM_SCHEDULER_L1	AUTH_SAP_SM_SCHED_L1
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REPOSITORY_DIS
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SM_RFC_DISP	AUTH_SAP_SM_RFC_DISP
SAP_SUPPDESK_PROCESS	AUTH_SAP_SUPPDESK_PROCESS
SAP_TASK_INBOX_ALL	AUTH_SAP_TASK_INBOX_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Display User (Technical User Name: JM\_DIS\_XXX)

#### In the Solution Manager

The technical name of the according composite role is SAP\_JOBMAN\_DIS\_COMP.

Table 169

Single Role	Help Text ID
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING
SAP_SOCM_REQUESTER	AUTH_SAP_SOCM_REQUESTER
SAP_SM_SCHEDULER_DIS	AUTH_SAP_SM_SCHED_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_JOB_MAN	AUTH_SAP_SMWORK_JOB_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAMEWORK

Single Role	Help Text ID
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMANPRO
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SUPPDESK_DISPLAY	AUTH_SAP_SUPPDESK_DISPLAY
SAP_TASK_INBOX_DIS	AUTH_SAP_TASK_INBOX_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### In the BW - System

The technical name of the according composite role is SAP\_SM\_BW\_JSCHED\_DIS\_COMP.

Table 170

Single Role	Help Text ID
SAP_BI_E2E_JSM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

## 6.4.4 CRM Standard Customizing for Solution Manager

The *Job Scheduling Management* scenario is partly based on CRM customizing for *Transaction Types*, *Action Profiles*, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects. The following table gives you an overview of the *Transaction Types* used.

### Caution

If you copy SAP standard customizing, you need to add the changed values in the according CRM - authorization objects for the scenario. See also *How-to Guide* on how to maintain authorization objects.

### Transaction Type

Table 171

Transaction Type	Usage	Remarks
SLFJ	Job Scheduling Management	supported

### Authorization Objects

You need to maintain the following authorization objects:

- CRM\_ORD\_OP
- CRM\_ORD\_PR
- B\_USERSTAT

## 6.4.5 External Integration

### 6.4.5.1 SAP Central Process Scheduler (SAP CPS)

You can integrate with SAP Solution Manager external products. The term *External Product* refers to either Third Party Products or SAP products, which can be used to complement a function within SAP Solution Manager. Using SAP CPS, you assign your end-user the user roles as described in the previous section *User Roles*. The technical user needs to be assigned the roles as described in the table underneath.

#### Roles for Technical User CPSCOMM

Table 172

Name	Type	Remarks
SAP_SM_REDWOOD_COMMUNICATION	ABAP	General authorization for the technical communication user (for instance) CPSCOMM between Solution Manager and SAP Central Process Scheduler, applied to technical user in SAP Solution Manager system
SAP_BC_REDWOOD_COMM_EXT_SDL	ABAP	Authorization for the technical user between SAP Solution Manager and SAP Central Process Scheduler for configuration of parameter <code>SAP_EnableRfcServer</code> on the process server; applied to technical communication user in Solution Manager system
SAP_BC_REDWOOD_COMMUNICATION	ABAP	Authorization for the technical user between managed (target) system and SAP Central Process Scheduler



---

# 7 Change Control and IT Service Management Scenarios

## 7.1 Getting Started

**What is this guide about?** SAP Solution Manager covers a wide range of diverse scenarios you can use. As a customer, you might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides which cover all relevant information for this specific scenario. This chapter contains information on all applications which are IT Service Management relevant. All these scenarios are based on CRM components:

- Change Management (containing Release Management and Requirement Management as well as CTS, System Recommendation)
- Quality Gate Management
- Incident Management
- Configuration Validation as part of Change Management Validation

Each guide covers the following topics:


- **Getting Started:** find out about target groups of this guide, and about documentation links for any additional components.
- **Prerequisites:** find out about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other. For other application links, see the core security guide.
- **CRM WebClient UI:** find out about the main aspects to be considered for the new *CRM WebClient UI*, such as the concept of Business Roles, User Interface authorization objects, and so on.
- **CRM Standard Customizing:** find out about the new transaction types for CRM, and related customizing entries which are relevant for CRM authorization objects.
- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).
- **Scenario Integration:** according to the life-cycle approach the various scenarios integrate with each other. Here, you can find out about authorizations you need to assign to your users for these cases.
- **External Integration:** for many scenarios, you can also integrate third-party products or other SAP products. Here, you can find out about which authorizations you need to assign to your users for these cases.

## 7.2 Document History

Here, all changes to the specific scenario guide are listed according to Support Package.

Table 173

Support Package Stacks (Version)	Description
SP01	<p><b>General</b></p> <p>Transaction CRM_DNO_SERVICE_MONITOR and associated authorization objects are not supported anymore with Release 7.2. For more information, see CRM application guides.</p> <p><b>Adaptations for Incident Management</b></p> <ul style="list-style-type: none"> <li>• Roles SAP_SM_BI_BILO, SAP_DNOTIFWL_DIS, and SAP_SMWORK_BASIC_INC_MAN obsolete.</li> <li>• Added new roles for Process Documentation integration SAP_SM_SL* and Systems SAP_SYSTEM_REPOSITORY_* to users</li> <li>• All roles for <i>Incident Management</i> have been adapted to the new functionality of <i>Process Documentation</i> and SAP_BASIS 7.40.</li> <li>• Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_INC_MAN has been transferred into roles: SAP_SUPPDESK_*.</li> <li>• Roles for <i>Service Provider</i> SAP_SUPPDESK_SP* and SAP_SUPPCF_* are not supported anymore. The authorization object SM_SP is added to roles SAP_SUPPDESK_*, see section <i>Authorization Objects</i>.</li> <li>• Added new Transaction Types, see section <i>CRM Customizing</i>.</li> </ul> <p><b>Adaptations for Change Request Management</b></p> <ul style="list-style-type: none"> <li>• Roles SAP_SOCM_PRODUCTION_MANAGER, SAP_SM_BI_BILO, and SAP_SMWORK_BASIC_CHANGE_MAN obsolete.</li> <li>• Roles SAP_SOLAR01_DIS and SAP_SOL_PROJ_ADMIN_ALL are removed from user composite roles.</li> <li>• All roles for <i>Change Request Management</i> have been adapted to the new functionality of <i>Process Documentation</i> and SAP_BASIS 7.40.</li> <li>• Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_CHANGE_MAN has been transferred into roles: SAP_CM_SMAN_*, SAP_SYSREC_*, SAP*QGM*, and SAP_CV_*.</li> <li>• New authorization objects due to new Process Documentation: SM_CM_FUNC and SM_CM_DGPN.</li> <li>• Roles for cPro are removed from composite roles, as cPro is no longer supported in Change Request Management</li> <li>• Introduction of new user definition <i>Release Manager</i> in Change Request Management process, see section on users.</li> <li>• Adapted authorization object S_RFC in all relevant roles for use of Function Modules</li> <li>• Obsolete application <i>Schedule Manager</i> removed from role SAP_SMWORK_CHANGE_MAN</li> <li>• All users allowed to call cProject Navigation (Role SAP_BPR_BPM)</li> <li>• Obsolete Transaction Types SMMM, SMMN, SMDV removed in according authorization objects</li> <li>• New Transaction Types SMAI, SMIM, SMRE added in according authorization objects</li> </ul> <p><b>New Functions and Users</b></p> <ul style="list-style-type: none"> <li>• New users and roles for <i>Release Management</i>, see section in <i>Change Management</i></li> </ul>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>New users and roles for <i>Requirement Management</i>, see section in <i>Change Management</i></li> <li>Additional roles SAP_SM_TREX_ADMIN and SAP_SM_ESH_ADMIN for TREX and Embedded Search administration assigned to all SMC* (configuration) users</li> </ul> <p><b>Adaptations for Quality Gate Management</b></p> <ul style="list-style-type: none"> <li>Roles SAP_SM_BI_BILO, and SAP_SMWORK_BASIC_CHANGE_MAN obsolete.</li> <li>Roles SAP_SOLAR* and SAP_SOL_PROJ_ADMIN_ALL are removed from user roles.</li> <li>All roles for <i>Quality Gate Management</i> have been adapted to the new functionality of <i>Process Documentation</i> and SAP_BASIS 7.40.</li> <li>Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_CHANGE_MAN has been transferred into roles: SAP_*QGM*.</li> <li>New authorization objects due to new Process Documentation: SM_CM_FUNC and SM_CM_DGPN.</li> </ul> <p><b>SAP Fiori Launchpad Integration</b></p> <ul style="list-style-type: none"> <li>All users receive SAP Fiori Launchpad authorization role SAP_SM_FIORI_LP_EMBEDDED.</li> </ul>
SP02	<p><b>Change Request Management</b></p> <ul style="list-style-type: none"> <li>adapted all composite roles (from SP01)</li> <li>adapted SAP_SOCM_REQUESTER</li> <li>adapted roles SAP_CM_SMAN_* (authorization object SM_CM_TASK)</li> </ul> <p><b>Quality Gate Management</b></p> <ul style="list-style-type: none"> <li>adapted roles SAP_*QGM* (authorization object SM_CM_TASK)</li> </ul> <p><b>Requirements Management</b></p> <ul style="list-style-type: none"> <li>adapted roles SAP_RM_ITREQ_ADMIN and SAP_RM_SOL_ARCHITECT</li> </ul> <p><b>Incident Management</b></p> <ul style="list-style-type: none"> <li>adapted all composite roles (from SP01)</li> <li>adapted SAP_BI_E2E (due to data activation in ITSM)</li> </ul> <p><b>Release Management</b></p> <ul style="list-style-type: none"> <li>adapted roles SAP_SM_CRM_UIU_RM_DISPLAY, SAP_RM_BUSINESS_MANAGER, SAP_RM_ITREQ_ADMIN, SAP_ITREQ_MANAGER, SAP_RM_SOL_ARCHITECT</li> </ul> <div data-bbox="316 1630 1359 1756" style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"> <p><b>i Note</b> see SAP Note <a href="#">2250709</a> </p> </div>
SP03	<p><b>Quality Gate Management</b></p> <ul style="list-style-type: none"> <li>Adapted section QGM, due to configuration of QGM in transaction SOLMAN_SETUP.</li> <li>Following authorization objects are obsolete and substituted in all relevant roles <ul style="list-style-type: none"> <li>/TMWFLOW/D</li> <li>/TMWFLOW/O</li> </ul> </li> </ul>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>○ /TMWFLOW/P</li> <li>○ /TMWFLOW/R</li> <li>○ /TMWFLOW/S</li> </ul> <p>Substitute authorization object: SM_CM_TASK. It allows differentiation from which User Interface the task can be triggered.</p> <ul style="list-style-type: none"> <li>● Template users and roles for Guided Procedure <i>QGM</i> in transaction SOLMAN_SETUP</li> <li>● Additional role SAP_CM_QGM_MANAGED_SETUP for Managed System Setup procedure for <i>QGM</i> and <i>Change Request Management</i></li> <li>● Adapted all roles SAP_SM_QGM*</li> </ul> <p><b>Change Request Management</b></p> <ul style="list-style-type: none"> <li>● Following authorization objects are obsolete and substituted in all relevant roles <ul style="list-style-type: none"> <li>○ /TMWFLOW/D</li> <li>○ /TMWFLOW/O</li> <li>○ /TMWFLOW/P</li> <li>○ /TMWFLOW/R</li> <li>○ /TMWFLOW/S</li> </ul> </li> </ul> <p>Substitute authorization object: SM_CM_TASK. It allows differentiation from which User Interface the task can be triggered.</p> <ul style="list-style-type: none"> <li>● Adapted all roles SAP_SOCM*</li> <li>● Adapted all roles SAP_CM_SMAN *</li> <li>● Removed transaction codes: /TMWFLOW/REPORTINGN; /TMWFLOW/REPORTING; /TMWFLOW/LOCKMON; /TMWFLOW/MAINT; /TMWFLOW/MAINTENANCE; /TMWFLOW/CMSCONF</li> <li>● Deactivated in all relevant roles authorization object PLOG (organization level for HR)</li> <li>● Adapted role SAP_CHARM_CONFIG</li> <li>● Added roles SAP_ITCALENDER and SAP_SETUP_BASIC_ARCHIVE to user SMC_CH (Configuration User)</li> <li>● Additional role SAP_CM_QGM_MANAGED_SETUP for Managed System Setup procedure for <i>QGM</i> and <i>Change Request Management</i></li> </ul> <p><b>Requirement Management</b></p> <p>Changes in roles are documented on the Menu tab of the respective role</p> <ul style="list-style-type: none"> <li>● Adapted role SAP_RM_CONFIG</li> <li>● Deactivated in all relevant roles authorization object PLOG (organization level for HR)</li> </ul> <p><b>Incident Management</b></p> <p>Changes in roles are documented on the Menu tab of the respective role</p> <ul style="list-style-type: none"> <li>● Adapted roles SAP_SUPPDESK*</li> </ul> <p><b>CTS Plug Managed System</b></p>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>• New role SAP_CM_MANAGED_CTS_ADOP (Administrator and Operator)</li> <li>• New role SAP_CM_MANAGED_CTS_DEV (Developer)</li> </ul>

## 7.3 Scenario-Specific Guide: Quality Gate Management

### 7.3.1 Prerequisites

#### 7.3.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete implementation and upgrade scenario. The SAP Solution Manager is connected via `READ - RFC`, `TRUSTED - RFC` (alternatively `LOGIN`), `TMW - RFC` to your managed systems, and your managed systems are connected to the SAP Solution Manager via `BACK - RFC`. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

##### Technical Infrastructure

- Quality Gate Management

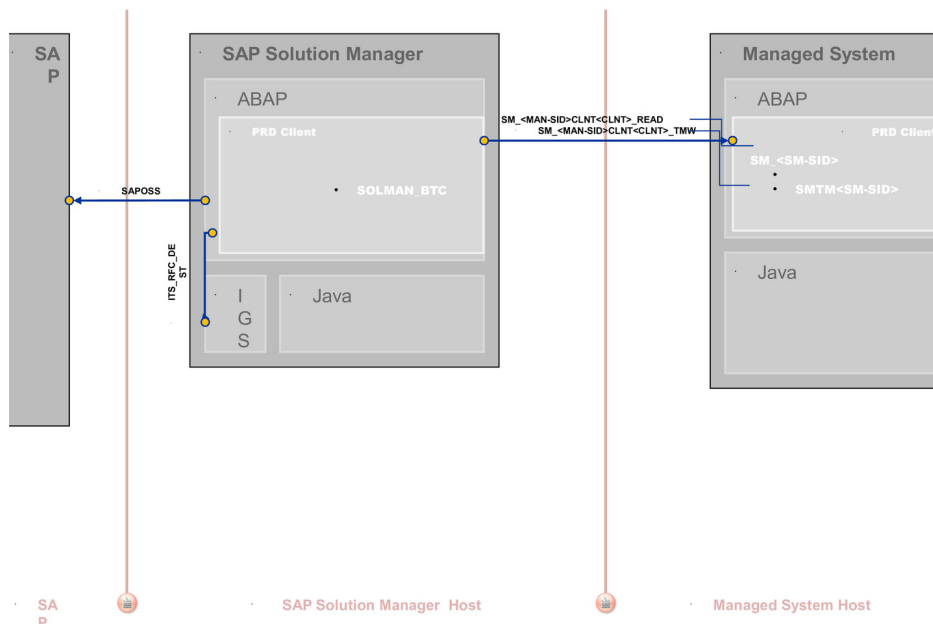


Figure 10: Infrastructure

## 7.3.1.2 Scenario Configuration User

### **i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see *Secure Configuration Guide* chapter *Configuration Users*.

The scenario *Quality Gate Management* is configured using transaction `SOLMAN_SETUP`.

To configure the scenario proceed as follows:

### Creating Configuration User transaction `SOLMAN_SETUP`

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic functions.

When calling the Guided Procedure, you are prompted to create a specific configuration user (default technical name: `SMC_QGM_<XXXClient>`) for QGM (Help Text ID: `USER_CONFIG_QGM`). The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration:

Table 174

Single Role	Help Text ID
<code>SAP_QGM_CONFIG</code>	<code>AUTH_SAP_QGM_CONFIG</code>
<code>SAP_SM_BP_ADMIN</code>	<code>AUTH_SAP_SM_BP</code>
<code>SAP_SM_SL_ADMIN</code>	<code>AUTH_SAP_SM_SL_ADMIN</code>
<code>SAP_SYSTEM_REPOSITORY_ALL</code>	<code>AUTH_SAP_SYSTEM_REP_ALL</code>
<code>SAP_SETUP_SYSTEM_PREP_DISP</code>	<code>AUTH_SAP_SETUP_SYSTEM_PREP_DISP</code>
<code>SAP_SM_SMUA_ALL</code>	<code>AUTH_SAP_SM_SMUA_ALL</code>
<code>SAP_SM_ROLECMP_ALL</code>	<code>AUTH_SAP_SM_ROLECMP_ALL</code>
<code>SAP_SM_USER_ADMIN</code>	<code>AUTH_SAP_SM_USER_ADMIN</code>
<code>SAP_SM_FIORI_LP_EMBEDDED</code>	<code>AUTH_SAP_SM_FIORI_LP_EMBEDDED</code>
<code>SAP_SM_ESH_ADMIN</code>	<code>AUTH_SAP_SM_ESH_ADMIN</code>
<code>SAP_CM_QGM_MANAGED_SETUP</code>	<code>AUTH_SAP_QGM_CONFIG</code>

If you want to create the configuration user manually, you need to assign:

- the composite role `SAP_QGM_CONF_COMP` which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

### **i** Note

To be able to create users and assign user roles, you need to assign as well role `SAP_SM_USER_ADMIN`.

## User Roles for Managed System Setup

The Managed System Setup is relevant for both scenarios, *Change Request Management* and *Quality Gate Management*. In order to run the procedure with complete authorizations, you need to add the following role to the respective configuration user for SMC\_QGM\_\*\*\* or SMC\_CM\_\*\*\*: SAP\_CM\_QGM\_MANAGED\_SETUP.

In case you would want to execute the procedure with a specific user, assign the following roles:

Table 175

Single Role	Help Text ID
SAP_CM_QGM_MANAGED_SETUP	AUTH_SAP_CM_QGM_MANAGED_SETUP
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SMWORX_CONFIG	AUTH_SAP_SMWORX_CONFIG
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

## 7.3.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 176

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to managed systems	RFC	Reading information from managed systems

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction SOLMAN\_SETUP (view: managed systems), see *Secure Configuration Guide*.

Table 177

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	reads data from the managed system, see scenario-specific guide for Change Request Management
SM_<SID>CLNT<Client>_TMW (ABAP connection)	Managed System	System-specific	System-specific	Default user: SMTM<SID> of Solution Manager system>	Used for specific Change Management authorization, see scenario-specific guide for Change Request Management

#### Internet Graphics Server (IGS) RFC Connection

Table 178

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

## 7.3.1.4 Technical Users

The technical users in the following tables are created automatically during configuration. For more information on the individual technical users, see the *Secure Configuration Guide* in section *Technical Users*.

### Users in Managed Systems

Table 179

User Name	User ID
<i>Read - User</i>	SM_<SID> of Solution Manager system>
<i>TMW - User</i>	SMTM<SID> of Solution Manager system>



## 7.3.2 CRM Standard Customizing for Solution Manager

The Quality Gate Management scenario is based on CRM, and uses CRM customizing such as Transaction Types, Action Profiles, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects. The following table gives you an overview of the transaction types used.

### Caution

If you copy SAP standard customizing you need to add the changed values in the according CRM - authorization objects for the scenario. See also How-to Guide on how to maintain authorization objects.

### Transaction Type

Table 180

Transaction Type	Usage	Remarks
SMQC	Quality Gate Management	supported

## 7.3.3 Scenario Integration

QGM refers to the phase in your product life-cycle when you approve the quality of your past activities. According to the end-to-end business process life-cycle, this phase needs to integrate with a number of other functions which come into play in your daily business. The following sections describe the integration of QGM with other scenarios within SAP Solution Manager, and which user roles would be applicable.

### Note

For more detail on each individual scenarios, see the according *Scenario-Specific Guide*.

### Change Request Management

If Q-Gates and phases are managed in QGM and the process is managed in Change Request Management, you need to assign QGM role: SAP\_QGM\_ADMIN\_COMP, the Change Request Management role SAP\_CM\_ADMINISTRATOR\_COMP.

### Issue Management

You need to assign role SAP\_ISSUE\_MANAGEMENT\_\*\_COMP in addition for your Administrator, Quality Manager, and Quality Advisory Board.

## 7.3.4 Users and Authorizations

### 7.3.4.1 User Roles in the SAP Solution Manager

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for Quality Gate Management. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information about User Interface authorizations, see Authorization Concept Guide.

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

#### IT Operator (Help Text ID: TP\_QGM\_ITO)

Technical role name: `SAP_QGM_TRANSPORT_COMP`

Table 181

Single Roles	Help Text ID
<code>SAP_SM_QGM_TRANSPORT</code>	<code>AUTH_SAP_SM_QGM_TRANSPORT</code>
<code>SAP_SMWOR_K_CHANGE_MAN</code>	<code>AUTH_SAP_SMWOR_K_CHANGE_MAN</code>
<code>SAP_SM_KW_ALL</code>	<code>AUTH_SAP_SM_KW_ALL</code>
<code>SAP_SM_QGM_CM_TRANSPORT</code>	<code>AUTH_SAP_SM_QGM_CM_TRANSPORT</code>
<code>SAP_SM_SL_DISPLAY</code>	<code>AUTH_SAP_SM_SL_DISPLAY</code>
<code>SAP_SYSTEM_REPOSITORY_DIS</code>	<code>AUTH_SAP_SYSTEM_REP_DIS</code>
<code>SAP_ITCALENDER_DIS</code>	<code>AUTH_SAP_ITCALENDER_DIS</code>
<code>SAP_SM_FIORI_LP_EMBEDDED</code>	<code>AUTH_SAP_SM_FIORI_LP_EMBED</code>
<code>SAP_SYSTEM_REPOSITORY_DIS</code>	<code>AUTH_SAP_SYSTEM_REP_DIS</code>
<code>SAP_SM_BP_DISPLAY</code>	<code>AUTH_SAP_SM_BP_DISPLAY</code>

#### Development Lead (Help Text ID: TP\_QGM\_DL)

Technical role name: `SAP_QGM_CHANGE_MANAGER_COMP`

Table 182

Single Roles	Help Text ID
<code>SAP_SM_QGM_CHANGE</code>	<code>AUTH_SAP_SM_QGM_CHANGE</code>
<code>SAP_SMWOR_K_CHANGE_MAN</code>	<code>AUTH_SAP_SMWOR_K_CHANGE_MAN</code>
<code>SAP_SM_KW_ALL</code>	<code>AUTH_SAP_SM_KW_ALL</code>

Single Roles	Help Text ID
SAP_SM_QGM_CM_TRANSPORT	AUTH_SAP_SM_QGM_CM_CHANGE
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY

### Quality Manager (Help Text ID: TP\_QGM\_QM)

Technical role name: SAP\_QGM\_QM\_COMP

Table 183

Single Roles	Help Text ID
SAP_SM_QGM_STATUS_QM	AUTH_SAP_SM_QGM_STATUS_QM
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SM_QGM_CM_QM	AUTH_SAP_SM_QGM_STATUS_QM
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY

### Quality Advisory Board Member (Help Text ID: TP\_QGM\_QAB)

Technical Role Name: SAP\_QGM\_QAB\_COMP

Technical role name: SAP\_QGM\_QM\_COMP

Table 184

Single Roles	Help Text ID
SAP_SM_QGM_STATUS_QAB	AUTH_SAP_SM_QGM_STATUS_QAB
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SM_QGM_CM_TRANSPORT	AUTH_SAP_SM_QGM_STATUS_QAB

Single Roles	Help Text ID
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY

### QGM Project Administrator (Help Text ID: TP\_QGM\_PM)

Technical role name: SAP\_QGM\_ADMIN\_COMP

Table 185

Single Roles	Help Text ID
SAP_SM_QGM_ALL	AUTH_SAP_SM_QGM_ALL
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SM_QGM_CM_ALL	AUTH_SAP_SM_QGM_ALL
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP_ADMIN

### Main Authorization Objects

#### Authorization Object SM\_CM\_FUNC

This object replaces authorization objects S\_PROJECT and S\_PROJ\_GEN for *Downgrade Protection* authorization. The object contains fields for *Solution Name* and *Branch*. These fields are also contained in *Process Documentation* authorization objects, for instance SM\_SDOC.

#### Authorization Object S\_TABU\_DIS

In user roles for QGM you find authorization object S\_TABU\_DIS. Authorization group CRMC protects all relevant customizing views and customizing clusters for this scenario.

#### Authorization Object S\_IWB

With Release 7.2, *Document Management* authorizations S\_IWB\* are substituted with new authorization objects in relation to the new *Process/Solution Documentation*, for more information see the Security Guide explaining the general *Authorization Concept*. Still, authorization object S\_IWB is nevertheless used in QGM, in case you use

the (old) document area `IWBSOLAR` to store documents. The object is therefore added separately to the relevant QGM core roles: `SAP_SM_QGM_*`.

## 7.3.4.2 User Descriptions and User Roles in the Managed Systems

For some of the users working in the SAP Solution Manager, you need to assign authorizations in the according managed systems:

- QGM Project Administrator (technical role name: `SAP_CM_MANAGED_ADMIN`)
- QGM Quality Manager (technical role name: `SAP_CM_MANAGED_TESTER`)
- QGM Quality Advisory Board Member (technical role name: `SAP_CM_MANAGED_TESTER`)
- QGM IT-Operator (technical role name: `SAP_CM_MANAGED_OPERATOR`)

### **i** Note

All users need authorization object `S_RFCACL` additionally assigned to be able to use the trusted - connection between systems.

## 7.3.4.3 Central CTS-Integration User Roles in the SAP Solution Manager

You can use CTS with QGM. To be able to use this integration, assign the following roles to your SAP Solution Manager users.

### RFC - Destinations

You require:

- `TMW` – RFC Destination
- `TMS` Deploy Destination (`TMSDPL@SID.DOMAIN`)

### Change Manager - Transport Authorization (technical role name: `SAP_BC_CCTS_QGM_CH_MGR_TMPL`)

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- changes in regard to previous Support Packages

The main critical authorization object is `S_CTS_ADMI` with value `PROJ`.

### IT Operator - Transport Authorization (technical role name: `SAP_BC_CCTS_QGM_OPERAT_TMPL`)

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- changes in regard to previous Support Packages
- trigger imports (system-specific and cluster-specific)
- create, change, delete, and release collections (system-specific and cluster-specific)
- change import queues

The main critical authorization object is S\_CTS\_ADMI with value PROJ.

### **QA Manager and Advisory Board - Transport Authorization (technical role name: SAP\_BC\_CCTS\_QGM\_QA\_MGR\_TMPL)**

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- changes in regard to previous Support Packages
- trigger imports (system-specific and cluster-specific)
- create, change, delete, and release collections (system-specific and cluster-specific)

### **Administrator - Transport Authorization (technical role name: SAP\_BC\_CCTS\_QGM\_ADMIN\_TMPL)**

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- changes in regard to previous Support Packages
- trigger imports (system-specific and cluster-specific)
- create, change, delete, and release collections (system-specific and cluster-specific)
- change import queues

The main critical authorization object is S\_CTS\_ADMI with value PROJ.

## **7.4 Scenario-Specific Guide: IT Service Management**

### **7.4.1 Prerequisites**

#### **7.4.1.1 Technical System Landscape**

The graphic below gives you an overview over the basic technical system landscape that is needed to run the *Incident Management* scenario. The SAP Solution Manager is connected via READ - RFC to your managed systems, and your managed systems are connected to the SAP Solution Manager via BACK - RFC. To connect to SAP, the destinations SAP-OSS and SAP-OSS-LIST\_001 are used. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

Technical Infrastructure  
 • Incident Management

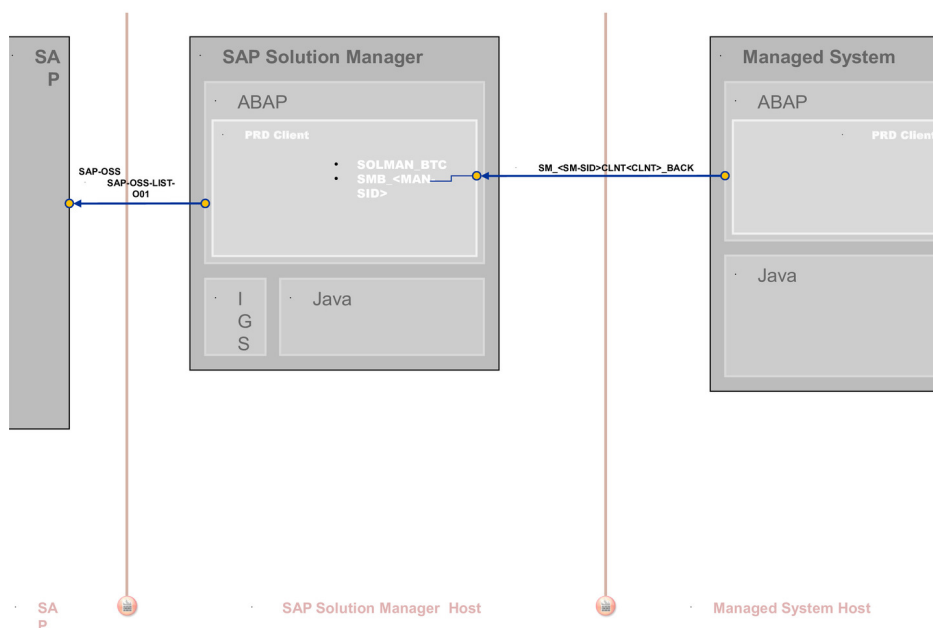


Figure 11: Infrastructure

## 7.4.1.2 Scenario Configuration User

**i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see *Secure Configuration Guide* section *Configuration Users*.
- the BW integration concept, see *Authorization Concept* section on *BW Integration*.

The scenario is configured using transaction `SOLMAN_SETUP`.

To configure the scenario proceed as follows:

### Creating Configuration User in Basic Configuration Transaction `SOLMAN_SETUP`

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic function to send an Incident message to SAP. For more information, see *Secure Configuration Guide*.

During basic automated configuration, you can create a specific configuration user (default technical user name: `SMC_IM_<XXXXClient>`) for Incident Management (Help Text ID: `USER_CONFIG_IM`). The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

If you want to create the configuration user manually, you need to assign:

- the composite role `SAP_SUPPDESK_CONF_COMP` which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

**i** Note

To be able to:

- create users and assign user roles, you need to assign as well role `SAP_SM_USER_ADMIN`.
  - use a trusted RFC connection between the Solution Manager and the managed systems, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system as well as the managed system.
- the composite role `SAP_BW_SUPPDESK_ADMIN_COMP` which contains all single roles that are automatically assigned to the configuration user in the BW-system.

**i Note**

To be able to use a trusted RFC connection between the Solution Manager and the BW-system, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system and role `SAP_SM_BW_S_RFCACL` in the BW-system.

### Scenario Configuration Transaction `SOLMAN_SETUP`

You can configure the basic technical settings using transaction `SOLMAN_SETUP`, running the guided procedure for Incident Management for `ITSAM` Service Management.

During the specific guided configuration you can create *Standard Template Users*. The system automatically adds all relevant user roles, see according sections on *Users and User Roles*.

## 7.4.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 186

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems and back	RFC	Reading information from managed systems
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes
Third Party Service Desk	SOAP over HTTP (S)	Data Exchange



## Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 187

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	Used during setup of incident management, and during operations when generating business partners

### RFC Connection from Managed System to SAP Solution Manager

Table 188

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	SMB_<managed system ID>	Generating Support Messages from managed systems (table: BCOS_CUST)	Automatically created via transaction SOLMAN_SETUP (view: managed systems)

### BW- Reporting RFC Connection

Table 189

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	
BI_CLNT<BWclient> if BW is realized in remote BW - scenario system, for content activation and data download	Managed System or Solution Manager System	System-specific	System-specific		in transaction SOLMAN_SETUP

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
<SolutionManagerSID>CLNT<SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client	System-specific	System-specific	BI_CALLBACK (customer specific)	in transaction SOLMAN_SETUP
Trusted RFC to remote BW systemSAP_BILO	remote BW - system (source: SAP Solution Manager)	System-specific	System-specific	Dialog User	Used to read data from remote BW for BI - Reporting , created during SOLMAN_SETUP

### RFC Connections from SAP Solution Manager to SAP

Table 190

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SAP-OSS (ABAP connection)	/H/SAPROUTER/S//sapser/H/oss001	01	001	S-User (Customer-specific)	in transaction SOLMAN_SETUP
SAP-OSS-LIST-001 (ABAP connection)	/H/SAPROUTER/S//sapser/H/oss001	01	001	S-User (Customer-specific)	in transaction SOLMAN_SETUP
SM_SP_<customer number>	/H/SAPROUTER/S//sapser/H/oss001	01	001	S-User (Customer-specific)	Automatically created

**i Note**  
For more information on Service Provider - specific settings, see [Service Provider Guideline](#)

### TREX RFC Connections

Table 191

RFC Destination Name	Activation Type	How Created
TREX_<server> (ABAP connection)	Registered Server Program (program TREXRfcServer_<instance number>)	Manually in transaction SM59

RFC Destination Name	Activation Type	How Created
IMSDEFAULT	Start on explicit host (program: <code>ims_server_admin.exe</code> )	TREX can be administered using the TREX admin tool, see IMG activity <i>Information and Configuration Prerequisites for TREX Setup</i>
IMSDEFAULT_REG	Registered Server Program (program: <code>rfc_sapretrieval</code> )	(technical name: <code>SOLMAN_TREX_INFO</code> )

### Internet Graphics Server (IGS) RFC Connection

Table 192

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: <code>IGS.&lt;SID&gt;</code> )	Manually in transaction SM59

## 7.4.1.4 Technical Users

The users in the following tables are created automatically or manually during configuration. All technical users are of type *System User*, except for user `DEFECTMAN` (Communication User). For more information on individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

### User in SAP Solution Manager System

Table 193

User Name	User ID
<i>Back - User</i>	<code>SMB_&lt;managed system ID&gt;</code>
User <i>Third Party Service Desk</i> <code>DEFECTMAN</code>	<p><b>i</b> Note</p> <p>User for web service; assigned roles <code>SAP_SUPPDESK_ADMIN</code> and <code>SAP_SUPPDESK_INTERFACE</code></p>

### Users in Managed Systems


Table 194

User Name	User ID
<i>Read - User</i>	<code>SM_&lt;SID of Solution Manager System&gt;</code>

## 7.4.1.5 SAP Support Portal Contact in SAP Solution Manager (Table: AISUSER)

Users who communicate with SAP Support Portal via RFC destination SAP-OSS need an SAP Support Portal contact to SAP Solution Manager. You maintain the contact in table AISUSER (transaction AISUSER). This contact corresponds to the S-User in the SAP Support Portal, without the initial **S**.

### Caution

The S-User for the SAP Support Portal must be requested via URL [service.sap.com](https://service.sap.com) 

## 7.4.1.6 S-User Authorization for Service Desk and Expert on Demand

Your S-User needs the following authorizations for SAP Support Portal functions.

### S-User Authorization

Table 195

Activity	Authorization
Create message	ANLEG: Create SAP message
Send messages	GOSAP: Send to SAP
	WAUFN: Reopen SAP message
Confirm messages	QUITT: Confirm SAP message
Display/change secure area	PWDISP: Display secure area
	PWCHGE: Change secure area

## 7.4.2 CRM Standard Customizing for Solution Manager

The Incident Management scenario is based on CRM 7.01, and uses CRM customizing such as Transaction Types, Action Profiles, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects for Incident Management. The following table gives you an overview of the *Transaction Types* used.

### Caution

If you copy SAP standard customizing you need to add the changed values in the according CRM - authorization objects for the scenario. See also *How-to Guide* on how to maintain authorization objects.

## Transaction Types (old)

### ➔ Recommendation

We recommend to use the new Transaction Types.

Table 196

Transaction Type	Usage	Remarks
SLEFN	Standard Service Desk	supported
SIST	Standard Service Desk	supported
SIVA	Service Request for Service Provider (VAR)	supported
SISV	Service Request for Software Partners (ISV)	supported

## Transaction Types (new)

Table 197

Transaction Type	Usage	Remarks
SMIN	CRM - Service Request	supported
SMIV	Service Request for Service Provider (VAR)	supported
SMIS	Service Request for Software Partners (ISV)	supported
SMIT	template for SMIN transaction types	supported
SMPR	Problem	supported
SMPT	template for problems	supported
SMRQ	Service Request	supported
SMRT	Service Request Template	supported
KNAR	Knowledge Article	supported
SMSO	ITSM Service Order	supported
SMST	Order Template	supported

## 7.4.3 Scenario Integration

Incident Management refers to all phases in your product life-cycle.

## Various Scenarios

According to the end-to-end business process life-cycle, this function needs to integrate with many other scenarios which come into play in your daily business, such as implementation, upgrade, monitoring, and so on. Within these scenarios, it is possible for users to create messages for Incident Management. The integration of Incident Management is described in the various scenario-specific guides for the individual scenarios. For more detail on each individual scenario, see the according *Scenario-Specific Guide*.

## Change Request Management

Apart from the function of creating an Incident Management message within different scenarios, an Incident Management message can also lead to a Change Request. If you are using this integration, you need to assign as well the role for user *Requester*: `SAP_CM_REQUESTER_COMP`. For more information about the Change Request Management scenario, see the according *Scenario-Specific Guide*.

## 7.4.4 Users and Authorizations

### 7.4.4.1 Authorizations and Roles

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for *Incident Management*. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information about user interface authorizations, see *Authorization Concept Guide* chapter on *User Interface Authorizations*.

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

#### Authorization for Trusted RFC between SAP Solution Manager and BW-System

In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object `S_RFCACL` (role `SAP_SM_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`). The user in the BW - system is also assigned authorization `S_RFCACL` (role `SAP_SM_BW_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`).

#### Administrator (Help Text ID: TP\_IM\_ADMIN)

Technical composite role name: `SAP_SUPPDESK_ADMIN_COMP` in the Solution Manager system/client

Table 198

Single Roles	Help Text ID
<code>SAP_SUPPDESK_ADMIN</code>	<code>AUTH_SAP_SUPPDESK_ADMIN</code>
<code>SAP_SMWORK_INCIDENT_MAN</code>	<code>AUTH_SAP_SMWORK_INCIDENT_MAN</code>
<code>SAP_SM_CRM_UIU_FRAMEWORK</code>	<code>AUTH_SAP_SM_CRM_UIU_FRAME</code>

Single Roles	Help Text ID
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_BI_INCMAN_REPORTING	AUTH_SAP_SM_BI_INCMAN_REP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_DSH_CONF	AUTH_SAP_SM_DSH_CONF

**Technical composite role name: SAP\_BW\_SUPPDESK\_ADMIN\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same *User ID* in the BW system.

Table 199

Single Roles	Help Text ID
SAP_BI_E2E_SD	AUTH_SAP_BI_E2E
SAP_BW_SPR_REPORTING	AUTH_SAP_BW_SPR_REPORT
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

**Processor (Help Text ID: TP\_IM\_PROC)**

**Technical composite role name: SAP\_SUPPDESK\_PROCESS\_COMP in the Solution Manager system/client**

Table 200

Single Roles	Help Text ID
SAP_SUPPDESK_PROCESS	AUTH_SAP_SUPPDESK_PROCESS
SAP_SMWORK_INCIDENT_MAN	AUTH_SAP_SMWORK_INCIDENT_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_BI_INCMAN_REPORTING	AUTH_SAP_SM_BI_INCMAN_REP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP

**Technical composite role name: SAP\_BW\_SUPPDESK\_DISPLAY\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same *User ID* in the BW system.

Table 201

Single Roles	Help Text ID
SAP_BW_SPR_REPORTING	AUTH_SAP_BW_SPR_REPORT
SAP_BI_E2E_SD	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Key User (Help Text ID: USER\_TP\_IM\_CREATE)

Technical composite role name: SAP\_SUPPDESK\_CREATE\_COMP in the Solution Manager system/client

Table 202

Single Roles	Help Text ID
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SMWORK_INCIDENT_MAN	AUTH_SAP_SMWORK_INCIDENT_MAN
SAP_SM_CRM_UIU_SOLMANPRO_CREA	AUTH_SAP_SM_CRM_UIU_CREA
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANREQU	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

#### **i** Note

If you want the Key-User to display:

- the created message, you need to add the display user authorizations as well.
- Incidents of other Key-Users (for instance, if you run *Incident Management* in a Service Provider scenario), set the value x for parameter IM\_RESPONSIBLE\_REL\_ENABLE in table AGS\_WORK\_CUSTOM. For complete information, see SAP Note [1256661](#).

### Display User (Help Text ID: TP\_IM\_DIS)

Technical composite role name: SAP\_SUPPDESK\_DISPLAY\_COMP in the Solution Manager system/client

Table 203

Single Roles	Help Text ID
SAP_SUPPDESK_DISPLAY	AUTH_SAP_SUPPDESK_DISPLAY
SAP_SMWORK_INCIDENT_MAN	AUTH_SAP_SMWORK_INCIDENT_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN



Single Roles	Help Text ID
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR
SAP_SM_BI_INCMAN_REPORTING	AUTH_SAP_SM_BI_INCMAN_REP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP

**Technical composite role name: SAP\_BW\_SUPPDESK\_DISPLAY\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same *User ID* in the BW system.

Table 204

Single Roles	Help Text ID
SAP_BI_E2E_SD	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP
SAP_BW_SPR_REPORTING	AUTH_SAP_BW_SPR_REPORT

**Dispatcher User (Help Text ID: TP\_IM\_DIS)**

**Technical composite role name: SAP\_SUPPDESK\_DISPATCHER\_COMP in the Solution Manager system/client**

Table 205

Single Roles	Help Text ID
SAP_SUPPDESK_DISPATCH	AUTH_SAP_SUPPDESK_DISPATCH
SAP_SMWORK_INCIDENT_MAN	AUTH_SAP_SMWORK_INCIDENT_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANDSPATCH	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

## 7.4.4.2 Authorization Objects

The following section gives information of some of the main authorization objects for Incident Management.

## ITSM Reporting Links in CRM WebUI

To allow any user to see and use the *ITSM Reporting* and *ITSM Dashboard* links in the CRM WebUI, the following authorization objects must be maintained:

- Solution Manager UI authorization (contained in role `SAP_SUPPDESK_*`)  
Authorization object `SM_WD_COMP` with value `ITSM_REPORTING`
- CRM WebUI authorization (contained in role `SAP_SM_UIU_COMP_SOLMANPRO_*`)  
Authorization object `C_LL_TGT` with value `C` (Launch Transaction) and the links for:
  - `ITSM_REPORTING`
  - `SM_ITSM_REPORTING_DASHBOARD`
  - `SM_ITSM_REPORTING_FRAMEWORK`

## Support Team Search: PLOG

To allow the support team search based on `PFAC` rule, you must activate authorization object `PLOG`. The object is contained in roles `SAP_SUPPDESK_*`.

### **i** Note

To be able to use this function, you need to maintain an organizational model.

## Authorization Object: SM\_SP

The object defines the use of the application for *Service Providers*. It is included into the core roles for Incident Management, set inactive. If you are using Incident Management as a Service Provider, you need to set the authorization object active.

## 7.4.5 External Integration

### 7.4.5.1 External Service Desk

#### Roles

##### Service Desk Interface

Table 206

Name	Type	Remarks
<code>SAP_SUPPDESK_INTERFACE</code> External Service Desk integration user	ABAP System User	Authorization for bi - directional interface and configuration; needs to be assigned in addition to the roles for the Service Desk scenario, for instance <code>SAP_SUPPDESK_ADMIN</code>
		User for data exchange; assigned roles <code>SAP_SUPPDESK_ADMIN</code> and <code>SAP_SUPPDESK_INTERFACE</code>

## 7.4.6 Integration of SAP Fiori Applications

Here, you find specific information on the individually delivered applications that can be used on a central Fiori Hub. For more information on the concept of SAP Fiori Launchpad and Central Hub Scenarios, see [Authorization Concept Guide](#).

### **i** Note

General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the Authorization Concept for Solution Manager.

### APP: My Incidents

This application allows users to view and respond to their ITSM Incidents. Users can do the following:

- View the details of their Incidents: Details include short text, long texts (restricted by authorization object CRM\_TXT\_ID authorizations), status, priority, attachments, and so on.
- Send an answer back to the Incident processor. This implicitly changes the status of the Incident to *In Process*.
- Add attachments such as Word documents, screen shots, and so on.
- Confirm or withdraw the Incident when they are finished with the Incident.

### Authorizations in the Back-End SAP Solution Manager (ST Component)

### **i** Note

As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, assign the relevant composite role SAP\_SUPPDESK\_CREATE\_COMP to the user or create the template user via transaction SOLMAN\_SETUP. The relevant Odata - Service is delivered per default in the core role for Key-Users for Incident Management SAP\_SUPPDESK\_CREATE.

Due to the nature of the application as a subset of the complete functionality of Incident Management for Key-Users, **not all authorizations for the key user in this role are required to run the application**. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the SAP\_SUPPDESK\_CREATE role accordingly. In this case, remove all roles relating to CRM WebClient, as well as BW-related roles.

To allow for a trusted RFC - destination, you need also assign role SAP\_SM\_FIORI\_FRONTEND in the back end system. The role contains S\_RFC and S\_RFCACL authorization.

### Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- SAP\_STUI\_ITSM\_MYINC\_TCR  
This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- SAP\_STUI\_ITSM\_MYINC\_AUTH  
This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:

1. Copy the Odata service into your name space.
2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

## 7.5 Scenario-Specific Guide: Change Management

### 7.5.1 Prerequisites

#### 7.5.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete *Change Request Management* scenario. The SAP Solution Manager is connected via `READ - RFC`, `TRUSTED - RFC`, `TMW - RFC` to your managed systems, and your managed systems are connected to the SAP Solution Manager via `BACK - RFC`. A `SAPOSS` connection to SAP is in place. Between managed systems `RFC` connections exist, for instance for *Retrofit* purposes. In addition, if `BW - Reporting` is used, all required `BW - Connections` must be in place. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

#### Technical Infrastructure

- Change Request Management

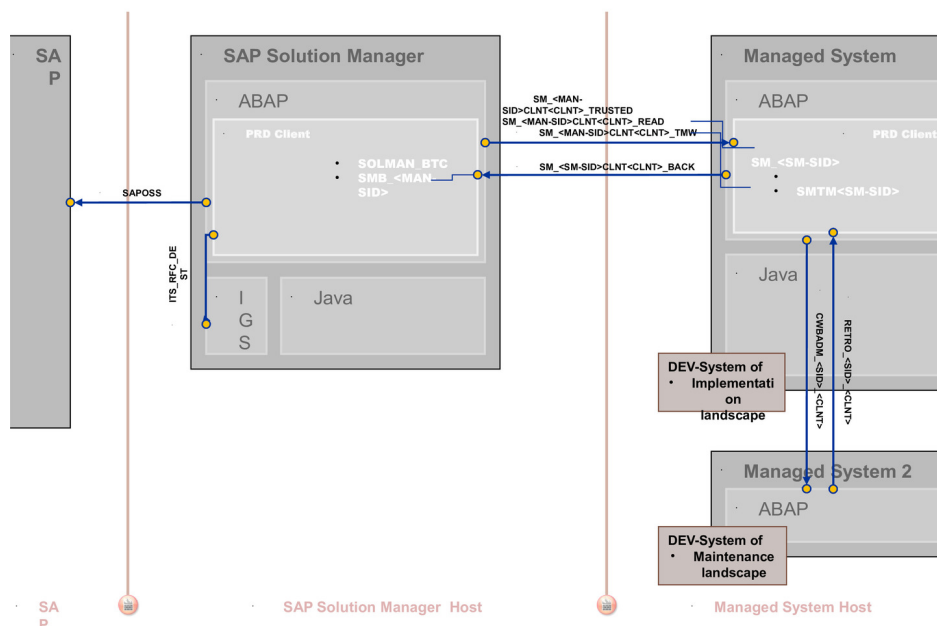


Figure 12: Infrastructure

## 7.5.1.2 Scenario Configuration User

### **i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see *Secure Configuration Guide* chapter *Configuration Users*.
- the BW integration concept, see *Authorization Concept Guide* chapter on BW integration.

The scenario *Change Request Management* is configured using transaction `SOLMAN_SETUP`.

To configure the scenario proceed as follows:

### Creating Configuration User for Transaction `SOLMAN_SETUP`

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic functions.

During basic automated configuration, you can create a specific configuration user (default technical name: `SMC_CHRM_<XXXXClient>`) for `CHARM` (Help Text ID: `USER_CONFIG_CHARM`). The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

If you want to create the configuration user manually, you need to assign:

- the composite role `SAP_CM_CONF_COMP` which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

### **i** Note

To be able to:

- create users and assign user roles, you need to assign as well role `SAP_SM_USER_ADMIN`.
  - use a trusted RFC connection between the Solution Manager and the managed systems, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system as well as the managed system.
- the composite role `SAP_SM_BW_CHARM_ADMIN_COMP` which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

### **i** Note

To be able to use a trusted RFC connection between the Solution Manager and the BW-system, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system and role `SAP_SM_BW_S_RFCACL` in the BW-system.

### User Roles for Managed System Setup

The Managed System Setup is relevant for both scenarios, *Change Request Management* and *Quality Gate Management*. In order to run the procedure with complete authorizations, you need to add the following role to the respective configuration user for `SMC_QGM_***` or `SMC_CM_***`: `SAP_CM_QGM_MANAGED_SETUP`.

In case you would want to execute the procedure with a specific user, assign the following roles:

Table 207

Single Role	Help Text ID
<code>SAP_CM_QGM_MANAGED_SETUP</code>	<code>AUTH_SAP_CM_QGM_MANAGED_SETUP</code>

Single Role	Help Text ID
SAP_SM_USER_ADMIN	AUTH_SAP_SM_BP
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Scenario Configuration transaction SOLMAN\_SETUP

You can configure the basic technical settings using transaction SOLMAN\_SETUP, running the guided procedure for Change Request Management for ITSM Service Management.

During the specific guided configuration you can create Standard template users. The system automatically adds all relevant user roles, see according sections on *Users and User Roles*.

## 7.5.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 208

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to managed systems	RFC	Reading information from managed systems

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction SOLMAN\_SETUP (view: managed systems), see *Secure Configuration Guide*.

Table 209

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client> >_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	This RFC is generally needed for reading data in connection with transports (transport infrastructure), such as tracking reporting or object changes, read status of transports.
SM_<SID>CLNT<Client> >_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific	The RFC - connection is mandatory for all tasks that involve system changes due to transports. Within the <i>Task List Framework</i> the login prompt is avoided.
SM_<SID>CLNT<Client> >_TMW (ABAP connection)	Managed System	System-specific	System-specific	Default user: SMTW<SID> of Solution Manager system>	Only necessary when <i>Transport Management</i> is in place; allows for creating and releasing of transport requests via remote pattern

### RFC Connection from Managed System to SAP Solution Manager

Table 210

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
SM_<SID>CLNT<Client> >_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	Default user:SMB_<m anaged system ID>		Automatically created via transaction SOLMAN_SETUP (view: managed systems)
SM_<SID>CLNT<Client> >_BACK_CSOL (ABAP connection)	Solution Manager System	System-specific	System-specific	Customer-specific	For function <i>Cross System Object Lock</i> CSOL	Manually created

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
					<p><b>i</b> Note</p> <p>SAP Solution Manager manages the lock information.</p>	

### BW- Reporting RFC Connection

Table 211

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	
BI_CLNT<BWclient>, if BW is realized in remote BW - scenario system , for content activation and data download	Managed System or Solution Manager System	System-specific	System-specific	System-specific	in transaction SOLMAN_SETUP
<SolutionManagerSID>CLNT<SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client	System-specific	System-specific	BI_CALLBACK (customer specific)	in transaction SOLMAN_SETUP
Trusted RFC to remote BW system SAP_BILO	remote BW - system (source: SAP Solution Manager)	System-specific	System-specific	Dialog User	Used to read data from remote BW for BI - Reporting . created during SOLMAN_SETUP

### Retrofit RFC - Connections



Table 212

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User	Remarks
RETRO_<SID>_<CLNT>	Managed system, development system (Implementation landscape)	System-specific	System-specific	Customer-specific	Trusted RFC - connection. For transport of copies
CWBADM_<SID>_<CLNT>	Managed System, development system (Maintenance landscape)	System-specific	System-specific	Customer-specific	Trusted RFC - connection, for comparison and merge of coding according to ToDo list in <i>Correction Workbench</i>

### TMS CI RFC - Connections

Instead of TMS CI RFC - connections, you can use the Trusted RFC - connection. For more information, see [SAP Note 1384598](#).

### Internet Graphics Server (IGS) RFC Connection

Table 213

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

## 7.5.1.4 Technical Users

### **i** Note

Check SAP Note [807228](#).

The technical users in the following tables are needed for the scenario. They are created automatically or manually during configuration. All technical users are of type *System User*, except for *CSOL - Back User*. *CSOL - Back User* is of type *Service*. For more information on the individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

### Users in Managed Systems

Table 214

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>
<i>TMW - User</i>	SMTM<SID of Solution Manager system>

## Users in SAP Solution Manager System

Table 215

User Name	User ID
<i>Back - User</i>	SMB_<managed system ID>
<i>CSOL - Back - User</i>	Manually created in transaction SOLMAN_SETUP (assigned role <namespace>SAP_SOLMANTMWCOL)

## 7.5.2 CRM Standard Customizing for Solution Manager

The *Change Request Management* scenario is based on CRM 7.0 EHP1, and uses CRM customizing such as *Transaction Types*, *Action Profiles*, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects for *Change Request Management*. The following table gives you an overview of the *Transaction Types* used.



### Caution

If you copy SAP standard customizing you need to add the changed values in the according CRM - authorization objects for the scenario. See also *How-to Guide* on how to maintain authorization objects.

### Transaction Types

Table 216

Transaction Type	Usage
SMHF	Urgent Change
SMMJ	Normal Change (Standard)
SMTM	Defect Correction
SMCG	General Change
SMCR	Request for Change
SMCT	Request for Change Template
SMAD	Administration
SMAI	Continual Cycle
SMIM	Phased Cycle
SMRE	Released Cycle

## 7.5.3 Scenario Integration

*Change Request Management* refers to the phase in your product life-cycle when you define and refine your business processes by means of projects and related activities. According to the end-to-end business process

life-cycle, this phase needs to integrate with a number of other functions which come into play in your daily business, such as handling of problems, and so on. The following sections describe the integration of *Change Request Management* with other scenarios within SAP Solution Manager, and which user roles would be applicable.

### **i** Note

For more detail on each individual scenario, see the according *Scenario—Specific Guide*.

## Customizing Synchronization

*Customizing Synchronization* is part of scenario *Implementation*, for more information see the *Scenario - Specific Guide for Implementation* as well as SAP Note [1061644](#).

## Incident Management

A Change Request can result from an Incident. Incidents can be created by any user. To be able to do so, you need to assign the user role `SAP_SUPPDESK_CREATE_COMP`.

## Test Management

- In the assignment block *Test Management*, you can maintain test plans and test packages. This requires authorization object `SM_TWB` for *Test Management*. You can either assign this authorization with required field values to your user or you can assign the role for test plans `SAP_STWB_2_*`.
- Testing normal corrections and urgent corrections requires Test Management role for the Tester `SAP_STWB_WORK_ALL`.

## Quality Gate Management (QGM)

You can integrate QGM with Change Request Management. When integrating assign the respective roles for QGM to your users according to the tasks they have to perform. See *Scenario-Specific Guide for QGM*.

## Business Process Change Analyzer

For BPCA integration, you need to add additional BPCA roles, depending on which BPCA functionality, see *Scenario-Specific Guide for Business Process Change Analyzer*.

## Configuration Validation

See *Scenario - Specific Guide for Configuration Validation*.

## Project Management

For ITPPM integration, you need to add additional ITPPM roles. Specifically, authorization object `S_TABU_DIS` with value `SMCP` (protecting integration data between PPM and Change Request Management) is required. You can either add this authorization manually to your users or add role `SAP_SM_ITPPM_DIS`. For more information, see *Scenario-Specific Guide for Process Management* section *Project Management*.

## 7.5.4 Users and Authorizations

### 7.5.4.1 Users and Roles Change Request Management

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for Change Request Management. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information about User Interface authorizations, see *Authorization Concept Guide*. The tables underneath give you a further overview, which single roles are included in the respective composite roles. Since the *Overview* in a work center always contains all links to the relevant sections in the navigation panel, it is not mentioned.

#### Authorization for Trusted RFCs between SAP Solution Manager, Managed Systems, and BW - System

Trusted authorizations are needed between SAP Solution Manager and its managed systems, as well as SAP Solution Manager and a remote BW - system.

- In case of a remote BW - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object `S_RFCACL` (role `SAP_SM_S_RFCACL`; Help Text-ID: `AUTH_SAP_S_SM_RFCACL`). The user in the BW - system is also assigned authorization `S_RFCACL` (role `SAP_SM_BW_S_RFCACL`; Help Text-ID: `AUTH_SAP_S_SM_RFCACL`).
- The user in the managed system receives role `SAP_SM_S_RFCACL` (Help Text-ID: `AUTH_SAP_S_SM_RFCACL`) with authorization object `S_RFCACL`.

Both roles are not contained in the respective composite roles, due to their highly security-relevant character.

#### Requester (Help Text-ID: TP\_CM\_REQ)

#### Single Roles for Requester (technical composite role name: SAP\_CM\_REQUESTER\_COMP) in the SAP Solution Manager System

Table 217

Role	Help Text-ID
<code>SAP_SMWORK_CHANGE_MAN</code>	<code>AUTH_SAP_SMWORK_CHANGE_MAN</code>
<code>SAP_SM_CRM_UIU_FRAMEWORK</code>	<code>AUTH_SAP_SM_CRM_UIU_FRAME</code>
<code>SAP_SM_CRM_UIU_SOLMANPRO</code>	<code>AUTH_SAP_SM_CRM_UIU_SOLMAN</code>
<code>SAP_SM_CRM_UIU_SOLMANPRO_CHARM</code>	<code>AUTH_SAP_SM_CRM_UIU_CHARM</code>
<code>SAP_SOCM_REQUESTER</code>	<code>AUTH_SAP_SOCM_REQ</code>
<code>SAP_ITCALENDER_DIS</code>	<code>AUTH_SAP_ITCALENDER</code>
<code>SAP_SYSTEM_REPOSITORY_DIS</code>	<code>AUTH_SAP_SYSTEM_REP_DIS</code>

Role	Help Text-ID
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS

### Change Manager (Help Text-ID: TP\_CH\_CM)

Single Roles for Change Manager (technical role name: SAP\_CM\_CHANGE\_MANAGER\_COMP) in the SAP Solution Manager System

Table 218

Role	Help Text-ID
SAP_CM_SMAN_CHANGE_MANAGER	AUTH_SAP_CM_SMAN_CM
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SOCM_CHANGE_MANAGER	AUTH_SAP_SOCM_CM
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS

### Technical composite role name: SAP\_SM\_BW\_CHARM\_DISPLAY\_COMP in the BW system

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID in the BW system.

Table 219

Single Roles	Help Text ID
SAP_BI_E2E_CHARM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Table 220

Assigned Role	Help Text-ID
SAP_CM_MANAGED_CHANGE_MANAGER	AUTH_SAP_CM_MANAGED_CHANGE
SAP_CM_MANAGED_IMPORT	AUTH_SAP_CM_MANAGED_IMPORT

## Developer (Help Text-ID: TP\_CM\_DEV)

### **i** Note

For import authorizations, see SAP Note [807228](#).

## Single Roles for Developer (technical role name: SAP\_CM\_DEVELOPER\_COMP) in the SAP Solution Manager System

Table 221

Role	Help Text-ID
SAP_CM_SMAN_DEVELOPER	AUTH_SAP_CM_SMAN_DEVELOP
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SOCM_DEVELOPER	AUTH_SAP_SOCM_DEVELOPER
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS

### Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Table 222

Assigned Role	Help Text-ID
SAP_CM_MANAGED_DEVELOPER	AUTH_SAP_CM_MANAGED_DEVELOP
SAP_CM_MANAGED_DEVELOPER_RETRO	Additional role for functionality of Retrofit. Needs to be assigned manually.
SAP_CM_MANAGED_IMPORT	AUTH_SAP_CM_MANAGED_IMPORT
SAP_CM_MANAGED_CTS_DEV	AUTH_SAP_CM_MANAGED_DEVELOP

## Tester (Help Text-ID: USER\_TP\_CH\_TESTER)

### Note

For import authorizations, see SAP Note [807228](#).

## Single Roles for Tester (technical role name: SAP\_CM\_TESTER\_COMP) in the SAP Solution Manager System

Table 223

Role	Help Text-ID
SAP_CM_SMAN_TESTER	AUTH_SAP_CM_SMAN_TESTER
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SOCM_TESTER	AUTH_SAP_SOCM_TESTER
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS

### Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Table 224

Assigned Role	Help Text-ID
SAP_CM_MANAGED_TESTER	AUTH_SAP_CM_MANAGED_TESTER
SAP_CM_MANAGED_IMPORT	AUTH_SAP_CM_MANAGED_IMPORT

## IT-Operator (Help Text-ID: TP\_CM\_OPERATOR)

### Single Roles for IT-Operator (technical role name: SAP\_CM\_OPERATOR\_COMP) in the SAP Solution Manager System

Table 225

Role	Help Text-ID
SAP_CM_SMAN_OPERATOR	AUTH_SAP_CM_SMAN_OPERATOR
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN

Role	Help Text-ID
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SOCM_IT_OPERATOR	AUTH_SAP_SOCM_OPERATOR
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS

**Technical composite role name: SAP\_SM\_BW\_CHARM\_DISPLAY\_COMP in the BW system**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID in the BW system.

Table 226

Single Roles	Help Text ID
SAP_BI_E2E_CHARM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

**Role in the Managed System**

The role must be assigned to the user with the same user ID in the managed system.

Table 227

Assigned Role	Help Text-ID
SAP_CM_MANAGED_OPERATOR	AUTH_SAP_CM_MANAGED_OPERATOR
SAP_CM_MANAGED_CTS_ADOF	AUTH_SAP_CM_MANAGED_ADMIN

**Administrator (Help Text-ID: TP\_CH\_ADMIN)**

**Single Roles for Administrator (technical role name: SAP\_CM\_ADMINISTRATOR\_COMP) in the SAP Solution Manager System**

Table 228

Role	Help Text-ID
SAP_CM_SMAN_ADMINISTRATOR	AUTH_SAP_CM_SMAN_ADMIN
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_CPR_PROJECT_ADMIN	AUTH_SAP_CPR_PROJECT_ADMIN
SAP_CPR_USER	AUTH_SAP_CPR_USER
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME



Role	Help Text-ID
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_ADMIN	AUTH_SAP_SM_CRM_UIU_ADMIN
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SOCM_ADMIN	AUTH_SAP_SOCM_ADMIN
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER
SAP_SM_DSH	AUTH_SAP_SM_DSH
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SYSTEM_REPOSITORY_EXE	AUTH_SAP_SYSTEM_REP_ALL
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS

#### Technical composite role name: SAP\_SM\_BW\_CHARM\_ADMIN\_COMP in the BW system

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID in the BW system.

Table 229

Single Roles	Help Text ID
SAP_BI_E2E_CHARM	AUTH_SAP_BI_E2E
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

#### Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Table 230

Assigned Role	Help Text-ID
SAP_CM_MANAGED_ADMIN	AUTH_SAP_CM_MANAGED_ADMIN
SAP_CM_MANAGED_CTS_ADOP	AUTH_SAP_CM_MANAGED_ADMIN

#### Release Manager (Help Text-ID: TP\_CH\_RM)

##### Single Roles for Release Manager (technical role name: SAP\_CM\_RELEASE\_MANAGER\_COMP) in the SAP Solution Manager System

Table 231

Role	Help Text-ID
SAP_CM_SMAN_RELEASE_MANAGER	AUTH_SAP_CM_SMAN_RM
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME

Role	Help Text-ID
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SOCM_RELEASE_MANAGER	AUTH_SAP_SOCM_RM
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS

### Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Table 232

Assigned Role	Help Text-ID
SAP_CM_MANAGED_RELEASEMAN	AUTH_SAP_CM_MANAGED_RELEASE
SAP_CM_MANAGED_IMPORT	AUTH_SAP_CM_MANAGED_IMPORT

## 7.5.4.2 Best Practice: Manage Import Authorizations in Managed Systems

Import authorizations are necessary in the Change Management process. It allows Business users to being able to automatically create transport requests and import transports from a source system into a target systems. The authorization object required is S\_CTS\_ADMI. If you use cluster or non-ABAP systems in TMS communication systems, we recommend to use the equivalent authorization object S\_CTS\_SADM instead. Authorization object S\_CTS\_SADM allows you to additionally restrict on systems and domains.

### Prerequisites

You are using delivered Standard Roles SAP\_CM\_MANAGED\_\* for users in your managed systems. These roles contain specific security-critical authorizations for the individual Business users, which should be handled separately.

## Procedure

We recommend two alternatives for handling these security-critical authorizations, depending on your level of security protection for your systems:

- a) Use Existing Standard Roles for Managed Systems (assigned import authorization)
- b) Use Delivered Import Role `SAP_CM_MANAGED_IMPORT`

### Use Existing Standard Roles

Use the existing roles for users with additional import authorizations.

### Use Delivered Import Role `SAP_CM_MANAGED_IMPORT`

This practice allows you to use role `SAP_CM_MANAGED_IMPORT` for any Business User required. This role contains all required import authorizations needed.

#### Caution

The above roles should only be assigned to the following users in the respectively mentioned systems, but never in production systems or security relevant systems:

- Developers in consolidation systems
- Testers in all test systems
- Change Managers in consolidation systems

A combination of authorization object `S_DATASET` and `S_CTS_ADMI` with value `IMPA` and `EPS1` can jeopardize security in your system. You should only use this practice if you require a smooth Change Request Management process.

## 7.5.4.3 User Roles for Additional Functions

### 7.5.4.3.1 User Roles for Retrofit

To be able to execute *Retrofit* functionality the developer needs additional authorizations in the managed system. You need to assign role `SAP_CM_MANAGED_DEVELOPER_RETRO` to the “developer” user. Check the user definition for the developer in your Solution Manager system, transaction `SOLMAN_SETUP`, guided procedure for *Change Request Management*.

### 7.5.4.3.2 User Roles for Communication Systems

In the communication systems, you require the same roles as for your managed systems. See section *Users and Authorizations*.

## 7.5.4.3.3 CTS-Integration User Roles in the SAP Solution Manager

You can use CTS with *Change Request Management*. To be able to use this integration, assign the following roles to your SAP Solution Manager users.

### RFC - Destinations

You require:

- TMW – RFC destination
- TMS Deploy destination (TMSDPL@SID.DOMAIN)

### Developer - Transport Authorization (technical role name: SAP\_BC\_CCTS\_CHARM\_DEVELOP\_TMPL)

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- trigger imports (system-specific and cluster-specific)
- create, change, delete, and release collections (system-specific and cluster-specific)

### IT Operator - Transport Authorization (technical role name: SAP\_BC\_CCTS\_CHARM\_OPERAT\_TMPL)

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- trigger imports (system-specific and cluster-specific)
- create, change, delete, and release collections (system-specific and cluster-specific)
- change import queues

### Change Manager - Transport Authorization (technical role name: SAP\_BC\_CCTS\_CHARM\_CH\_MGR\_TMPL)

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- trigger imports (system-specific and cluster-specific)
- create, change, delete, and release collections (system-specific and cluster-specific)
- change import queues

### Administrator - Transport Authorization (technical role name: SAP\_BC\_CCTS\_CHARM\_ADMIN\_TMPL)

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- trigger imports (system-specific and cluster-specific)

- create, change, delete, and release collections (system-specific and cluster-specific)
- change import queues

### Tester - Transport Authorization (technical role name: SAP\_BC\_CCTS\_CHARM\_TESTER\_TMPL)

This role allows the user to:

- create projects in CTS (system-specific and cluster-specific)
- create and delete import locks (system-specific and cluster-specific)
- trigger imports (system-specific and cluster-specific)
- create, change, delete, and release collections (system-specific and cluster-specific)

## 7.5.4.3.4 Users and Roles Requirement Management

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for *Requirement Management*.

### Process Description

1. The Business Process Expert or a Business Manager have received a new requirement from the business department. They create and describe the business requirement (BR) document, the target release as well as important attributes of the requirement.
2. Using multiple status, the description of the BR is checked and validated. It can then be handed over to the IT Department. At this point of time, the IT Requirement (ITR) document is created. The ITR document contains all the information of the requirement description.
3. The requirement is validated on the ITR document from a technical perspective for technical feasibility and capacity of developers in the IT department. After the validation, the IT department commits itself to implement the requirement on the specific time, cost, and method.
4. After the commitment from IT department, the business side commits itself to 'purchase' the requirement to the specific conditions specified in the BR.
5. Then, the IT department can start with implementing the requirement using one of the following procedures:
  1. Creating a project (ITR is closed). This is for extensive requirements, like upgrades of systems, and so on. The changes are then triggered from the ITPPM project.
  2. Creating a Request for Change and closing the ITR. This is the implementation of the change via maintenance, for smaller requirements.
  3. Creating changes directly from the ITR, mostly for smaller to midsize requirements.

### System Landscape/Data Flow

The Requirements Management process runs locally on the SAP Solution Manager. End users log on to the *CRM Web Client* on SAP Solution Manager to access Requirements Management.

### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information about User Interface authorizations, see *Authorization Concept Guide*.

IT Requirement itself is displayed within the Work Center as it functions as Request for Change for Innovation. On the other hand, Business Requirement is not visible in the Work Center, but in the CRM WebClient and SAP Fiori Application.

## Configuration

### Transaction SOLMAN\_SETUP

You can configure the scenario using transaction SOLMAN\_SETUP. When you call the procedure view *Requirement Management*, the system asks you to create a specific configuration user. You can create this user SMC\_RM\_\*\*\*, or you can add the suggested user roles to another user.

### Configuration User SMC\_RM\_\*\*\* (Help TXT: USER\_CONFIG\_RM)

#### Single Roles (technical composite role name: SAP\_RM\_CONF\_COMP)

Table 233

Role	Help Text-ID
SAP_RM_CONFIG	AUTH_SAP_RM_CONFIG
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_ITADM	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_SM_CRM_UIU_SOLMANREQU_BRAD	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_TREX_ADMIN	AUTH_SAP_SM_TREX_ADMIN
SAP_SM_ESH_ADMIN	AUTH_SAP_SM_ESH_ADMIN
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

### Business Manager: RM\_BM\_\*\*\* (Help TXT: TP\_RM\_BM)

#### Single Roles (technical composite role name: SAP\_RM\_BUSINESS\_MANAGER\_COMP)

Table 234

Role	Help Text-ID
SAP_RM_BUSINESS_MANAGER	AUTH_SAP_RM_BUSINESS_MANAGER
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANREQU	AUTH_SAP_SM_CRM_UIU_SOLMAN

Role	Help Text-ID
SAP_SM_CRM_UIU_SOLMANREQU_RMBM	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

### Business Process Expert: RM\_BPE\_\*\*\* (Help TXT: TP\_RM\_BPE)

#### Single Roles (technical composite role name: SAP\_RM\_BP\_EXPERT\_COMP)

Table 235

Role	Help Text-ID
SAP_RM_BP_EXPERT	AUTH_SAP_RM_BP_EXPERT
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANREQU	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANREQU_BEX	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

### Business Process Administrator: RM\_BRADM\_\*\*\* (Help TXT: TP\_RM\_BRADM)

#### Single Roles (technical composite role name: SAP\_RM\_BR\_ADMIN\_COMP)

Table 236

Role	Help Text-ID
SAP_RM_BR_ADMIN	AUTH_SAP_RM_BR_ADMIN
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANREQU	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANREQU_BRAD	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS

Role	Help Text-ID
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_PPR_PPM

### IT Requirements Manager: RM\_MAN\_\*\*\* (Help TXT: TP\_RM\_MAN)

#### Single Roles (technical composite role name: SAP\_RM\_ITREQ\_MANAGER\_COMP)

Table 237

Role	Help Text-ID
SAP_RM_ITREQ_MANAGER	AUTH_SAP_RM_ITREQ_MANAGER
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_RM	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

### Solution Architect: RM\_SOLA\_\*\*\* (Help TXT: TP\_RM\_SOLA)

#### Single Roles (technical composite role name: SAP\_RM\_SOL\_ARCHITECT\_COMP)

Table 238

Role	Help Text-ID
SAP_RM_SOL_ARCHITECT	AUTH_SAP_RM_SOL_ARCHITECT
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_SOLA	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED



Role	Help Text-ID
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

## IT Requirements Administrator: RM\_ITADM\_\*\*\* (Help TXT: TP\_RM\_ITADM)

### Single Roles (technical composite role name: SAP\_RM\_ITREQ\_ADMIN\_COMP)

Table 239

Role	Help Text-ID
SAP_RM_ITREQ_ADMIN	AUTH_SAP_RM_ITREQ_ADMIN
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_ITADM	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

## Display User: RM\_DISP\_\*\*\* (Help TXT: TP\_RM\_DISP)

### Single Roles (technical composite role name: SAP\_RM\_DISPLAY\_COMP)

Table 240

Role	Help Text-ID
SAP_RM_DISPLAY	AUTH_SAP_RM_DISPLAY
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANPRO	AUTH_SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_RM_DISPALY	AUTH_SAP_SM_CRM_UIU_DELTA
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

## Specific Authorization Objects

### S\_DATASET

The authorization object activity field contains `ACTVT 06` (delete). The objects allows, that attachments which are added in the *Attachment* Assignment Block can be deleted.

### Application Log

Application logs are restricting the relevant document (like `BR` document and `ITR` document). In these documents, the log is displayed in the *Text* Assignment Block. In addition, transaction `SLG1` is accessible for administrators to check logs. Authorization object `S_APPL_LOG` allows log display of the following application objects and its subobjects:

- `CRM_SMF`
- `CRM_DOCUMENT`
- `PPF`

### Scenario Integration

- Change Request Management as follow-up process
- `ITPPM` (optional), see application-specific section for *Process/Solution Documentation*

## 7.5.4.4 Main Authorization Objects

This section gives you an overview over the main authorization objects.

### General Information

Roles `SAP_SOCM_*` and `SAP_CM_SMAN_*` are maintained according to profile generator default values for all `ST` - relevant transactions. The following transactions contain values according to Software Component `SAP_ABA` and `BBPCRM`: `SCMA`, `CRMD_ORDER`, `CRM_DNO_MONITOR`. Therefore, all `CRM` - objects, `TMWFLOW` - objects, `PPF` objects, and authorization object `S_PROGRAM` appear in status *manual* within the roles.

Roles `SAP_CM_SMAN_*` contain a number of `/TMWFLOW/` - authorization objects with status `MANUAL` due to transaction `SCMA`. Authorization object `B_BUPA_RTL` and `CRM` authorizations are set inactive in `SAP_CM_SMAN*` as all `BP` authorization are contained in roles `SAP_SOCM_*`.

In `SAP_SOCM_*` roles, development environment authorizations are set inactive. `SAP_SOCM_*` roles contain `BP` authorizations, product master authorizations, status change authorizations, `HR` authorizations such as authorization object `PLOG`, and all relevant `CRM` - authorizations.

As *Change Request Management* is highly integrated into `CRM`, see section on `CRM` integration in the *Authorization Concept Guide*.

### CRM Authorization Objects

Roles for *Change Request Management* contain `CRM` - authorizations. For more information on `CRM` - authorization objects, see *Authorization Concept Guide*, section on `CRM` integration.

## Authorization Objects B\_USERST\_T and B\_USERSTAT (status change)

In the roles for *Change Request Management*, the authorization object B\_USERST\_T (status of a previous change document can only be set by the system) is used instead of B\_USERSTAT (The status of the change document is influenced by the user).

## Authorization Object S\_RFC (RFC access)

Roles for the managed system contain authorization object S\_RFC. The authorization object contains values with added asterisk (\*). The field length of the authorization field for these function groups is not efficient with SAP\_BASIS Release 4.6C.

## Authorization Object S\_TABU\_DIS (table access)

In user roles for *Change Request Management*, you find authorization object S\_TABU\_DIS. Authorization group CRMC protects all relevant customizing views and customizing clusters for this scenario.

## Authorization Object S\_TABU\_NAM

S\_TABU\_NAM is set inactive in all roles. If you require to restrict access to specific tables, the object can be set active in the roles. The object is always checked if authorization object S\_TABU\_DIS is not active.

## Authorization Object SM\_CM\_FUNC

This object replaces authorization objects S\_PROJECT and S\_PROJ\_GEN for *Release Cycles*. The objects contain fields for Solution Name and Branch. These fields are also contained in *Process Documentation* authorization objects.

## Authorization Object SM\_CM\_DGPN

This object replaces authorization objects SM\_CM\_DGP and SM\_CM\_CSOL for *Downgrade Protection* authorization. The object contains fields for *Solution Name* and *Branch*. These fields are also contained in *Process Documentation* authorization objects.

## Authorization Object /TMWFLOW/M

This authorization object controls in which phase cycle a user can work. With Release 7.2, the release cycle and phase model are newly defined, therefore the values for this authorization object have changed completely in contrast to Release 7.1.

## Authorization Object PLOG

The authorization object is relevant for Organization Levels for Human Resources (HR). If you work with HR Organization Levels for Business Users, you need to activate the authorization objects PLOG as well as P\_TCODE, and maintain the according values.

## 7.5.5 System Recommendations

The single tabs for SAP Notes can be restricted (authorization object SM\_FUNCS).

The following roles are needed in addition to the existing composite roles for *Change Request Management* or *Configuration Validation*:

## Administrator (technical role name: SAP\_SYSTEM\_RECOMMEND\_COMP)

Table 241

Single role	Restriction on
SAP_SYSREC_ALL	Full authorization for System Recommendations tab
SAP_SM_SL_EDIT	Maintenance authorization for processes
SAP_SYSTEM_REPOSITORY_ALL	Full authorization for systems, host, and so on
SAP_SMWORK_CHANGE_MAN	Allows access to the Change Management work center
SAP_SM_FIORI_LP_EMBEDDED	Allows SAP Fiori Launchpad access

## Administrator (technical role name: SAP\_SYSTEM\_RECOMMEND\_DIS\_COMP)

Table 242

Single role	Restriction on
SAP_SYSREC_DIS	Display authorization for System Recommendations tab
SAP_SM_SL_DISPLAY	Display authorization for processes
SAP_SYSTEM_REPOSITORY_DIS	Display authorization for systems, host, and so on
SAP_SMWORK_CHANGE_MAN	Allows access to the Change Management work center
SAP_SM_FIORI_LP_EMBEDDED	Allows SAP Fiori Launchpad access

## Authorization Groups for S\_TABU\_DIS

All tables relevant for System Recommendation are secured by authorization group SMSR.

## 7.5.6 Integration of SAP Fiori Applications

Here you find specific information on the individually delivered applications that can be used on a Central Fiori Hub.

### **i** Note

General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the security guide for the Authorization Concept for Solution Manager.

### APP: My Requirements

This application allows users to create, edit, and display Business Requirements. Users, can do the following:

- View the details of their Incidents: Details include short text, long texts (restricted by authorization object CRM\_TXT\_ID authorizations), status, priority, attachments, and so on.

- Send an answer back to the Incident processor. This implicitly changes the status of the Incident to *In Process*.
- Add attachments such as Word documents, screen shots, and so on.
- Confirm or withdraw the Incident when they are finished with the Incident.

### Authorizations in the Back-end SAP Solution Manager

The relevant Odata - Service is added to the core roles for the *Business Process Expert* (maintain and create) and *Business Manager* (determine priorities and decide realization) for Requirement Management .

In the back-end SAP Solution Manager system assign the relevant composite roles for these users. Due to the nature of the application, as a subset of the complete functionality of Requirement Management, not all authorizations in these roles are required. If your security does not allow this many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_RM*` role accordingly, remove all roles relating to CRM WebClient, as well as BW-related roles.

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

#### **i** Note

As you can modify SAP Fiori Apps to your own purpose, we do not deliver any specifically predefined roles for them.

### Authorizations in the Frond-end

The following two roles are delivered for front-end usage for the application:

- `SAP_STUI_ITSM_MYREQ_TCR`  
This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_ITSM_MYREQ_AUTH`  
This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, do the following:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

### App: My System Recommendations

This application allows users to view SAP Notes. It completely substitutes the former Web-based application for System Recommendation.

### Authorizations in the Back-end SAP Solution Manager

The relevant Odata - Service is added to the core roles for the System Recommendation application.

In the back-end SAP Solution Manager system assign the relevant composite role `SAP_SYSTEM_RECOMMENDATIONS_COMP` to the user or create the template user via transaction `SOLMAN_SETUP`.

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

## Authorizations in the Frond-end

The following two roles are delivered for front-end usage for the application:

- SAP\_STUI\_ITSM\_SYSREC\_TCR

This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.

- SAP\_STUI\_ITSM\_SYSREC\_AUTH

This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, do the following:

1. Copy the Odata service into your name space.
2. Add the copied service to your role *Menu*.
3. Check that authorization object S\_SERVICE is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

## 7.6 Scenario-Specific Guide: Configuration Validation

### 7.6.1 Prerequisites

To use configuration validation, you need to have *Root Cause Analysis* configured, see *Landscape Setup Guide*.

#### Technical System Landscape

##### Technical Infrastructure

- Configuration Validation

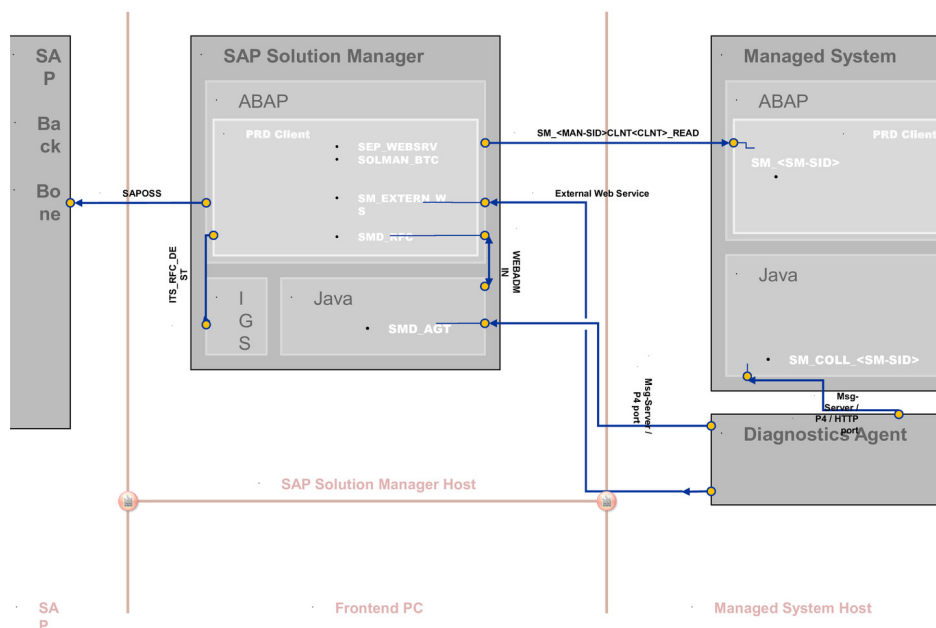


Figure 13: Technical Landscape Overview

## 7.6.2 Users and Authorizations

### 7.6.2.1 User Descriptions and User Roles in the SAP Solution Manager

This paragraph gives an overview over users as recommended by SAP and their according user roles. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WD_COMP`. For more information about User Interface authorizations, see [Authorization Concept Guide](#).

The tables underneath give you a further overview, which single roles are included in the respective composite roles. In the work center, you find the configuration validation function in section [Related Links](#).

#### Administrator (Technical Role Name: SAP\_CV\_ADMIN\_COMP)


Table 243

Single Roles	Restriction on
SAP_CV_ALL	Full authorization for Configuration Validation, especially Report Directory  <b>i Note</b> Authorization object <code>AI_CCDB_SC</code> is set inactive in the role. The authorization restricts access to the User ConfigStores, and therefore security-relevant data. If you allow your administration user to read these data, set the authorization object active in this role.
SAP_SYSTEM_REPOSITORY_DIS	Display authorization for System Repository (LMDB)
SAP_SMWORK_CHANGE_MAN	Access to work center Change Management
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori Launchpad
SAP_BI_E2E	BI - Reporting authorizations.
SAP_SM_BI_ADMIN	<b>! Caution</b> If the BI - scenario is remote, these roles have to be assigned to the BI - user in the remote system in addition with authorization object <code>S_RFCACL</code> .

#### Display User (Technical Role Name: SAP\_CV\_DISPLAY\_COMP)

Table 244

Single Roles	Remarks
SAP_CV_DIS	Display authorization for Configuration Validation, especially Report Directory

Single Roles	Remarks
SAP_SYSTEM_REPOSITORY_DIS	Display authorization for System Repository (LMDB)
SAP_SMWORK_CHANGE_MAN	Access to work center Change Management
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori Launchpad
SAP_BI_E2E	BI - Reporting authorizations.
SAP_SM_BI_DISP	 <b>Caution</b> If the BI - scenario is remote, these roles have to be assigned to the BI - user in the remote system in addition with authorization object S_RFCACL.

## 7.6.2.2 Critical Authorizations

The following authorization objects are checked for *Configuration Validation*:

### AI\_CCDB\_SC (Store Content)

The Configuration Change Database (CCDB), transaction CCDB, contains configuration data of the managed systems in so called ConfigStores. The authorization object AI\_CCDB\_SC controls which protected ConfigStore content can be accessed by a user. Only ConfigStores which are defined to be protected are checked. All other not protected ConfigStores are available for all users. Refer to the documentation how to protect a ConfigStore of CCDB.

#### Note

If you use RFC BI\_CALLBACK with scenario Configuration Validation, activate authorization object AI\_CCDB\_SC to be able to read data from the User ConfigStore.

### AI\_CCDB\_CU

There are a few ConfigStores containing customizing which can influence the content of a ConfigStore. The authorization object restricts this customizing access.

## 7.7 Additional Security Measures

Consider the following actions for additional measures in regard to preventing security breaches and reacting to according events.

### Activate Logging of Major Configuration Tables

The activation of table logs for configuration tables allows you to determine at which time a user has changed specific values that are important for the configuration settings of your application.



## ➔ Recommendation

We highly recommend logging of at least major configuration tables.

For the following tables the flag *Log Data Changes* is set by SAP:

- AGS\_WORK\_CUSTOM (AGS: Work Centers Customizing)
- In case of external interface: ICT\_CUSTOM (SM SD Interface: System Configuration)

We recommend you to activate logging for the following table:

- DNOC\_USERCFG (Service Desk Customizing)

### Steps to Activate Table Logging

1. Set *Log Data Changes* for the required tables using transaction SE13.
2. Set parameter value for parameter: `rec/client`.

### How-to Information

For detailed information on logging, how-to activate logging of tables, and its system requirements, see on the Service Marketplace: ► [help.sap.com/saphelp\\_nw74/helpdata/en/4d/b6d15036311dcee10000000a42189c/frameset.htm](https://help.sap.com/saphelp_nw74/helpdata/en/4d/b6d15036311dcee10000000a42189c/frameset.htm) ↗ ↘.

See also SAP Note [1916](#) ↗.

### Virus Scanning for Attachments

## ➔ Recommendation

We recommend to use ABAP Virus Scanning Interface (VSI) for virus scans of attachments.

In Incident Management 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.

# 8 Custom Code, DVM, and Value Management Dashboard

## 8.1 Document History

Here, all changes to the specific scenario guide are listed according to Support Package.

Table 245

Support Package Stacks (Version)	Description
SP01	<p><b>General Adaptations</b></p> <ul style="list-style-type: none"> <li>Roles SAP_SM_BI_BILO and SAP_SMWORK_BASIC_* obsolete.</li> <li>All roles for have been adapted to the new functionality of <i>Process Documentation</i> and SAP_BASIS 7.40.</li> <li>Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_* has been transferred into core authorization roles.</li> </ul> <p><b>SAP Fiori Integration</b></p> <ul style="list-style-type: none"> <li>All users receive SAP Fiori Launchpad authorization role SAP_SM_FIORI_LP_EMBEDDED</li> </ul> <p><b>Data Migration</b></p> <ul style="list-style-type: none"> <li>You can run data migration for CCM using application <i>Custom Code Management Migration</i> within transaction SOLMAN_SETUP in the <i>Related Links</i> area.</li> </ul> <p><b>Value Management Dashboard (iCI)</b></p> <ul style="list-style-type: none"> <li>new configuration user SMC_ICI_*** available, and according roles</li> </ul>
SP02	<p><b>DVM</b></p> <p>Adapted authorization objects are described within the <i>Menu</i> tab of the respective roles</p> <ul style="list-style-type: none"> <li>adapted roles SAP_DVM*_COMP</li> </ul> <p><b>CCM</b></p> <p>Adapted authorization objects are described within the <i>Menu</i> tab of the respective roles</p> <ul style="list-style-type: none"> <li>adapted roles SAP_CCLM*_COMP</li> <li>adapted single role SAP_CCLM_ALL</li> <li>adapted single role SAP_SM_CCM_CONFIG</li> <li>added role SAP_SM_DASHBOARDS_ADMIN to CCM_ADM* user, composite role SAP_CCLM_ALL_COMP (to be able to configure Dashboards)</li> </ul> <p><b>Ici - Dashboard (Value Management)</b></p> <p>Adapted authorization objects are described within the <i>Menu</i> tab of the respective roles</p>

Support Package Stacks (Version)	Description
	<ul style="list-style-type: none"> <li>Added Work Center navigation role for SAP Engagement and Services to Ici users:SAP_SMWORK_SERVICE_DEV</li> <li>Adapted BI - role SAP_BI_ICI</li> </ul>
SP03	<p><b>CCM</b></p> <p>Adapted authorization objects are described within the <i>Menu</i> tab of the respective roles</p> <ul style="list-style-type: none"> <li>adapted single role SAP_CCLM_ALL (authorization object S_DEVELOP)</li> <li>adapted single role SAP_SMWORK_CCLM</li> </ul> <p><b>DVM</b></p> <p>Adapted authorization objects are described within the <i>Menu</i> tab of the respective roles</p> <ul style="list-style-type: none"> <li>adapted role SAP_DVM_CONFIG</li> <li>adapted role SAP_DVM_ALL</li> <li>in case of Test Plan integration and BPCA, role SAP_SM_KW_ALL must be assigned to the DVM administration user</li> </ul>

## 8.2 Scenario-Specific Guide: Custom - Code Life Cycle Management

### 8.2.1 Getting Started

**What is this guide about?** SAP Solution Manager covers a wide range of divers scenarios you can use. As a customer, you might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides per scenario which cover all relevant information for this specific scenario.

#### Caution

Before you start using this scenario-specific guide, you must read the core information about security issues in SAP Solution Manager, and the *Secure Configuration Guide*, which refers to all security-relevant information during basic configuration of SAP Solution Manager. Without this information, we do not recommend to set up any specific scenario. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

This guide covers the following topics:

- **Getting Started:** find out about target groups of this guide. Links for any additional components can be found in the Core Guide.
- **Prerequisites:** find out about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other.

- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).

## Custom Code Life-Cycle Management Use Cases

### ATC Monitoring and Exemption Monitoring Integration

It allows to extract ATC messages and exemptions for transparency on the quality dimension of custom code objects. The Development Manager needs to have central access to all kinds of exemptions within a system landscape.

## 8.2.2 Prerequisites

### 8.2.2.1 Technical System Landscape and Data Migration

The graphic below gives you an overview over the basic technical system landscape that is needed to run the CCLM scenario. The SAP Solution Manager is connected via READ - RFC, to your managed systems. For more information about the connection, when it is used, and which technical user is required, you can find out in the following sections.

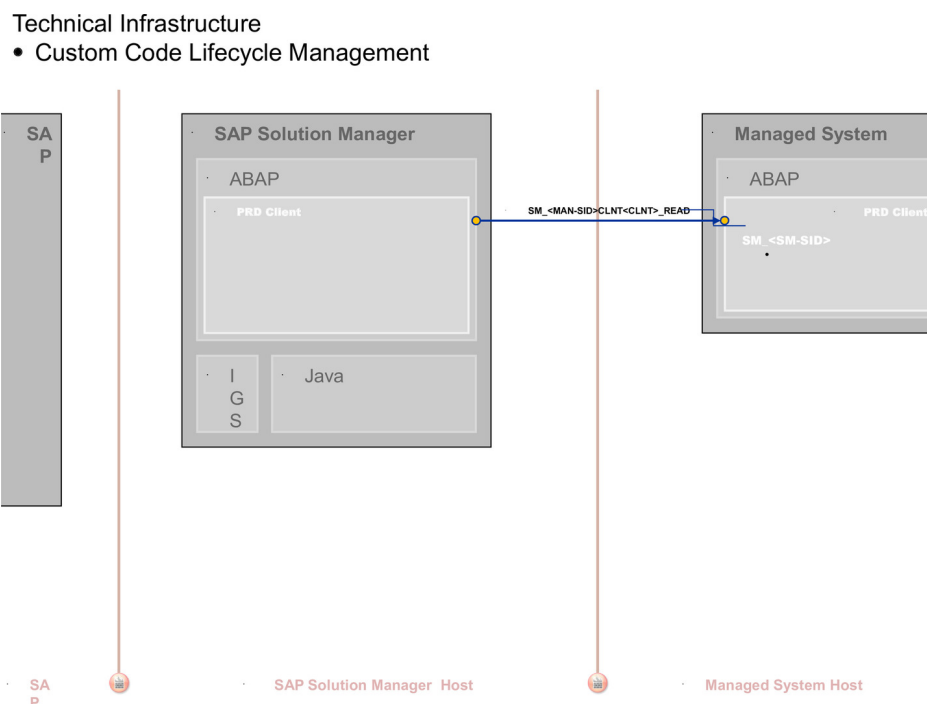


Figure 14: CCLM Technical System Landscape

### Data Migration from Release 7.1 to Release 7.2

The data migration in CCM is required to move from solutions to the new process management.

When calling transaction `SOLMAN_SETUP`, the Migration Wizard for CCM Data Migration appears as a link in the *Related Link* area. You need to perform this activity after upgrade/installation, and prior to configure/update your CCM scenario. You can run the Data Migration with the template user for administration for CCM. You can find

this user in the guided procedure for CCM in a separate step or choose to assign the delivered composite role for it in transaction `PECG`. For more information on template users for CCM, see the according section in this guide.

## Data Migration Application Flow

The Migration application runs on the Solution Manager system and connects to:

- the managed systems in order to schedule background processes and alter specific settings if required
- the BW server to perform data migration from/to Infocubes and DSOs
- the Solution Manager system, locally, to activate extractors and collectors within the EFWK framework. It also alters specific database tables and DDIC objects.

## ATC and Exemption Monitoring Integration

ATC and Exemption Monitoring uses the Extractor Framework (EFWK). The ATC extractor reads the data (messages and exemptions) via the EFWK from the managed systems via RFC function modules (technical user: `READ-user` and `READ RFC-connection`). The data is then uploaded into the BW-system/client. The ATC monitoring comprises two parts:

- The ATC messages monitoring displays data read from the BW-system/client.
- The ATC Exemptions monitoring displays data read from BW-system/client, but also allows users with special authorizations to update the exemptions on the remote system via RFC-connection.

## 8.2.2.2 Scenario Configuration User

### **i** Note

For conceptual information on:

- configuration users in SAP Solution Manager, see *Authorization Concept Guide* chapter *Configuration Users*.
- the BW integration concept, see *Authorization Concept Guide* chapter on *BW Integration*.

The scenario is configured using transaction `SOLMAN_SETUP`.

To configure the scenario proceed as follows:

### Creating Configuration User in Basic Configuration Transaction `SOLMAN_SETUP`

When you call the Guided Procedure for Custom Code Management, the system asks you to create a specific configuration user (default technical user name: `SMC_CCM_<XXXClient>`) for Custom Code Management (Help Text ID: `USER_CONFIG_IM`). You can either create a separate configuration user or use an existing user and add all required additional roles. The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

If you want to create the configuration user manually, you need to assign the composite role `SAP_CCM_CONF_COMP`, which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

Table 246

Single Role	Help TXT ID
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SMWORK_CCLM	AUTH_SAP_SMWORK_CCLM
SAP_SM_CCM_CONFIG	AUTH_SAP_SM_CCM_CONFIG
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REPOSITORY_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### **i** Note

To be able to:

- create users and assign user roles, you need to assign as well role `SAP_SM_USER_ADMIN`.
- use a trusted RFC connection between the Solution Manager and the managed systems, you need to assign role `SAP_SM_S_RFCACL` in the Solution Manager system as well as the managed system.

## Scenario Configuration Transaction `SOLMAN_SETUP`

You can configure the basic technical settings using transaction `SOLMAN_SETUP`, running the Guided Procedure for Custom Code Management for CCM.

During the specific guided configuration you can create *Template Users*. The system automatically adds all relevant user roles, see according sections on *Users and User Roles*.

## 8.2.2.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 247

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to managed systems and back	RFC	Reading information from managed systems
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes

## Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 248

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID of Solution Manager system>	Reads data from the managed system, such as object lists, usage information, code inspector data, version of program information, and so on

## 8.2.2.4 Technical Users

The technical user in the following table is created automatically during configuration. Technical users are of type *System User*. For more information on the individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

### User in Managed Systems

Table 249

User	Remarks
<i>Read - User</i>	SM_<SID of Solution Manager System>

## 8.2.3 Users and Authorizations

### 8.2.3.1 User Descriptions and User Roles in the SAP Solution Manager

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information about user interface authorizations, see [Authorization Concept Guide](#).

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

#### Authorization for Trusted RFC between SAP Solution Manager and BW - System

In case of a remote BW - connection, the user in the SAP Solution Manager system must be assigned trusted authorization object `S_RFCACL` (role `SAP_SM_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`). The user in the BW - system is also assigned authorization `S_RFCACL` (role `SAP_SM_BW_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`).

#### Administrator User ID: `CC_ADM_XXX` (Help Text ID: `TP_CC_ADMIN`)

Corresponding composite role: `SAP_CCLM_ALL_COMP` in the Solution Manager system

Table 250

Single Roles	Help Text ID
<code>SAP_CCLM_ALL</code>	<code>AUTH_SAP_CCLM_ALL</code>
<code>SAP_SMWORK_CCLM</code>	<code>AUTH_SAP_SMWORK_CCLM</code>
<code>SAP_SM_SL_DISPLAY</code>	<code>AUTH_SAP_SM_SL_DISPLAY</code>
<code>SAP_SYSTEM_REPOSITORY_DIS</code>	<code>AUTH_SAP_SYSTEM_REP_DIS</code>
<code>SAP_SM_FIORI_LP_EMBEDDED</code>	<code>AUTH_SAP_SM_FIORI_LP_EMBED</code>
<code>SAP_SM_DASHBOARDS_ADMIN</code>	<code>AUTH_SAP_SM_DASHBOARDS_ADMIN</code>

#### Technical composite role name: `SAP_BW_CCLM_ADMIN_COMP` in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID in the BW system.

Table 251

Single Roles	Help Text ID
<code>SAP_BI_CCM</code>	<code>AUTH_SAP_BI_E2E</code>



Single Roles	Help Text ID
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

Managed system role

Table 252

Single Roles	Remarks
SAP_CCA_ALL	CCA full authorizations

### Display User ID: CC\_DIS\_XXX (Help Text ID: TP\_CC\_DIS)

Corresponding composite role: SAP\_CCLM\_DISPLAY\_COMP in the Solution Manager system

Table 253

Single Roles	Help Text ID
SAP_CCLM_DISP	AUTH_SAP_CCLM_DISP
SAP_SMWORK_CCLM	AUTH_SAP_SMWORK_CCLM
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Technical composite role name: SAP\_BW\_CCLM\_DISPLAY\_COMP in the BW system/client

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID in the BW system.

Table 254

Single Roles	Help Text ID
SAP_BI_E2E_CCM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

## ATC Monitoring

ATC Monitoring can be used within CCM. The application authorization is included in the CCM-roles. If your security requires to separate the ATC application due to Segregation of Duty, you need to do the following:

1. Create a new role, and add the ATC Web Dynpro Applications to the roles.
2. Assign the new role to your user.
3. Assign the following roles in addition:
  - SAP\_SMWORK\_CCLM
  - SAP\_SYSTEM\_REPOSITORY\_\*

## Trusted RFC-Destination

ATC can also be used with LOGIN RFC-destination.

## 8.2.3.2 Authorizations

### Custom Code Management

#### Relevant WebDynpro Applications

- AGS\_CCL\_DEFINITION
- AGS\_CCL\_OBJECTS
- AGS\_CCL\_SETTINGS
- AGS\_CUSTOM\_CODE

Additionally, transaction CCLM calls the work center WDA.

#### Authorization Object SM\_CC\_AUT

The authorization object contains all relevant activities for CCLM. It is checked when the transaction (WDA) is initially called. If activities are restricted the according activity buttons in the application are disabled.

### ATC and Exemption Monitoring Integration

#### Authorization Object SM\_ATC\_APP

To separate the display of ATC messages and exemptions as well as to provide change access to work with exemptions, a special authorization is required.

Users with display authorization for SM\_ATC\_APP can access both, the ATC monitoring screen and the Exemption monitoring screens. However, in the Exemption monitoring screen, the buttons to validate or reject exemptions are greyed out. Users with administration authorization for SM\_ATC\_APP can access both ATC and Exemption monitoring screens. They can use the buttons to validate or reject the exemptions. The authorization object is included in standard roles for CCLM: SAP\_CCLM\_\*.

### Critical Authorizations

#### S\_DEVELOP

Within role SAP\_CCLM\_ALL authorization object S\_DEVELOP is included for package AGS\_CUSTOM\_CODE\_LIB with ACTVT 42 for creating z-attributes in Custom Code and write to the database.

## 8.3 Scenario-Specific Guide: Data Volume Management

### 8.3.1 Prerequisites

#### 8.3.1.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete scenario. The SAP Solution Manager is connected via READ - RFC, TRUSTED - RFC (alternatively LOGIN) to your managed systems. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.

Technical Infrastructure  
 • Data Volume Management

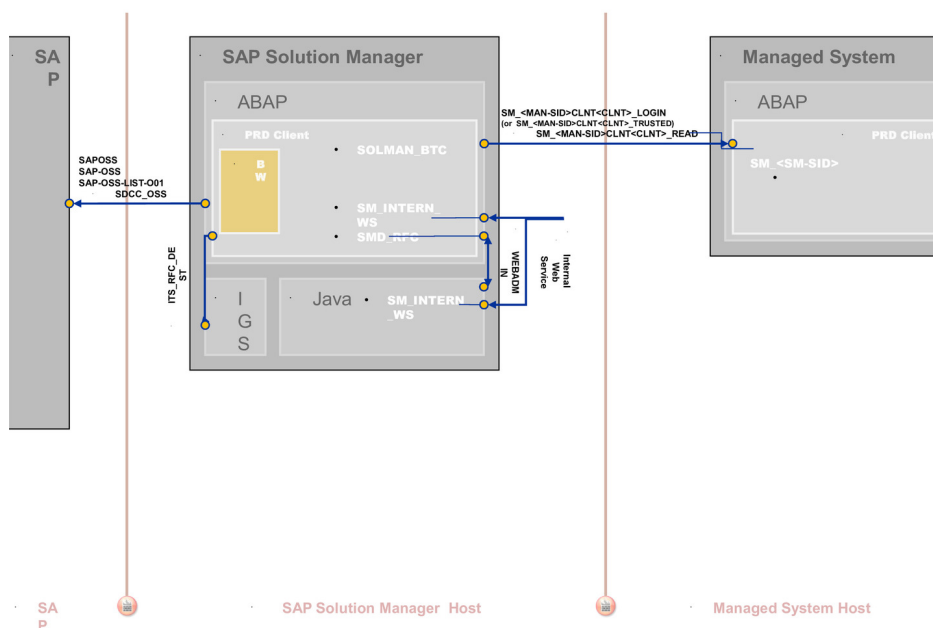


Figure 15: Infrastructure

### 8.3.1.2 Scenario Configuration

The scenario *DVM* is configured using transaction `SOLMAN_SETUP`.

To configure the scenario proceed as follows:

#### Basic Configuration transaction `SOLMAN_SETUP`

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic functions.

When you call the *DVM Configuration Guided Procedure*, the system asks you to create a configuration user. You can either create a new specific configuration user (Help Text ID: `USER_CONFIG_DVM`) or use an existing user and add the relevant roles for *DVM*. The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

If you create a configuration user manually, the composite role `SAP_DVM_CONF_COMP` contains all single roles which are automatically assigned to the configuration user.

Table 255

Single Roles	Help TXT ID
<code>SAP_DVM_CONFIG</code>	<code>AUTH_SAP_DVM_CONFIG</code>
<code>SAP_SETUP_SYSTEM_PREP</code>	<code>AUTH_SAP_SETUP_SYSTEM_PREP</code>
<code>SAP_SMWORK_DVM</code>	<code>AUTH_SAP_SMWORK_DVM</code>
<code>SAP_SM_BP_DISPLAY</code>	<code>AUTH_SAP_SM_BP_DISPLAY</code>

Single Roles	Help TXT ID
SAP_SM_DASHBOARDS_DISP_DVM	AUTH_SAP_SM_DASHBOARDS_DISP_DVM
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

### Note

To be able to create users and assign user roles, you need to assign as well role SAP\_SM\_USER\_ADMIN.

### Specific Authorization

The configuration is allowed to jump to Early Watch Management Guided Procedure to start the DVM report generation. The authorization is added in object SM\_SETUP This is relevant, if the DVM section in an EWA alert report is to be displayed with detailed data.

## 8.3.1.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

#### Communication Channels

Table 256

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems	RFC	Reading information from managed systems
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

**i Note**

All mentioned RFC - destinations are automatically created via transaction SOLMAN\_SETUP (view: managed systems), see *Secure Configuration Guide*.

Table 257

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	To read DVM statistics and analyses
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific	for self-service and user authentication when starting analysis in the managed system

**BW- Reporting RFC Connection**

Table 258

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client	System-specific	System-specific	System-specific	
BI_CLNT<BWclient> if BW is realized in remote BW - scenario system , for content activation and data download	Managed System or Solution Manager System	System-specific	System-specific		In transaction SOLMAN_SETUP
<SolutionManagerSID>CLNT<SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client	System-specific	System-specific	BI_CALLBACK (customer specific)	In transaction SOLMAN_SETUP
Trusted RFC to remote BW systemSAP_BILO	remote BW - system (source: SAP Solution Manager)	System-specific	System-specific	Dialog User	Used to read data from remote BW for BI - Reporting

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
					. created during SOLMAN_SETUP

### 8.3.1.4 Technical Users

The technical users in the following tables are created automatically during configuration. All technical users are of type *System User*. For more information on individual users, see *Secure Configuration Guide* in section *Technical Users*.

#### Users in Managed Systems

Table 259

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>
<i>TMW - User</i>	SMTM<SID of Solution Manager system>

### 8.3.2 Scenario Integration

According to the end-to-end business process life-cycle, this scenario needs to integrate with a number of other functions, which come into play in your daily business. The following sections describe the integration of DVM with other scenarios within SAP Solution Manager, and which user roles would be applicable.

#### **i** Note

For more detail on each individual scenario, see the according *Scenario—Specific Guide*.

#### Technical Scenarios (Technical Monitoring)

Depending on the technical sub scenario, you need one of the composite roles for Technical Monitoring.

#### DVM Impact Reference Integration with BPCA

Within view *DVM Impact Reference* authorizations of TBOM BPCA is required by the user. Therefore, additionally assign the following roles to the user in the Solution Manager system:

- SAP\_SM\_BPCA\_TBOM\*
- SAP\_SM\_BPCA\_RES\*
- SAP\_STWB\_2\*

As BPCA requires a user in the managed system, you need to create a user in the managed system with the same User ID and assign to it role: SAP\_SM\_BPCA\_TBOM.

The *BPCA* scenario also requires a trusted RFC - connection between the SAP Solution Manager system and its managed systems. Therefore, you need to assign authorization for trusted RFC connections to both users. For more information, see the scenario-specific guide for Business Process Change Management (BPCA).

## Test Plan Management

You can create Test Plans from within DVM Management. To be able to do so, you require:

- role `SAP_SM_KW_*` for authorization object `S_IWB`
- according role for Test Plan Management: `SAP_STWB_2_*`

## 8.3.3 Users and Authorizations

### 8.3.3.1 User and Roles

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for *Data Volume Management*. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information about User Interface authorizations, see *Authorization Concept Guide*.

The tables underneath give you a further overview, which single roles are included in the respective composite roles.

#### Authorization for Trusted RFCs between SAP Solution Manager, and Managed Systems

Trusted authorizations are needed between SAP Solution Manager and its managed systems. The user in the managed system and the user in the Solution Manager system receive role `SAP_SM_S_RFCACL` (Help Text ID: `AUTH_SAP_S_SM_RFCACL`) with authorization object `S_RFCACL`.

#### **i** Note

Both roles are not contained in the respective composite roles, due to their highly security-relevant character.

#### Authorization for Trusted RFC between SAP Solution Manager and BW-System

In case of a remote *BW* - connection, the user in the SAP Solution Manager system is additionally assigned trusted authorization object `S_RFCACL` (role `SAP_SM_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`). The user in the *BW* - system is also assigned authorization `S_RFCACL` (role `SAP_SM_BW_S_RFCACL`; Help Text ID: `AUTH_SAP_S_SM_RFCACL`).

#### Administrator User (Help Text ID: `TP_DVM_ADMIN`)

**Technical composite role name: `SAP_DVM_ADMIN_COMP` in the SAP Solution Manager system**

Table 260

Single Roles	Help Text ID
SAP_DVM_ALL	AUTH_SAP_DVM_ALL
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SMWORK_DVM	AUTH_SAP_SMWORK_DVM
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

**Technical composite role name: SAP\_BW\_DVM\_ADMIN\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 261

Single Roles	Help Text ID
SAP_BI_E2E_DVM	AUTH_SAP_BI_E2E
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

**Technical role in managed system**

Table 262

Single Roles	Help Text ID
SAP_DVM_SERVICE	AUTH_SAP_DVM_SERVICE
SAP_DVM_GSS	AUTH_SAP_DVM_GSS

**Display User (Help Text ID: TP\_DVM\_DIS)**

**Technical composite role name SAP\_DVM\_DISPLAY\_COMP in the SAP Solution Manager system**

Table 263

Single Roles	Help Text ID
SAP_DVM_DIS	AUTH_SAP_DVM_ALL
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SMWORK_DVM	AUTH_SAP_SMWORK_DVM
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

**Technical composite role name: SAP\_BW\_DVM\_DISPLAY\_COMP in the BW system/client**

In case you use remote BW scenario, these roles must be assigned to the user with the same user ID and Password in the BW system.

Table 264

Single Roles	Help Text ID
SAP_BI_E2E_DVM	AUTH_SAP_BI_E2E



Single Roles	Help Text ID
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

### Technical role in managed system

Table 265

Single Roles	Help Text ID
SAP_DVM_SERVICE	AUTH_SAP_DVM_SERVICE
SAP_DVM_GSS	AUTH_SAP_DVM_GSS

## 8.3.3.2 Critical Authorization Objects

The following section gives information of some of the main authorization objects for *Data Volume Management*.

### Authorization Object S\_TABU\_DIS

In user roles for Data Volume Management you find authorization object S\_TABU\_DIS. Authorization groups SARC, BCTA protect all relevant customizing views and customizing clusters for this scenario.

## 8.4 Value Management Dashboard (iCI - Interactive Continuous Improvement)

### 8.4.1 Getting Started

The purpose of Value Management is to provide you with a holistic overview and actual status of the application and life-cycle management of your mission critical operations. The objective is to ensure that the appropriate service and support is provided for the SAP Software Solutions and that actions are taken to address any open issues that might have a negative effect on the operations of the installed application or business solutions. The data shown in the ESR is based on the information available in the customer's SAP Solution Manager or SAP Global Support Backbone and is measured against the SAP E2E standards. The Balanced Scorecard (BSC) and status overview results from the individual Top Issues.

Based on the analyzed data the objective is to provide information on the actual status of the support engagement and the level of support needed for the SAP Software Solutions. This includes all necessary services, recommendations and actions. Key elements of the SelfService are a status overview based on the referring Top Issues and the detailed chapters with the analyzed data and recommendations for each area. Strategy discussions and planning within the customer's IT organization as well as between customer and SAP may be based on this report. The Self-Service allows you to get an up-to-date insight of their customers from point of view of system landscape management and application lifecycle management. The partner has 3 possibilities:

- focus on one single system/installation
- focus on a group of systems/installations
- look at all systems/installations overall

Accordingly, the final report can be discussed and handed over to SAP or it can be used for customer internal plannings and optimizations.

## 8.4.2 Prerequisites

### 8.4.2.1 Scenario Configuration

You can configure Value Management Dashboard using transaction `SOLMAN_SETUP` or work center SAP Solution Manager configuration.

#### Creating Configuration User in Basic Configuration Transaction `SOLMAN_SETUP`

When you call the Guided Procedure for *Value Management Dashboard* (iCI), the system asks you to create a specific configuration user (default technical user name: `SMC_ICI_<XXXClient>`) for iCI (Help Text ID: `USER_CONFIG_ICI`). You can either create a separate configuration user or use an existing user and add all required additional roles. The system automatically adds all relevant user roles. Authorizations in these roles are all fully maintained due to automated configuration.

If you want to create the configuration user *manually*, you need to assign the composite role `SAP_ICI_CONF_COMP`, which contains all single roles that are automatically assigned to the configuration user in the SAP Solution Manager system.

Table 266

Single Role	Help TXT ID
<code>SAP_SETUP_SYSTEM_PREP</code>	<code>AUTH_SAP_SETUP_SYSTEM_PREP</code>
<code>SAP_SMWORK_CONFIC</code>	<code>AUTH_SAP_SMWORK_CCLM</code>
<code>SAP_SM_ICI_CONFIG</code>	<code>AUTH_SAP_SM_CCM_CONFIG</code>
<code>SAP_SM_SMUA_ALL</code>	<code>AUTH_SAP_SM_RFC_ADMIN</code>
<code>SAP_SM_SL_ADMIN</code>	<code>AUTH_SAP_SM_SL_DISPLAY</code>
<code>SAP_SM_USER_ADMIN</code>	<code>AUTH_SAP_SM_USER_ADMIN</code>
<code>SAP_SYSTEM_REPOSITORY_ALL</code>	<code>AUTH_SAP_SYSTEM_REPOSITORY_DIS</code>
<code>SAP_SM_ROLECMP_ALL</code>	<code>AUTH_SAP_SM_ROLECMP_ALL</code>
<code>SAP_SM_FIORI_LP_EMBEDDED</code>	<code>AUTH_SAP_SM_FIORI_LP_EMBED</code>

### 8.4.2.2 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

## Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

### Communication Channels

Table 267

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems	RFC	Reading information from managed systems
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes

## Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

### RFC Connections from SAP Solution Manager to Managed Systems

#### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 268

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	to read data form the managed system

### BW- Reporting RFC Connection

Table 269

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution	System-	System-	System-specific	during installation

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	How Created
	Manager productive client	specific	specific		
BI_CLNT<BWclient>if BW is realized in remote BW - scenario system , for content activation	Managed System or Solution Manager System	System-specific	System-specific	System-specific	in transaction SOLMAM_SETUP
<SolutionManagerSID>CLNT<SolutionManager- ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client	System-specific	System-specific	BI_CALLBACK(customer specific)	in transaction SOLMAM_SETUP

### 8.4.2.3 Technical Users

The technical user in the following table is created automatically during configuration. Technical users are of type *System User*. For more information on individual technical users, see *Secure Configuration Guide* in section *Technical Users*.

#### User in Managed Systems

Table 270

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>

### 8.4.3 Interactive Continuous Improvement (iCI) Dashboard

The iCI Dashboard and Value Management comprises an automated process of KPI collection. It focuses on the following features:

- Value Management Dashboard (iCI)
- Integration into DVM and CCM

## Technical System Landscape

The iCI Dashboard is called via [URL](#) from a browser. The iCI Dashboard and iCI Maintenance applications are both BSP-applications, which are located in the SAP Solution Manager. The BSP-applications call the iCI ODataService to fetch data from `ST-BCO` component (BW-system). The ODataService is located in `ST` component (Solution Manager). The ODatasevice encapsulates the iCI queries based on Multiprovider `0SM_ESRSK`, on basic cube `0SM_ESRSG` and several iCI function modules which are responsible to fetch data from iCI tables or to create/update data in iCI tables. All function modules used in the ODataService are `RFC` enabled if the BW-system is configured as standalone BW-system (remote BW).

## Trusted RFC Connection

If you run your scenario with a remote BW - system, you need to have a trusted RFC - connection in place. Due to this, the user must be created with the same User-ID in both systems, the SAP Solution Manager system as well as the BW - system.

## Authorizations and Roles (Integration with DVM and CCM)

As iCI runs in Solution Manager and collects data in BW-system, you need authorizations in the Solution Manager to display the collected data. In addition, this users must be present in the BW-system with the correct authorization to collect the relevant data. This is possible per default with template users for [DVM](#) and [CCM](#).

## Users and Roles in Solution Manager

If you want to use the iCI Dashboard, role `SAP_SM_DASHBOARDS_DISP_ICI` is relevant. This role is assigned in transaction `SOLMAN_SETUP` to template users for [DVM](#) and [CCM](#).

## Authorization Object

Authorization object `SM_ICICONF` is used to restrict categories for iCI usage. The object is included in various roles for BW:

- `SAP_BI_E2E_DVM`
- `SAP_BI_E2E_CCM`
- `SAP_BI_E2E`

## Authorizations and Roles (Standalone)

You can use iCI independent of DVM and CCM scenarios.

## Users and Roles in Solution Manager

You can create template users in transaction `SOLMAN_SETUP` via guided procedure Value Management Dashboard (`ICI_ADM_***` and `ICI_DIS_***`). According to whether you run your BW in the Solution Manager client or separate, the `SOLMAN_SETUP` step assigns the relevant roles.

## Administration User ICI\_ADM\_XXX

Roles in the SAP Solution Manager system

Table 271

Role	Help TXT
SAP_SMWORK_SERVICE_DEV	AUTH_SAP_SMWORK_SERVICE_DEV
SAP_SM_DASHBOARDS_ADM_ICI	AUTH_SAP_SM_DASHBOARDSDISICI
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL

Roles in the BW system

Table 272

Role	Help TXT
SAP_BI_ICI	AUTH_SAP_BI_ICI
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN
SAP_SM_BW_S_RFCACL	AUTH_SAP_SM_S_RFCACL

### Display User ICI\_DIS\_XXX

Roles in the SAP Solution Manager system

Table 273

Role	Help TXT
SAP_SMWORK_SERVICE_DEV	AUTH_SAP_SMWORK_SERVICE_DEV
SAP_SM_DASHBOARDS_DISP_ICI	AUTH_SAP_SM_DASHBOARDSDISICI
SAP_SM_S_RFCACL	AUTH_SAP_SM_S_RFCACL

Roles in the BW system

Table 274

Role	Help TXT
SAP_BI_ICI_DISP	SAP_SM_BI_DISP_ROLE
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP
SAP_SM_BW_S_RFCACL	AUTH_SAP_SM_S_RFCACL

### Authorization object S\_RFC

To be able to configure favorites and personal user settings, the display user also receives write and delete authorization for this configuration part. It is included in the SAP\_BI\* roles.

# 9 Services

## 9.1 Document History

Here, all changes to the specific scenario guide are listed according to Support Package.

Table 275

Support Package Stacks (Version)	Description
SP01	<b>General Adaptations to Previous Release 7.1 (Due to new Process Documentation functionality)</b> <ul style="list-style-type: none"><li>Removed roles SAP_SMWORK_BASIC* (obsolete)</li><li>Substituted roles SAP_SOL_PROJ_ADMIN_*, SAP_SOLAR_* and SAP_SM_SOLUTION_* with SAP_SM_SL_*</li><li>Substituted roles SAP_SOL_KW_* with SAP_SM_KW_*</li></ul> <b>SAP Fiori Launchpad Integration</b> <ul style="list-style-type: none"><li>All users receive SAP Fiori Launchpad authorization role SAP_SM_FIORI_LP_EMBEDDED</li></ul>
SP02	<b>Service Request Management</b> <ul style="list-style-type: none"><li>adapted roles SAP_SERVICE_REQUEST_*.</li></ul>
SP03	<b>Service Delivery</b> <ul style="list-style-type: none"><li>added role SAP_OP_DSWP_EWA to composite role SAP_SERV_DELIVERY_*COMP and SAPSERVICE user.</li></ul>

## 9.2 Scenario-Specific Guide: SAP Engagement and Service Delivery

### 9.2.1 Getting Started

**What is this guide about?** SAP Solution Manager covers a wide range of divers scenarios you can use. As a customer, you might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides per scenario which cover all relevant information for this specific scenario.



#### Caution

Before you start using this scenario-specific guide, you must read the core information about security issues in SAP Solution Manager, and the *Secure Configuration Guide*, which refers to all security-relevant information during basic configuration of SAP Solution Manager. Without this information, we do not recommend to set up

any specific scenario. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

This guide covers the following topics:

- **Getting Started:** find out about target groups of this guide. Links for any additional components can be found in the Core Guide.
- **Prerequisites:** find out about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other.
- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).
- **Security Optimization Services:** find out about authorizations for these services.
- **Service Delivery User:** find out about the service delivery user (Premium Engagement)
- **Scenario Integration:** according to the life-cycle approach the various scenarios integrate with each other. Here, you can find out about authorizations you need to assign to your users for these cases.

## 9.2.2 Prerequisites

### 9.2.2.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete scenario. The SAP Solution Manager is connected via `READ - RFC` to your managed systems, and your managed systems are connected to the SAP Solution Manager via `BACK - RFC`. More information on all connections, when they are used, and which technical users are required, you can find out in more detail in the following sections.



## Technical Infrastructure

- SAP Engagement and Service Delivery

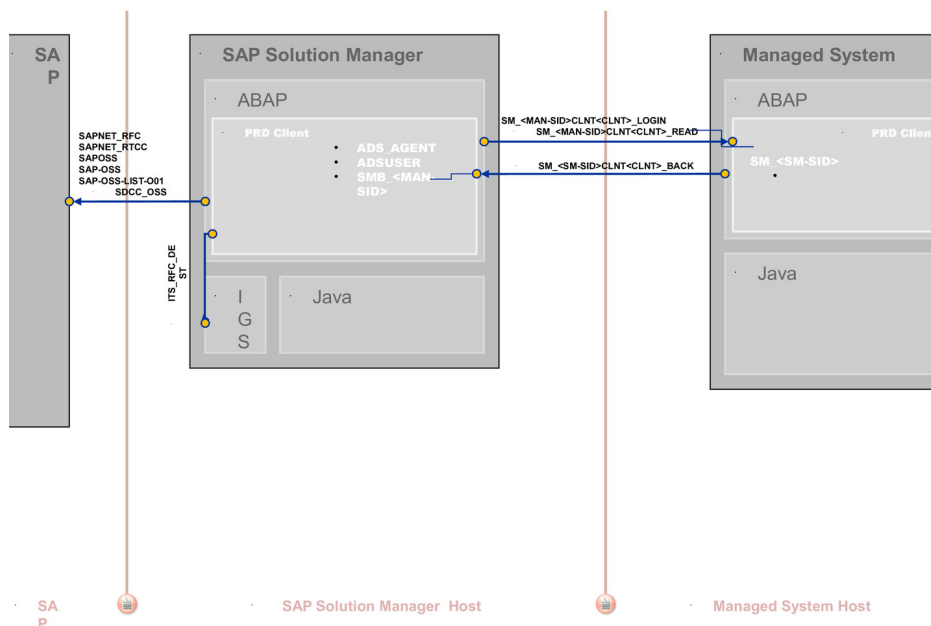


Figure 16: Infrastructure

## 9.2.2.2 Configuration

### Basic Configuration transaction SOLMAN\_SETUP

After you have run the basic automated configuration for SAP Solution Manager, you are able to run basic functions, like creating and sending an EarlyWatch Alert report.

### Configuration Roles

There are no specific configuration roles when using transaction `SPRO`. Nevertheless, you can use the possibility in creating your own configuration roles. For more information, see the according [How-to Guide](#).

## 9.2.2.3 Communication Channels and Destinations

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario.

### Communication Channels

The table below shows the communication channels used by SAP Solution Manager, the protocol used for the connection, and the type of data transferred.

### Communication Channels

Table 276

Communication Channel	Protocol	Type of Data Transferred / Function
Solution Manager to OSS	RFC	Exchange of problem messages, retrieval of services
Solution Manager to managed systems and back	RFC	Reading information from managed systems
Solution Manager to managed systems within customer network	FTP	Update route permission table, content: IP addresses, see section <i>File Transfer Protocol (FTP)</i>
Solution Manager to SAP Service Marketplace	HTTP (S)	Search for notes

### Communication Destinations

The table below shows an overview of the main communication destinations used by SAP Solution Manager (including its managed systems and SAP Support Portal).

#### RFC Connections from SAP Solution Manager to Managed Systems

##### **i** Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems), see *Secure Configuration Guide*.

Table 277

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Remarks
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	Customer-specific	Customer-specific	In case of not using trusted RFC
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>	To retrieve data from the managed systems for service sessions; collect information on product licence and maintenance certificates

#### RFC Connection from Managed System to SAP Solution Manager

Table 278

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	SMB_<managed system ID>	Send service data from managed systems	Automatically created via transaction

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	How Created
					to SAP Solution Manager	n SOLMAN_SETUP (view: managed systems)

### Internet Graphics Server (IGS) RFC Connection

Table 279

RFC Destination Name	Activation Type	How Created
ITS_RFC_DEST	Registered Server program (program: IGS.<SID>)	Manually in transaction SM59

### RFC Connections from SAP Solution Manager to SAP

Table 280

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	Remarks
SAPOSS (ABAP connection)	/H/ SAP ROUTER /S // sap serv v/H	01	001	OSS_RFC (CPIC)	Notes Assistant	Maintain technical settings in transaction OSS1
SAP-OSS (ABAP connection)	/H/ SAP ROUTER /S // sap serv v/H	01	001	S-User (Customer-specific)	Exchange problem messages with SAP (function: Service Desk), synchronize system data with Support Portal and send data about managed systems; transfer of solution, issue data; transfer feedback to	Automatically created via transaction SOLMAN_SETUP (view: managed systems)

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	Remarks
	/oss001				SAP Service Connection, product data download	
SAP-OSS-LIST-001 (ABAP connection)	/H/SAPROUTER/S//sapserver/H/oss001	01	001	S-User (Customer-specific)	Retrieve information about which messages have been changed at SAP	Created in transaction SM59
SDCC_OSS (ABAP connection)				See SAP Note <a href="#">763561</a>	Used by the <i>Service Data Control Center</i> to communicate with the SAP Support Portal front-end system; update Service Definitions (functions: System Monitoring for EWA and Service Plan)	User is a copy of the SAPOSS connection to SDCC_OSS; userSDCC_NEW with default password: download  <b>i Note</b> If SDCCN is used locally, that is Solution Manager is not Master System, SDCC_OSS is created automatically in the managed system;
SAPNET_RFC (ABAP connection)	/H/SAPROUTER/S//sapserver/H	01	001		Send EarlyWatch Alerts (functions: System Monitoring for EWA and Service Plan)	A copy of the SAPOSS connection to SAPNET_RFC

RFC Destination Name	Target Host Name	System Number	Logon Client	Logon User (Password)	Use	Remarks
	/oss001					
SAPNET_RTCC (ABAP connection)	/H/SAPROUTER/S//sapserver/H/oss001	01	001	OSS RFC (CPIC)	Service Preparation Check (RTCCTOOL)	Created automatically by RTCCTOOL, copy of SAPOSS

### CCMSPing RFC Connection

Table 281

RFC Destination Name	Activation Type	Logon User (Password)	Use (Scenario)	Remarks
CCMSPING.<server><SystemNr.>	Registered Server Program (program ccmsping.00)	CSMREG (customer-specific)	Service Level Reporting with CCMSPING	User created during configuration of Central Monitoring (CCMS).

## 9.2.2.4 Technical Users

The technical users in the following tables are created automatically during configuration. All technical users are of type *System User*. For more information on individual users, see *Secure Configuration Guide* in section *Technical Users*.

### User in Managed Systems

Table 282

User Name	User ID
<i>Read - User</i>	SM_<SID of Solution Manager system>

## User in SAP Solution Manager System

Table 283

User Name	User ID
<i>Back - User</i>	SMB_<managed system ID>

### 9.2.2.5 SAP Support Portal Contact in SAP Solution Manager (Table: AISUSER)

Users who communicate with SAP Support Portal via RFC destination SAP-OSS need an SAP Support Portal contact to SAP Solution Manager. You maintain the contact in table AISUSER (transaction AISUSER). This contact corresponds to the S-User in the SAP Support Portal, without the initial **S**.

#### Caution

The S-User for the SAP Support Portal must be requested via URL [service.sap.com](https://service.sap.com)

### 9.2.2.6 S-User Authorization for Service Desk and Expert on Demand

Your S-User needs the following authorizations for SAP Support Portal functions.

#### S-User Authorization

Table 284

Activity	Authorization
Create message	ANLEG: Create SAP message
Send messages	GOSAP: Send to SAP
	WAUFN: Reopen SAP message
Confirm messages	QUITT: Confirm SAP message
Display/change secure area	PWDISP: Display secure area
	PWCHGE: Change secure area

### 9.2.2.7 S-User Authorization for Data Download from SAP

Your s-user needs the following authorizations for the SAP Support Portal functions.

#### S-user Authorization Download Data from SAP

Table 285

Activity	Authorization
Administration	ADMIN
Maintain all logon data	PWCHGE
Maintain user data	USER
Maintain system data	INSTPROD
Request license key	LICKEY

## 9.2.2.8 Business Partners Created During Configuration

When you configure the SAP Solution Manager using the automatic basic settings configuration, additional business partners are created.

### For SAP Engagement and Service Delivery

The business partners are created as follows:

Table 286

First Name	Last Name	Remarks
SAP	Technical Quality Manager	Automatically assigned <i>ID</i> TQM or SAP TQM
SAP	Support Advisor	Automatically assigned <i>ID</i> SAPSUPAD
SAP	Engagement Architect	Automatically assigned <i>ID</i> SAPENAR
SAP	Back Office	Automatically assigned <i>ID</i> SAPBACKO
SAP	Consulting	Automatically assigned <i>ID</i> SAPCON
Customer	Program Management	Automatically assigned <i>ID</i> CUSTPM
Customer	Business Process Operations	Automatically assigned <i>ID</i> CUSTBPM
Customer	Custom Development	Automatically assigned <i>ID</i> CUSTCD
Customer	Technical Operations	Automatically assigned <i>ID</i> CUSTTO
Customer	Partner	Automatically assigned <i>ID</i> CUSTPAR

### **i** Note

An additional business partner (name: SAP Support) is automatically created for user SAPSUPPORT as soon as this user is created during the automatic basic settings configuration (see section: *User SAPSUPPORT*).

## For SOLMAN\_SETUP Template Users and Configuration Users

Users created using transaction `SOLMAN_SETUP` are assigned an according business partner, if the scenario requires this. The system displays the relevant Business Partner number in the log when you create the relevant user.

## More Information

on how to configure the basic settings, see *Configuration Guide SAP Solution Manager* in the Service Marketplace:

► [service.sap.com/instguides](https://service.sap.com/instguides) ► *SAP Components* ► *SAP Solution Manager <current release>* ►

## 9.2.3 CRM Standard Customizing for Solution Manager

The Service Request and Issue Management use cases are based on CRM, and uses CRM customizing such as transaction types, action profiles, and so on. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects. The following table gives you an overview of the transaction types used.



### Caution

If you copy SAP standard customizing you need to add the changed values in the according CRM - authorization objects for the scenario. See also How-to Guide on how to maintain authorization objects.

### Transaction Types Issue Management

Table 287

Transaction Type	Usage	Remarks
SLFI	Issues	supported
SLFT	Top Issues	supported
SLFE	Expert on Demand	supported
TASK	Actions	supported
SLFC	Engagement Cycle (Service Request)	supported

### Transaction Type Service Request

Table 288

Transaction Type	Usage	Remarks
SLFS	Service Request	supported



## 9.2.4 Scenario Integration

SAP Engagement and Service Delivery combines a number of tools with Services, such as Issue Management or Support Request with Services. The integration with other scenarios is described in the following section.

### Incident Management

To be able to create incidents from issues, you need to assign role `SAP_SUPPDESK_CREATE`.

## 9.2.5 Recommended Users and Authorizations

To enable your users to work with the application, you need to assign them authorizations in the Solution-Manager-system.

When you are working in a project to implement new business processes, change existing ones, operate your systems, and so on, you may need SAP support. SAP delivers recommended user descriptions on which SAP delivered roles are modeled. These user descriptions and roles can only be regarded as templates for you. You need to first define which tasks the individual members in your company execute, and then adjust the according roles. These roles are described in the section *User Description and User Roles for the Service Delivery User*.



### Caution

The roles delivered by SAP can only be regarded as models for adjustment to your company's needs.

### 9.2.5.1 User Descriptions and User Roles to Use the Work Center

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for SAP Engagement and Service Delivery. All users are assigned a composite role, which contains a number of single roles.

#### Work Center

The work center represents a work space for a user, which allows access to all tools necessary for the work of the user. You can use the delivered composite roles to assign to your users. Still, you may want to restrict the access and/or the authorizations for a particular user. Access in the navigation panel is restricted by using the authorization object `SM_WC_VIEW`. For more information on User Interface authorizations, see [Authorization Concept Guide](#).

#### Manager/Administrator (technical role name: `SAP_SERV_DELIVERY_COMP`)

Table 289

Single Role	Restriction on
<code>SAP_ISSUE_MANAGEMENT_EXE</code>	Authorization to execute issues
<code>SAP_SERVICE_REQUEST_ALL</code>	Full authorization to use Service Requests

Single Role	Restriction on
SAP_SMWORK_SERVICE_DEV	Access to work center SAP Engagement and Service Delivery
SAP_SM_SL_ADMIN	Full authorization for Process Management
SAP_SYSTEM_REPOSITORY_DIS	Display authorization for transaction LMDB
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori Launchpad
SAP_SM_ITPPM_ALL	Full authorization to use Project Management
SAP_OP_DSWP_EWA	EWA authorization

### Display User (technical role name: SAP\_SERV\_DELIVERY\_DIS\_COMP)

Table 290

Single Role	Remarks
SAP_ISSUE_MANAGEMENT_DIS	Authorization to display issues
SAP_SERVICE_REQUEST_DIS	Authorization to display service requests
SAP_SMWORK_SERVICE_DEV	Access to work center SAP Engagement and Service Delivery
SAP_SM_SL_DISPLAY	Display authorization for solutions
SAP_SYSTEM_REPOSITORY_DIS	Display authorization for transaction LMDB
SAP_SM_FIORI_LP_EMBEDDED	Access to SAP Fiori Launchpad
SAP_SM_ITPPM_DIS	Display authorization to use Project Management
SAP_OP_DSWP_EWA	EWA authorization

## 9.2.5.2 User Description and User Roles for Service Delivery (Premium Engagement)

You can assign a composite role for SAP Support employees. This role contains a number of single roles. You should assign the composite role to the user in your system which you created for SAP Support employees. You can also execute all self-services yourself. Assign composite role `SAP_PREMIUM_ENGAGEMENT_COMP`.

## 9.2.5.3 Supportability Performance Platform

The goal of the *Supportability Performance Platform* (SPP) is to provide a database for SAP customers, that collects and reports standardized and customer specific KPI information. It allows customers to initiate explicit actions in case of deviations from the target values or in comparison to other companies in the same industry or size. This allows customer IT organizations to understand and collaborate better with the lines of business. For SAP, SPP and the derived KPI/Benchmark overview is a starting point to stabilize the SAP engagement with the customer. By benchmarking customer KPIs with related industries, transparency and follow up activities based

on improving specific KPIs can be initiated by the TQMS and ESAs. Midterm, the information transferred to SAP can support SAP's service portfolio and strategy. Additionally, with the collected benchmark information SAP can provide business cases for possible improvements that can support the customer IT collaboration with the business. The quality KPIs are aligned with the IT strategy (for instance innovation driver, service, or solution provider) during an ACCOE assessment together with the customer. The KPIs are activated and a baseline measurement is performed. The initial action plan to reach the KPI target is agreed. The KPIs are in the responsibility of the quality managers (customer, partner, and SAP).

## Features

Assign one of the following roles to your Service and Support User:

- SAP\_SM\_SPP\_ALL (full authorization)
- SAP\_SM\_SPP\_DIS (display authorization)

### 9.2.5.4 User Descriptions and User Integration Roles for Issue Management

This paragraph gives an overview over users as recommended by SAP and their according user roles assignment for SAP Engagement and Service Delivery. All users are assigned a composite role, which contains a number of single roles.

The roles are primarily to be used with integrations, for instance Change Request Management, QGM, and so on. If you only require your users to be able to run Issue Management, you assign these roles in addition to the work center relevant roles.

#### Manager/Administrator (technical role name: SAP\_ISSUE\_MANAGEMENT\_ALL\_COMP)

Table 291

Single Role	Restriction on
SAP_ISSUE_MANAGEMENT_ALL	Authorization to execute Issues
SAP_SM_SL_ADMIN	Full authorization for Process Management

#### Operations (technical role name: SAP\_ISSUE\_MANAGEMENT\_EXE\_COMP)

Table 292

Single Role	Restriction on
SAP_ISSUE_MANAGEMENT_ALL	Authorization to execute Issues
SAP_SM_SL_EDIT	Maintenance authorization for Process Management

#### Display User (technical role name: SAP\_ISSUE\_MANAGEMENT\_DIS\_COMP)

Table 293

Single Role	Restriction on
SAP_ISSUE_MANAGEMENT_DIS	Display authorization for Issues

Single Role	Restriction on
SAP_SM_SL_DISPLAY	Display authorization for Process Management

## 9.2.5.5 Main Authorization Objects

This section gives you some information on the main authorization objects.

### CRM Authorization Objects

Issue Management is based on the CRM - functionality. The main CRM - objects are included in the roles for Issue Management. For more information on CRM authorizations, see in the *Authorization Concept Guide* the section on CRM integration.

#### Authorization Object DSWP\_ISSUE

This authorization object controls activities for Issues.

#### Authorization Object DSWP\_TOPIS

This authorization object controls activities for Top Issues.

#### Authorization Object DSWP\_EOD

This authorization object controls activities for Expert on Demand.

#### Authorization Object DSWP\_ACTIO

This authorization object controls activities for Actions.

#### Authorization Object D\_SVAS\_SES

This authorization object restricts services. The following List of Self Service Package IDs and Types are delivered:

- GSS\*
- SELF\* (including SELF\_TSM, SELF\_ALM, SELF\_GV, SELF\_SQL, SELF\_TEE)
- EWA\_HANP
- EW\_ALERT
- CP\_BPM\_A
- E2ETR\_AN
- EW\_SELF
- SUG\_REP
- EWA\_HPS
- PR\_SETUP

---

## 9.2.6 Security Optimization Service

For Security Optimization service, you need to assign additional authorizations. For more information, see [SAP Note 69647](#).

## 9.3 Early Watch Alert Management and Service Level Reporting

The Early Watch Alert service monitors the most important areas of a SAP component with focus on performance and stability. EWA data is based on weekly statistics of performance and system as well as data of system configuration and error analysis. The data is collected by unmodifiable data collectors using transaction `SDCCN` in the target system and is stored in cluster tables `BDDT0C` and `BDDATCOL` in SAP Solution Manager to be persisted. The report displays aggregates of these data as analysis results, trend graphics, and so on.

### Configuration

You can configure Early Watch Alert (EWA) Reporting in transaction `SOLMAN_SETUP`. Since the setup for EWA is mandatory for all systems in your system landscape, the procedure for the setup of Early Watch Alert Management can be run by user `SOLMAN_ADMIN`.

### Data Protection

The report does not contain data for specific users. Even though the statistical data can contain user names, they are without any relation to application data, but only to technical data, such as response times or information for technical error analysis. In case, the user who collects the data in the source system has authorization to run transaction `ST03` (Workload Monitor) and display application-relevant data, the EWA report also displays technical transaction codes with user names. This can be avoided by de-assigning value `S_TOOLS_EX_A` in authorization object `S_TOOLS_EX` for the user in question.

### Data Archiving

For more information, see [SAP Note 546685](#).

### Service Level Reporting

Service Level Reporting is based on the data of Early Watch Alert, and does not contain any additional data collectors.

## 9.4 Integration of SAP Fiori Applications

Here, you find specific information on the individually delivered applications that can be used on a central Fiori Hub. For more information on the concept of SAP Fiori Launchpad and Central Hub Scenarios, see [Authorization Concept Guide](#).

## **i** Note

General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the Authorization Concept for Solution Manager.

### **APP: My EarlyWatch Alert Reports**

This application allows users to view Early Watch Alert Reports. Users can do the following:

- view EWA reports
- filter report list
- mark report lists/chapters as favourites

### **Authorizations in the Back-End SAP Solution Manager (ST Component)**

## **i** Note

As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, assign the relevant single role `SAP_OP_DSWP_EWA` to the user. The relevant OData - Service is delivered per default in this role.

## **i** Note

As this role allows for change authorization, you may want to reduce the authorizations for display purposes. In general, activity fields for all authorization objects should be restricted to view or display activities.

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S RFC` and `S RFCACL` authorization.

### **Authorizations in the Frond-End (ST-UI Component)**

The following two roles are delivered for front-end usage for the application:

- `SAP_STUI_EWA_CHK_TCR`

This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.

- `SAP_STUI_EWA_CHK_AUTH`

This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:

1. Copy the Odata service into your name space.
2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.



# A Reference

## A.1 The Main SAP Documentation Types


The following is an overview of the **most important** documentation types that you need in the various phases in the life cycle of SAP software.

### Cross-Phase Documentation


**SAPterm** is SAPs terminology database. It contains SAP-specific vocabulary in over 30 languages, as well as many glossary entries in English and German.

- Target group:
  - Relevant for all target groups
- Current version:
  - On SAP Help Portal at [help.sap.com](https://help.sap.com)  > [Glossary](#) 
  - In the SAP system in transaction `STERM`

**SAP Library** is a collection of documentation for SAP software covering functions and processes.

- Target group:
  - Consultants
  - System administrators
  - Project teams for implementations or upgrades
- Current version:
  - On SAP Help Portal at [help.sap.com](https://help.sap.com)  (also available as documentation DVD)

The **security guide** describes the settings for a medium security level and offers suggestions for raising security levels. A collective security guide is available for SAP NetWeaver. This document contains general guidelines and suggestions. SAP applications have a security guide of their own.

- Target group:
  - System administrators
  - Technology consultants
  - Solution consultants
- Current version:
  - On SAP Service Marketplace at [service.sap.com/securityguide](https://service.sap.com/securityguide) 

### Implementation

The **master guide** is the starting point for implementing an SAP solution. It lists the required installable units for each business or IT scenario. It provides scenario-specific descriptions of preparation, execution, and follow-up of an implementation. It also provides references to other documents, such as installation guides, the technical infrastructure guide and SAP Notes.

- Target group:
  - Technology consultants

- Project teams for implementations
- Current version:
  - On SAP Service Marketplace at [service.sap.com/instguides](https://service.sap.com/instguides) ↗

The **installation guide** describes the technical implementation of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
  - Technology consultants
  - Project teams for implementations
- Current version:
  - On SAP Service Marketplace at [service.sap.com/instguides](https://service.sap.com/instguides) ↗

**Configuration Documentation in SAP Solution Manager** – SAP Solution Manager is a life-cycle platform. One of its main functions is the configuration of business scenarios, business processes, and implementable steps. It contains Customizing activities, transactions, and so on, as well as documentation.

- Target group:
  - Technology consultants
  - Solution consultants
  - Project teams for implementations
- Current version:
  - In SAP Solution Manager

The **Implementation Guide (IMG)** is a tool for configuring (Customizing) a single SAP system. The Customizing activities and their documentation are structured from a functional perspective. (In order to configure a whole system landscape from a process-oriented perspective, SAP Solution Manager, which refers to the relevant Customizing activities in the individual SAP systems, is used.)

- Target group:
  - Solution consultants
  - Project teams for implementations or upgrades
- Current version:
  - In the SAP menu of the SAP system under ► *Tools* ► *Customizing* ► *IMG* ▾

## Production Operation

The **technical operations manual** is the starting point for operating a system that runs on SAP NetWeaver, and precedes the application operations guides of SAP Business Suite. The manual refers users to the tools and documentation that are needed to carry out various tasks, such as monitoring, backup/restore, master data maintenance, transports, and tests.

- Target group:
  - System administrators
- Current version:
  - On SAP Service Marketplace at [service.sap.com/instguides](https://service.sap.com/instguides) ↗

The **application operations guide** is used for operating an SAP application once all tasks in the technical operations manual have been completed. It refers users to the tools and documentation that are needed to carry out the various operations-related tasks.

- Target group:
  - System administrators



- Technology consultants
- Solution consultants
- Current version:
  - On SAP Service Marketplace at [service.sap.com/instguides](https://service.sap.com/instguides) ↗

## Upgrade

The **upgrade master guide** is the starting point for upgrading the business scenarios and processes of an SAP solution. It provides scenario-specific descriptions of preparation, execution, and follow-up of an upgrade. It also refers to other documents, such as upgrade guides and SAP Notes.

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Service Marketplace at [service.sap.com/instguides](https://service.sap.com/instguides) ↗

The **upgrade guide** describes the technical upgrade of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Service Marketplace at [service.sap.com/instguides](https://service.sap.com/instguides) ↗

**Release notes** are documents that contain short descriptions of new features in a particular release or changes to existing features since the previous release. Release notes about ABAP developments are the technical prerequisite for generating delta and upgrade Customizing in the Implementation Guide (IMG).

- Target group:
  - Consultants
  - Project teams for upgrades
- Current version:
  - On SAP Service Marketplace at [service.sap.com/releasenotes](https://service.sap.com/releasenotes) ↗
  - In the SAP menu of the SAP system under ► *Help* ► *Release Notes* ▾ (only ABAP developments)

---

# Typographic Conventions

Table 294

Example	Description
---------	-------------





[www.sap.com](http://www.sap.com)

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

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see [www.sap.com/corporate-en/legal/copyright/index.epx#trademark](http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark) for additional trademark information and notices.

Please see [www.sap.com/corporate-en/legal/copyright/index.epx](http://www.sap.com/corporate-en/legal/copyright/index.epx) for disclaimer information and notices.

