

Security Guide | PUBLIC
Document Version: 7.2 SPS 21 – 2025-12-02

Application-Specific Security Guide

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Security Guide - Application Specific. 6

2 Overview. 8

2.1 Users and Roles Changes per Support Package: Document History. 8

2.2 List of Roles Updated per SP. 16

2.3 Adapting SAP Documentation (Help Text IDs) for Users and Roles to Your Needs. 20

2.4 Overview: SAP Cloud Integrations. 21

2.5 Overview: Capabilities/Functions. 22

2.6 Overview: SAP Solution Manager Functions Integration. 25

2.7 Overview: Third Party Products to Be Used with SAP Solution Manager. 27

2.8 SAP Solution Manager Business Roles Overview. 28

2.9 Overview: VAR - Specific Chapters. 35

3 Technical Administration. 36

3.1 Introduction. 36

3.2 Document History. 36

3.3 Scenario-Specific Guide: Technical Administration. 39

Prerequisites. 39

Users and Authorizations. 41

Integration. 51

Traces and Logs. 52

4 Process Management and Test Suite. 53

4.1 Document History. 53

4.2 Getting Started. 65

4.3 Scenario-Specific Guide: Process Management. 66

Prerequisites. 66

Scenario Integration. 73

Users and Authorizations. 75

User Roles for Additional Functions. 80

External Integration. 90

4.4 Scenario-Specific Guide: Business Process Change Analyzer. 91

Introduction. 91

Prerequisites. 91

CRM Standard Customizing. 96

Scenario Integration. 97

Users and Authorizations. 98

Additional Security Measures. 101

4.5 Scenario-Specific Guide: Test Suite. 102
Prerequisites. 102
Scenario Integration. 106
Users and Authorizations. 107
Additional User Roles. 111
Partner Integration. 120
Additional Security Measures. 125
4.6 Main Authorization Objects. 126
4.7 Scenario-Specific Guide: Scope and Effort Analyzer (SEA). 128
Introduction. 128
Getting Started. 128
Prerequisites. 129
User Descriptions and User Roles. 131
Authorization Objects. 133

5 Application Operations and Business Process Operation. 135
5.1 Introduction. 135
5.2 Document History. 135
5.3 Scenario-Specific Guide: Technical Monitoring. 144
Prerequisites. 144
Scenario Integration. 149
User Descriptions. 150
Early Watch Alert Management Configuration. 151
User Roles for System, Database, Host Monitoring, and Self - Monitoring. 152
User Roles for Process Integration - Monitoring. 153
User Roles for Message Flow Monitoring. 155
User Roles for End-User Experience Monitoring. 160
User Roles for HANA and Business Intelligence Monitoring. 161
User Roles for Interface (Channel) Monitoring. 163
End-User Roles for Job Monitoring. 165
User Roles for Infrastructure Monitoring. 168
Users and Roles for Exception Management. 169
Integration Visibility in Managed Systems. 171
Role for Technical Monitoring Support. 172
Main Authorization Objects. 172
Background Jobs. 174
5.4 Scenario-Specific Guide: Business Process Operations. 175
Getting Started. 175
Prerequisites. 175
Scenario Integration. 180
Users and Authorizations. 181
User Roles for Additional Functions. 188

5.5 Scenario-Specific Guide: Job Management. . . . 193
Prerequisites. . . . 193
Scenario Integration. . . . 197
Users and Authorizations. . . . 198
CRM Standard Customizing for Solution Manager. . . . 206
External Integration. . . . 207

6 Change Control and IT Service Management Scenarios. . . . 210
6.1 Getting Started. . . . 210
6.2 Document History. . . . 210
6.3 Scenario-Specific Guide: Quality Gate Management. . . . 226
Prerequisites. . . . 226
CRM Standard Customizing for Solution Manager. . . . 230
Users and Authorizations. . . . 231
Specific Authorization Objects. . . . 236
6.4 Scenario-Specific Guide: IT Service Management. . . . 237
Prerequisites. . . . 237
CRM Standard Customizing for Solution Manager. . . . 241
Scenario Integration. . . . 242
Users and Authorizations. . . . 243
External Integration. . . . 248
6.5 Scenario-Specific Guide: Change Management. . . . 248
Prerequisites. . . . 248
CRM Standard Customizing for Solution Manager. . . . 256
Users and Authorizations. . . . 257
E2E Integrations. . . . 270
Using System Recommendations Application. . . . 273
Requirements Management. . . . 275
Main Authorization Objects Change Request Management. . . . 283
6.6 Scenario-Specific Guide: Configuration Validation. . . . 288
Prerequisites. . . . 288
Users and Authorizations. . . . 288
6.7 Additional Security Measures. . . . 290

7 Custom Code, DVM, and Value Management Dashboard. . . . 292
7.1 Document History. . . . 292
7.2 Scenario-Specific Guide: Custom - Code Life Cycle Management. . . . 296
Getting Started. . . . 296
Prerequisites. . . . 296
Users and Authorizations. . . . 301
7.3 Scenario-Specific Guide: Data Volume Management. . . . 305
Prerequisites. . . . 305

Scenario Integration. . . . 309
Users and Authorizations. . . . 309
7.4 Value Management Dashboard (iCI - Interactive Continuous Improvement). . . . 312
Getting Started. . . . 312
Prerequisites. . . . 313
Interactive Continuous Improvement (iCI) Dashboard. . . . 315

8 Services. . . . 318
8.1 Document History. . . . 318
8.2 Scenario-Specific Guide: SAP Engagement and Service Delivery. . . . 320
Getting Started. . . . 320
Prerequisites. . . . 320
CRM Standard Customizing for Solution Manager. . . . 326
Scenario Integration. . . . 327
Recommended Users and Authorizations. . . . 328
Security Optimization Service. . . . 333
SAP EarlyWatch Alert Management. . . . 333
Service Level Reporting. . . . 334
Service Download - Rapid Content Delivery. . . . 335
SAP Readiness Check. . . . 335
Main Authorization Objects. . . . 336

9 Dashboard Framework Integration. . . . 338
9.1 Dashboard Users based on Dashboard Builder. . . . 338
9.2 Dashboard User for OLD Framework. . . . 340

1 Security Guide - Application Specific

Use

> ⚠ Caution
>
> For **Usage Rights for SAP Solution Manager**, check the following information in SAP Support Portal at: http://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 SAP Support Portal at: https://help.sap.com/viewer/p/SAP_Solution_Manager.

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

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 *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.

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

What is Your Opinion?

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

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

More Information

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

2 Overview

2.1 Users and Roles Changes per Support Package: Document History

> ⚠ Caution
>
> Before you start the implementation and configuration of SAP Solution Manager, make sure you have the latest version of this document. You can find the latest version at the following location: https://help.sap.com/viewer/p/SAP_Solution_Manager.

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

Support Package Stacks (Version)	Date	Description
SP21	2025-12-01	Changes have been made in scenarios: • ITSM
SP20	2024-12-02	Changes have been made in scenarios: • Change Control Management • ITSM • Process Management Process Management - Selective Data Transfer → Tip • For security recommendations, see the *Security Guide for Selective Data Transfer* on the Service Marketplace. • For online help documentation, see Help Documentation

Support Package Stacks (Version)	Date	Description
SP19	2024-07-01	Changes have been made in scenarios: • Test Suite • Job Scheduling Management • ITSM Process Management - Selective Data Transfer → Tip • For security recommendations, see the *Security Guide for Selective Data Transfer* on the Service Marketplace. • For online help documentation, see Help Documentation
SP18	2023-12-18	Changes have been made in scenarios: • Test Suite
SP16	2023-01-30	Changes have been made in scenarios: • Change Request Management (Test Suite integration) • Test Suite
SP15	2022-07-18	Changes have been made in scenarios: • Change Request Management (ATC integration) • Test Suite • Solution Documentation • IT Service Management
SP14	2022-02-24	Changes have been made in scenarios: • Change Request Management (git-enabled CTS) • Test Suite • Solution Documentation
SP13	2021-08-02	Changes have been made in scenarios: • Business Process Operations • Custome Code Management (CCM) • Data Volume Management (DVM) • Change Request Management • Test Suite • Technical Monitoring **General** New section *List of Roles Updates per SP*

Support Package Stacks (Version)	Date	Description
SP12	2021-02-01	Changes have been made in scenarios: • Change Request Management (Testplan Creation Integration; Best Practices; Integration with Git-enabled CTS) • Job Management (Redwood Integration) • Dashboard Framework Roles: adapted roles `SAP_SM_DASHBOARDS*` • Technical Administration (Task Inbox)
SP11	2020-05-11	Changes have been made in scenarios: • Change Request Management (E2E Integration: SAP Cloud Platform) • Business Process Monitoring (function *Integration Repository and Interface Discovery*) • Business Process Improvement (new function *Automation Rate Cockpit*) • Job Scheduling Management • Incident Management (new technical backgroundjob user)
SP10	2019-12-02	Changes have been made in scenarios: • Test Management • Process Management • Job Management • Change Request Management • Requirements Management • SAP Engagement • DVM, CCM • Application Monitoring For details, see the individual *Document History* per application scenario section.
`SP09`	2019-06-17	Changes have been made in scenarios: • Test Management • Process Management • Job Management • Technical Monitoring (Interface Connection) • Change Request Management • Quality Gate Management • Incident Management • Requirements Management • Dashboard Role: `SAP_SM_DSH_DISP` • Web Assistant: Web Asssitant Fiori Catalog is included in all relevant navigation roles `SAP_SMWORK_<scenario>` For details, see the individual *Document History* per application scenario section.

Support Package Stacks (Version)	Date	Description
SP08	2019-03-11	**General Changes** • Removed all references to work center security, as the main user interface is SAP Fiori based, for more information see section on *SAP Fiori User Interface* in the *Authorization Concept Guide*. • Removed the complete section on *Root Cause Analysis (RCA)*, as the main users are created and described in the configuration transaction `SOLMAN_SETUP`. For more information, see the Secure Configuration Guide. • Restructured all scenario-specific sections due to new SAP Backbone RFC connections. For more information, see section *Communication Channel Security* in the *Secure Configuration Guide*.
SP08		**Changes per Area** • Process Management and Test Management • Change Control Management • DVM and CCM • Application Operation (CDC) **Changes on Administration roles due to Personal Data Protection** Changes have been shipped to administration roles of almost all scenarios, due to Data Protection measures. For more information, see *Security Optimization Guide for SAP Solution Manager SP08*. **Support Hub Connectivity** As of SP08, the following SAP Backend RFCs are replaced by the **Support Hub Connectivity**: • `SAP-OSS` • `SAP-OSS-LIST-001` • `SAPNET_RTCC` • `SAPOSS` For more information on: • the configuration of the support hub connectivity, check the according step in transaction `SOLMAN_SETUP` → *System Preparation → Set Up Connections to SAP*. • the authorizations required to run the configuration, see *Secure Configuration Guide → View: System Preparation → Step 3.2 Support Hub Connectivity.* • data protection measures, see *Secure Optimization Guide → Data Privacy and Protection*.

Support Package Stacks (Version)	Date	Description
SP07	2018-05-14	**Composite Roles** As of SP07, composite roles in SAP Solution Manager are no longer supported. All business user definitions with accordingly assigned roles are available with their documentation in application Solution Manager User Administration (SMUA) and in transaction SOLMAN_SETUP. For more information on business users (Use Case IDs), see the according section in the *Authorization Concept Guide*. For more information on the application SMUA, see the *Secure Configuration Guide*. **Adaptations in Application Specific Guides** Changes have been made in regard to authorizations in the following scenario: • Application Operations • Change Management • Test Suite • Process Management • Root Cause Analysis (RCA) • Custom Code Management (CCM) • Technical Administration (License Management)
SP06		**Adaptations in Application Specific Guides** Changes have been made in regard to authorizations in the following scenario • Change Request Management • Requirements Management • ITSM Management • Quality Gate Management • Test Management
SP05	2017-05-08	**Template Dialog Users and Composite Roles** Template Users are available for all SAP Solution Manager scenarios in application *Solution Manager Users Administration* (SMUA) and *Template Users*, see more information on SMUA in the according section in the *Authorization Concept Guide*. **SAP Fiori Applications** All information on SAP Fiori Applications for usage in Central Hub are moved to a separate guide *SAP Fiori Application Security Guide*.

Support Package Stacks (Version)	Date	Description
SP04		**Adaptations in Application Specific Guides** Changes have been made in regard to authorizations in the following scenario • Change Request Management • Custom Code Management • Service Availability Management • Work Mode Management • Notification Management • System Monitoring • Data Volume Management • Test Management

Support Package Stacks (Version)	Date	Description
SP03	2016-08-15	**Default Users Created in Earlier Releases** • **⚠ Caution** Please check passwords for default users created within transaction `SOLMAN_SETUP` in earlier releases. See SAP Note 2293011. **Adaptations in Application Specific Guides** Changes have been made in regard to authorizations in the following scenario • Quality Gate Management (QGM) • Change Request Management • Requirement Management • Job Monitoring • BI-Monitoring (new: Data Readiness Monitoring) • PI-Monitoring • Message Flow Monitoring (new: SAP Fiori App) • BP Operations (new: Data Consistency Management and Business Process Improvement) • Process Management (new: Business Process Monitoring Graphics; Execution Analytics Dashboard; ITPPM) • Project Management • Custom Code Management • Data Volume Management • Test Management renamed Test Suite (new: Partner Test Management) • Application Operations (End-User Experience, new: Exception Management) • Value Management Dashboard • Business Process Change Analyzer • Incident Management • Services (EWA SAP Fiori App) **ⓘ Note** Scenario *Solution Documentation Assistant* is removed as to SAP Solution Manager Release 7.2.

Support Package Stacks (Version)	Date	Description
SP02		**Adaptations in Application Specific Guides** Changes have been made in regard to authorizations in the following scenario • BPCA • Process Management • Test Management • CBTA • BPO • System Monitoring • Interface Channel Monitoring • PI Monitoring • End-User Experience Monitoring (EEM) • DVM • Custom Code Management • Change Request Management • Incident Management • Requirement Management • ICi Dashboards (Value Management) • Service Engagement

Support Package Stacks (Version)	Date	Description
SP01	2015-12-11	**General Information** • As of Release 7.2, the security information is published within three separate guides: • *SAP Solution Manager Authorization Concept* This guide contains all information referring to the general concept of security and authorizations for the complete stack for SAP Solution Manager. • *Secure Configuration Guide* This guide contains all information referring to security aspects, users and authorizations used in transactions SOLMAN_SETUP and SMUA. In addition, users and authorization for the migration procedure for the process documentation are included. • *Application Security Guide* This guide contains all information referring to security aspects and authorizations for individual scenarios/applications. **Note** All relevant changes for the individual applications//scenarios are documented in the document history of the individual sections. **Adaptations in Application Specific Guides** • Changes have been made in regard to authorizations and roles in **all scenario roles**. • *Implementation* Transactions SOLAR01, SOLAR02, SOLAR_PROJECT_ADMIN are obsolete. All references to these transactions are deleted in the relevant user roles. For more information, see *Document History* of the according section Old user roles SAP_SOLAR_* are removed. New roles for *Embedded Search* and TREX Setup *Upgrade Dependency Analyzer* obsolete • *Migration Procedure* Authorizations are included in the relevant sections for configuration, see as well information in the *Secure Configuration Guide*. • New sections on SAP Fiori Application authorizations in the according scenario - specific sections • New scenario *Requirement Management* in ITSM **Note** Make sure to consult SAP Note 2250709 for any additional roles or changes.

2.2 List of Roles Updated per SP

Starting as of SP13, you can find here a list of all updated roles per SP. For each role, we recommend to check in the menu tab of the role in transaction PFCG for detailed change information.

Updated Roles per SP

SP	Roles
SP20	SAP_CM_SMAN_DEVELOPER
	SAP_SM_CALM_DATA_TRANSFER*
	SAP_SM_TSTR_THIRD_PARTY_INT
SP19	SAP_STWB_2_ALL
	SAP_STWB_2_DIS
	SAP_STWB_INFO_ALL
	SAP_STWB_INFO_DIS
	SAP_STWB_WORK_ALL
	SAP_STWB_WORK_DIS
	SAP_SM_TSTR_THIRD_PARTY_INT
	SAP_SM_REDWOOD_COMMUNICATION
	SAP_SM_SCHEDULER_ADMIN
	SAP_SM_SCHEDULER_TOP
	SAP_SM_ITSM
SP18	SAP_STWB_2_ALL
	SAP_TST_AGENT_RFC
SP17	SAP_SERVICE_CONNECT
	SAP_SERVICE_CONNECT_DISP
	SAP_SM_QGM_CM_ALL
	SAP_SM_QGM_CM_TRANSPORT
	SAP_SM_SL_ADMIN
	SAP_SM_SL_DISPLAY
	SAP_SM_SL_EDIT
	SAP_SOLMAN_READ_702
	SAP_STWB_WORK_ALL
	SAP_SDCCN_ALL
	SAP_CM_SMAN_ADMINISTRATOR
	SAP_CM_SMAN_OPERATOR

SP	Roles
SP16	• SAP_CM_SMAN_CHANGE_MANAGER • SAP_CM_SMAN_ADMINISTRATOR • SAP_CM_SMAN_DEVELOPER • SAP_CM_SMAN_RELEASE_MANAGER • SAP_CM_SMAN_OPERATOR • SAP_CM_SMAN_TESTER • SAP_SM_CBTA_ADMIN • SAP_SM_CHM • SAP_SM_ITSM • SAP_SM_SL_ADMIN • SAP_SM_SUTMAN_ADMIN • SAP_SM_SUTMAN_EDIT • SAP_SOCM_TESTER • SAP_SOCM_ADMIN • SAP_SOCM_REQUESTER • SAP_SOCM_DEVELOPER • SAP_SOCM_CHANGE_MANAGER • SAP_STWB_WORK_ALL • SAP_STWB_2_ALL • SAP_SUPPDESK_DISPATCH • SAP_SM_CHARM_EXTRACTOR • SAP_SDCCN_ALL

SP	Roles
SP15	• SAP_CM_SMAN_CHANGE_MANAGER • SAP_CM_SMAN_ADMINISTRATOR • SAP_CM_SMAN_DEVELOPER • SAP_CM_SMAN_RELEASE_MANAGER • SAP_CM_SMAN_OPERATOR • SAP_CM_SMAN_TESTER • SAP_SM_CBTA_ADMIN • SAP_SM_CHM • SAP_SM_ITSM • SAP_SM_SL_ADMIN • SAP_SM_SUTMAN_ADMIN • SAP_SM_SUTMAN_EDIT • SAP_SMWORK_DIAG • SAP_SOCM_ADMIN • SAP_SOLMAN_READ_702 • SAP_SOCM_CHANGE_MANAGER • SAP_SOLMAN_TMW_702 • SAP_STWB_2_ALL • SAP_SUPPDESK_DISPATCH • SAP_RCA_DISP • SAP_CM_SMAN_ADMINISTRATOR
SP14	• `SAP_CM_MANAGED_CTS_DEV` (with Software Component ST-PI 740 SP16) • `SAP_CM_MANAGED_CTS_OPERATOR` (new with Software Component ST-PI 740 SP16) • `SAP_CM_MANAGED_CTS_CHANGEM` (new with Software Component ST-PI 740 SP16) • `SAP_CM_MANAGED_CTS_TESTER` (new with Software Component ST-PI 740 SP16) • `SAP_CM_MANAGED_CTS_ADMIN` (new with Software Component ST-PI 740 SP16) • `SAP_SM_COMM` • `SAP_STWB_WORK_ALL` • `SAP_CM_MANAGED_CTS_DEV` • `SAP_CM_SMAN_OPERATOR` • `SAP_SDCCN_ALL` • `SAP_SOLMAN_TMW_702` • `SAP_SOLMAN_READ_702` • `SAP_SM_SL_ADMIN` • `SAP_SM_TSTR_THIRD_PARTY_INT`

SP	Roles
SP13	SAP_CCLM_ALL
	SAP_CCLM_DIS
	SAP_DVM_SERVICE
	SAP_CM_SMAN_ADMINISTRATOR
	SAP_OP_DSWP_BPM
	SAP_OP_DSWP_BPM_DIS
	SAP_SETUP_BASIC_ARCHIVE
	SAP_SETUP_NOTEDOWNLOAD
	SAP_SETUP_SYSTEM_PREP
	SAP_SM_BASIC_SETTINGS
	SAP_SM_ITSM
	SAP_SM_TSTR_THIRD_PARTY_INT
	SAP_SOLMAN_READ_702
	SAP_SOLMAN_TMW_702
	SAP_STWB_WORK_ALL
	SAP_STWB_WORK_DIS
	SAP_SM_ECET
	SAP_TM_CONFIG
	SAP_SMWORK_TECH_MON

2.3 Adapting SAP Documentation (Help Text IDs) for Users and Roles to Your Needs

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

Adapt SAP Documentation to Your Own Purposes

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

Find and Check SAP Documentation

1. Open 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 the *Display* button.
   The system displays the text, which is also linked in SAP Solution Manager Configuration.

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

Adapt SAP Documentation or Create Your Own

1. Open transaction SE61.
2. Choose *Document Class* **General text** (TX).
3. Choose your language.
4. In both cases, when you adapt or when you create documentation, enter the new technical ID of the help text.

   > → Tip
   >
   > When you adapt the SAP documentation, use a common namespace for your documentation technical ID. Copy the SAP technical ID and substitute either namespace AUTH, USER or TP with your own namespace.
5. Choose the *Change* button.
   The system displays the text. Adapt the text to your needs.

2.4 Overview: SAP Cloud Integrations

SAP Cloud Platform

This section lists all scenarios with integrations to SAP Cloud Platform. A more detailed description is given in the application section to which the integration belongs.

For a general overview on the SAP Cloud Platform, see SAP Cloud Platform Planning and Life-Cycle Management Guide:

Applications with SAP Cloud Platform Integrations

Application	Additional Notes
Change Request Management	Transport Management Related Tasks

SAP Cloud ALM

This section lists all scenarios with integrations to SAP Cloud ALM. A more detailed description is available in the respective application help and security guide.

Applications with SAP Cloud ALM Integrations

+	Application	Additional Notes
Process Management	For more information, see Selective Data Transfer Security Guide	
Test Management		

2.5 Overview: Capabilities/Functions

The following table gives you an overview over the functions covered in this guide and which launchpad group, scenario, and specific guide they belong to.

Specific Functions	Launchpad Group, Scenario, or Specific Guide
System, host, database monitoring	Technical Administration
PI monitoring	
BI and HANA monitoring	
User experience monitoring	
Channel monitoring	
Self-monitoring	
Infrastructure monitoring	
Message flow monitoring	

Specific Functions	Launchpad Group, Scenario, or Specific Guide
BI reporting	Technical Monitoring Test Suite Incident Management SAP Solution Manager Administration Business Process Operations Change Management / Change Control Management DVM
Project Management	Implementation and Upgrade SAP Solution Manager Administration Change Management
Roadmaps	Implementation and Upgrade Change Management
Process documentation	
Business functions	
Customizing distribution	
BC Set activities	
Help Center	
Learning Maps	
Digital signature	
Document management	Implementation and Upgrade Test Suite Change Management
Test automation	Test Suite
Test plans, test packages	
Test information	
Testing	
Test Workbench	
Extended capabilities	
TBOMs	Test Suite / Business Process Change Analyzer

Specific Functions	Launchpad Group, Scenario, or Specific Guide
Business Process Change Analyzer	Test Suite / Business Process Change Analyzer
Incident Management	Incident Management
Job Management	Job Management
Issue Management	SAP Engagement and Service Delivery
Support Requests	
Services	
Expert on demand	
Service Level Reporting	
Security Optimization Service	
SAP Early Watch Alert (SDCCN)	SAP Engagement and Service Delivery Root Cause Analysis
Work Mode Management	Technical Administration
MDM Administration Cockpit	
Notification management	
IT calendar	
IT event	
IT Task Inbox	
IT Task Planner	
Service availability management	
Guided procedure	
Cross-database comparison	Business Process Operations
Business Process Monitoring	
Business Process Analytics	
Change Request Management	Change Management Implementation Quality Gate Management
cProjects	
Retrofit	

Configuration Validation	
System Recommendation	
Quality gate management	Quality Gate Management
Data volume management	Data Volume Management
Custom code lifecycle management	Custom Code Lifecycle Management
Custom code analysis	
Component-based test automation (CBTA)	Test Suite / Business Process Change Analyzer

2.6 Overview: SAP Solution Manager Functions Integration

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

For more information, see the scenario-specific guides.

How to read the table

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

1. Process Management
2. CDMC
3. Customizing Distribution
4. Document Management
5. Alert Inbox
6. Project Management
7. Business Process Change Analyzer
8. Incident Management
9. Issue Management
10. Test Management
11. Business Process Monitoring
12. Change Request Management
13. Job Management
14. SAP Engagement and Service Delivery
15. Root Cause Analysis
16. Technical Monitoring
17. Notification Management (Instant Notification)
18. Quality Gate Management

19. Configuration Validation
20. Data Volume Management
21. Exception Management
22. Guided Procedure Browser
23. CBTA
24. cProject
25. IT Calendar
26. Message Flow Monitoring
27. Work Mode Management
28. Service Availability Management
29. BI Reporting
30. Dashboards

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1		X	X	X		X	X	X	X	X	X	X	X																	
2	X																													
3	X																													
4	X						X																							
5																									X		X			
6	X																													
7	X			X						X		X											X							
8	X				X					X	X	X	X			X					X				X	X				
9	X																	X												
10	X						X	X				X									X		X							
11	X												X			X	X					X								
12	X						X	X					X					X						X	X					
13	X															X														
14																														
15														X		X														
16													X							X	X									
17											X					X					X						X			
18												X																		

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
19												X																		
20																														
21	X				X			X								X	X					X								
22																					X				X					
23							X			X																				
24												X												X						
25					X			X				X					X					X				X				
26								X									X					X								
27					X											X											X		X	
28																														
29																														
30																														

2.7 Overview: Third Party Products to Be Used with SAP Solution Manager

Here you find an overview of third party integration with individual scenarios. For more information, see the scenario-specific guide, section *External Integration*. For more information on security for external tools, see the corresponding documentation for the tool.

1. Implementation
2. Incident Management
3. Test Management (Partner Test Management)

4. Business Process Change Analyzer
5. Job Management

	1	2	3	4	5
Business Process Management Suite (NW CE)	X				
Enterprise Service Repository (PI)	X				
SAP Productivity Pak by RWD	X				
Service Desk		X			
HP QC			X		
ECatt			X		
Test Tools			X		
IBM Rational Test Management Tool			X		
SAP TAO				X	
SAP CPS					X

2.8 SAP Solution Manager Business Roles Overview

The following table gives an overview over all relevant business roles for SAP Solution Manager. All business roles are of type *Dialog User*. All business roles contain a specific role assignment, and can be used as reference or template users in the system.

> **Note**
>
> If you want to use such a user productively, you must modify its role assignment accordingly.

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
CBTA Configurator					Test Management: CBTA

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
CBTA Test Engineer					
CBTA Test Coordinator (Read User)					
BPCA Configurator					Business Process Change Analyzer (BPCA)
BPCA Quality Expert			X	X	
BPCA Business Process Expert			X	X	
BPCA Read User				X	
BPCA ECATT User				X	
BPO Configurator					Business Process Operation (BPO)
BPO Administrator			X	X	
BPO Analytics and Reporting User			X	X	
BPO Alert User			X	X	
BPO CDC User				X	
BPO Read User				X	
ChaRM Configurator					Change Request Management (ChaRM)
ChaRM Requester					
ChaRM Change Manager			X	X	
ChaRM Developer				X	
ChaRM Tester				X	
ChaRM IT Operator			X	X	
ChaRM Administrator			X	X	
ChaRM Release Manager				X	
Configuration Validation Administrator					Configuration Validation

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
Configuration Validation Read User					
CCM Configurator					Custom- Code Life Cycle Management (CCM)
CCM Admninistrator			X		
CCM Read User			X		
DVM Configurator					Data Volume Management (DVM)
DVM Administrator			X	X	
DVM Read User			X	X	
Exception Management Configurator					Exeption Management
Exception Management Cockpit User					
Exception Management Read User (SAPSUPPORT)					
Hana and PI Monitoring Configurator					Hana and PI Monitoring
Hana and PI Monitoring Level 1					
Hana and PI Monitoring Level 2			X		
ICI Configurator					Value Management Dashboard (ICI)
ICI Admninistrator			X		
ICI Read User			X		
ICM Configurator					Interface Channel Monitoring (ICM)
ICM Level 1					
ICM Level 2			X		
Incident Management Configurator					IT Service Management

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
Incident Management Administrator			X		
Incident Management Processor			X		
Incident Management Key User					
Incident Management Dispatcher					
Incident Management Read User			X		
Infrastructure Monitoring Configurator					Infrastructure Monitoring
IT Task Inbox Configurator					Technical Administration: IT Task Inbox
IT Task Inbox Administrator					
IT Task Inbox Author					
IT Task Inbox IT Manager					
IT Task Inbox IT Operator					
IT Task Inbox Read User					
Job Management Configurator					Job Management
Job Management Administrator			X		
Job Management Technical Operator			X		
Job Management Business Process Operator			X		
Job Management Application Manager					
Job Management Level 1					
Job Management Level 2					

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
Job Management Read User					
Job Monitoring Configurator					Job Monitoring
Job Monitoring Level 1					
Job Monitoring Level 2			X		
MFM Configurator					Message Flow Monitoring (MFM)
MFM Level 1					
MFM Level 2			X		
PI Monitoring Configurator					PI Monitoring
PI Monitoring Level 1					
PI Monitoring Level 2			X		
PTM Configurator					Partner Test Management (PTM)
PTM Administration User					
PTM Read User					
Process Management Configurator					Process Management
Process Management Project Manager					
Process Management Application Consultant					
Process Management Read User					
Project Management Configurator					Project Management
Project Management Project Manager					
Project Management Team Member					

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
Project Management Read User (Missing as of SP03)					
QGM Configurator					Quality Gate Management (QGM)
QGM Project Administrator				X	
QGM IT Operator				X	
QGM Development Lead					
QGM Quality Manager				X	
QGM Quality Advisory Board Member					
QGM Read User (missing with SP03)					
Requirement Management Configurator					Requirement Management
Requirement Management Business Manager					
Requirement Management Business Process Expert					
Requirement Management Administrator					
IT Requirements Manager					
IT Requirements Administrator					
Requirement Management Solution Architect					
Requirement Management Read User					
SAM Configurator					Technical Administration: Service Availability Management (SAM)
SAM Administrator					
SAM Editor					

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
SAM Reviewer					
SAM Read User					
SAPSUPPORT					Root Cause Analysis
SAPSERVICE					SAP Engagement and Delivery
SEA Administrator					Scope and Effort Analyzer (SEA)
SEA Read User					
Solution Manager Configurator (SOLMAN_ADMIN)					Solution Manager Administration
Solution Manager Administrator					
Solution Manager Administration Read User					
System Monitoring Configurator					System, Connection, Interface Monitoring
System Monitoring Level 1 (Could be a READ?? User)					
System Monitoring Level 2 (Could be just a "User")			X		
System Recommendation Administrator					System Recommendation
System Recommendation Read User					
Technical System Administrator					Technical Administration
Technical System Administration Read User					
Test Management Configurator					Test Management
Tester Test Organizer			X		
Test Management Consultant			X		

Business Role	Use Case ID	User Documentation Help Text ID	BW System	Managed System	For Information, See Section...
Test Management Read User			X		
UXMON Configurator					End - User Experience Monitoring (UXMON)
UXMON Level 1					
UXMON Level 2			X		

2.9 Overview: VAR - Specific Chapters

This section provides an overview of chapters which are relevant for Value Added Resellers (VAR).

Section
ITSM: CRM Standard Customizing for SAP Solution Manager
Custom Code Development: User Roles in SAP Solution Manager
Custom Code Development: Main Authorization Objects

3 Technical Administration

3.1 Introduction

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

3.2 Document History

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

Support Package Stacks (Version)	Description
SP12	**Task Inbox** • adapted role `SAP_TASK_INBOX_ALL` • added role `SAP_SM_BATCH_RELE` to users with user IDs: `ITTM_ADM; ITTM_AUTH; ITTM_ITO`

Support Package Stacks (Version)	Description
SP01	**General** • First version **Adaptations to Previous Release 7.1 (Due to new Process Documentation functionality)** • Removed role SAP_SMWORK_BASIC* (obsolete) • Substituted roles SAP_SOL_PROJ_ADMIN_* and SAP_SM_SOLUTION_* with SAP_SM_SL_* **SAP Fiori Integration** • All users receive Embedded SAP Fiori related authorizations with role SAP_SM_FIORI_LP_EMBEDDED **Work Management Mode and EEM Robots** • SAP_SM_DTM_* substituted by SAP_SM_WMM_* in composite role for *Service Availability Management* and *Technical Monitoring* • new roles for EEM Robots: SAP_SM_EEM_ROBOT_* (substitute DTM roles only for EEM robot part)
SP03	**Technical Administration** • adapted role SAP_ITCALENDER • adapted role SAP_NOTIF_ADMIN (containing *Instant Notification*) **Redesign of Service Availability Management** • 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*
SP04	**Service Availability Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role SAP_SM_SAM_ALL **Work Mode Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles SAP_SM_WMM_* **Notification Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles SAP_NOTIF_* **SAP Solution Manager Administration** • moved the section to *Secure Configuration Guide*

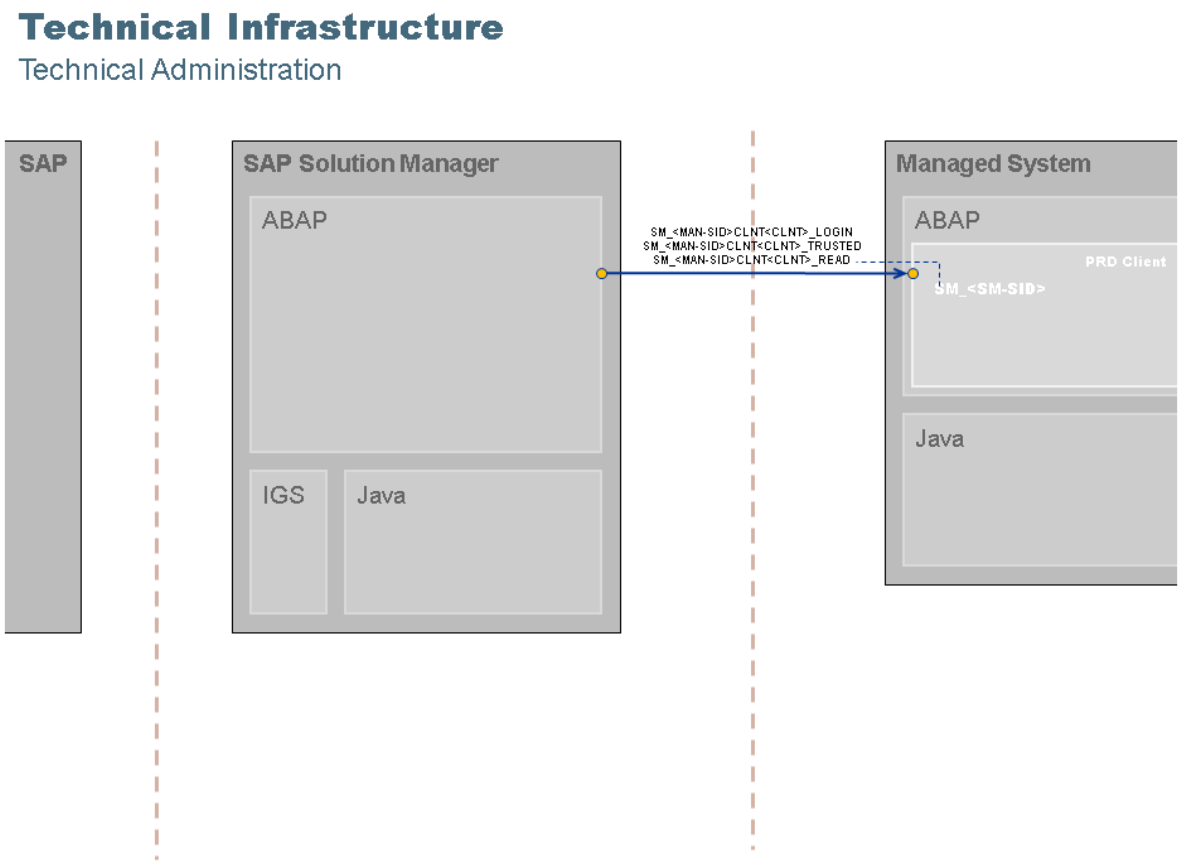
Support Package Stacks (Version)	Description
SP05	**Notification Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles `SAP_NOTIF_*` **Service Availability Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles `SAP_SM_SAM*` **IT Calendar** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles `SAP_ITCALENDAR*` **Technical Administration** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • New template users with Default ID: `TA_<user description>_<system ID>` added in the system, see the extention in this guide for section *Users and Authorizations*. The users are available in application *Solution Manager User Administration* (SMUA) in work center *SAP Solution Manager Administration* view *Users*. For more information on SMUA, see in the *Secure Configuration Guide* the according section. • adapted role `SAP_SMWORK_SYS_ADMIN` (new link, new tile group and catalogue for SAP Fiori)
SP06	**Service Availability Management (SAM)** Removed `SAM` configuration link *Service Availability Management Setup* from role `SAP_SMWORK_CONFIG`, as `SAM` is removed from the `SOLMAN_SETUP` transaction. **Technical Administration** Adapted navigation role `SAP_SMWORK_SYS_ADMIN`
SP07	**New Section on: License Management** New License Management Roles delivered, see sections on *License Management* and *Technical Administration Users*. **IT Calendar** • Updated roles for IT Calendar (Odata Service) • Possibility of IT Calendar for non - SAP Solution Manager users **IT Events** • Updated roles for IT Events (Odata Service) `SAP_SM_IT_EVENTS_*`
SP08 Plus	• adapted section on *Communication Channels* • removed section *Technical Users*

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.



Infrastructure

3.3.1.2 Configuration

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

> **Note**
>
> For conceptual information about configuration users in SAP Solution Manager, see the *Secure Configuration Guide*.

CRM Transaction Type

For IT Task Inbox and Guided Procedure, you require CRM relevant authorizations, due to the use of transaction type `SMOT`.

3.3.1.3 Communication Channels and Technical Users

The tables below show the communication channels and destinations used by SAP Solution Manager in this scenario, as well as the required technical users. For more information about the communication channel setup security and the relevant technical users, see section *Communication Channel Security* in the *Secure Configuration Guide*.

> **Note**
>
> All mentioned RFC destinations are automatically created in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`) under *Managed Systems*. For information, see the *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to SAP backend system	HTTPS	Technical Communication User	Search for SAP Notes
SAP Solution Manager to managed systems (Read) `SM_<SID>CLNT<Client>`	RFC	`SM_<SID of SAP Solution Manager>`	For *Notification Management* to fetch users and business partners
SAP Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	RFC	Named end-user (customer specific)	*IT Task Inbox and Guided Procedure*: RFC connections are only used for automated activities that can be used in the self-defined guided procedures.
SAP Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section *File Transfer Protocol (FTP)*
SAP Solution Manager to Exchange Server	LDAP		Reading distribution lists
SAP Solution Manager to Mail Server/SMS Sever	HTTP(S)/ RFC, SMTP		For e-mail and SMS

3.3.2 Users and Authorizations

3.3.2.1 IT Task Inbox and Guided Procedure

IT Task Planning allows you to plan guided procedures. The *IT Task Inbox* displays all available tasks that are assigned to a user, to a support organization, or that are planned for certain managed objects. When a user performs a task, the system opens a related guided procedure and the task is performed via the steps and activities of the guided procedure.

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

Scenario Configuration

You can configure the *IT Task Management* scenario in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`). You can create template users in the 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 in the following table:

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

> **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.

Single Role	Help Text ID
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL

Administration User (Technical Name: TP_ITTM_ADM)

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
SAP_SM_BATCH_RELE	AUTH_SAP_SM_BATCH

Authoring User (Technical Name: TP_ITTM_AUTH)

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_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_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBEDDED

Single Role	Help Text ID
SAP_SM_BATCH_RELE	AUTH_SAP_SM_BATCH

IT Manager (Technical Name: TP_ITTM_ITM)

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_DIS	AUTH_SAP_ITCALENDER_DIS
SAP_TASK_INBOX_DIS	AUTH_SAP_TASK_INBOX_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
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

IT Operator (Technical Name: TP_ITTM_ITO)

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_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_GP_EXE	AUTH_SAP_SM_GP_EXE
SAP_TASK_PLANNING_DIS	AUTH_SAP_TASK_PLANNING_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_BATCH_RELE	AUTH_SAP_SM_BATCH

Display User (Technical Name: TP_ITTM_DIS)

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_DIS	AUTH_SAP_SYSTEM_REP_DIS
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

Authorization Objects

SM_TP_AUTH

The authorization object is used to restrict on activities for the task plan. It is contained in roles SAP_TASK_PLANNING*.

SM_ITE_ACT

This object is contained in roles SAP_SM_IT_EVENTS*. It can be used to control the access to IT events in the IT calendar.

3.3.2.2 Technical Administration Users

Here, you can find an overview of users as recommended by SAP and their corresponding user roles assignment for Technical Administration.

Template Users

You can use template users with default ID TA_<user description>_<system ID>. The users are available in the Solution Manager User Administration (SMUA) application in the *SAP Solution Manager Administration*

launchpad group, in the *User Administration* application. For more information about SMUA, see in the *Secure Configuration Guide*.

> → Tip
>
> If you search for users for Technical Administration in the *User Administration* application, filter in the *Used In* column for the *Empty* entry. This entry filters all users for scenarios and functions that are not represented in any of the configuration scenarios in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`), and are therefore **only** available in SMUA.

> ⓘ Note
>
> The roles for Technical Administration contain all relevant single roles for all sub-scenarios.

Administrator User TA_ADM_XXX (Help Text ID: TP_TA_ADM)

Single Role	Help Text ID
SAP_SM_WMM_ALL	AUTH_SAP_SM_WMM_ALL
SAP_SM_EEM_ROBOT_ALL	AUTH_SAP_SM_EEM_ROBOT_ALL
SAP_SM_ADMIN_COMPONENT_ALL	AUTH_SAP_SM_ADMIN_COMP_ALL
SAP_NOTIF_ADMIN	AUTH_SAP_NOTIF_ADMIN
SAP_ITCALENDAR	AUTH_SAP_ITCALENDAR
SAP_TASK_INBOX_ALL	AUTH_SAP_ITCALENDAR
SAP_SM_IT_EVENTS_ADMIN	AUTH_SAP_SM_IT_EVENTS_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_GP_ADMIN	AUTH_SAP_SM_GP_ADMIN
SAP_SM_SAM_ALL	AUTH_SAP_SM_SAM_ALL
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_TASK_PLANNING_ALL	AUTH_SAP_TASK_PLANNING_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Display User TA_DIS_XXX (Help Text ID: TP_TA_DIS)

Single Role	Help Text ID
SAP_SM_WMM_DIS	AUTH_SAP_SM_WMM_DIS
SAP_SM_EEM_ROBOT_DIS	AUTH_SAP_SM_EEM_ROBOT_DIS
SAP_SM_ADMIN_COMPONENT_DIS	AUTH_SAP_SM_ADMIN_COMP_DIS
SAP_NOTIF_DISP	AUTH_SAP_NOTIF_DISP
SAP_ITCALENDAR_DIS	AUTH_SAP_ITCALENDAR_DIS
SAP_SM_IT_EVENTS_DISP	AUTH_SAP_SM_IT_EVENTS_DISP
SAP_TASK_INBOX_DIS	AUTH_SAP_TASK_INBOX_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REPOSITORY_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_GP_DIS	AUTH_SAP_SM_GP_DIS
SAP_SM_SAM_DIS	AUTH_SAP_SM_SAM_DIS
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_TASK_PLANNING_DIS	AUTH_SAP_TASK_PLANNING_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

IT Calendar Application

The roles SAP_ITCALENDAR* contain main authorizations for the IT Calendar. For more information, see IT Calendar [page 51].

Notification Management Authorization Object SM_CNM_AUTH

The role for *Notification Management* SAP_NOTIF_ADMIN contains:

- *Global Recipient Notification* with authorization object SM_NOTI_TA to maintain recipient lists
- *Central Notification Management (CNM) - Instant Notification* (as a feature of Gateway services) - enhanced version of *Global Recipient Notification* with authorization object SM_CNM_AUT to schedule notifications
- Access to **Data Resource Management (DRM)**, **IT Events (ITE)**, **Work Mode Management (WMM)**, and is used in these functions

Guided Procedures Role SAP_SM_GP_ADMIN

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, you need to deactivate these objects in the role SAP_SM_GP_ADMIN.

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.

Here, you find an overview of users as recommended by SAP and their corresponding user roles assignment for SAM. All users are assigned a composite role, which contains a number of single roles.

Configuration

You configure SAM in SAP Solution Manager Configuration (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:

Role	Help Text-ID
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP_DISP
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONF
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
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
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL

> ### Note
>
> For conceptual information about configuration users in SAP Solution Manager, see the *Secure Configuration Guide*.

Administrator (Help Text ID: TP_SAM_ADMIN)

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_WMM_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)

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_WMM_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_EDIT)

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_WMM_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)

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_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Authorization Objects

The authorization objects for SAM are SM_SAM*.

3.3.2.4 License Management

The roles for License Management are part of the use case ID SA_* to use *Technical Administration*. The following tables display roles that are relevant if only License Management is allowed for a user.

Administrator

Role	Help Text ID
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_LICMAN_ALL	AUTH_SAP_SM_LICMAN_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Display User

Role	Help Text-ID
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_SYS_ADMIN	AUTH_SAP_SMWORK_SYS_ADMIN
SAP_SM_LICMAN_DIS	AUTH_SAP_SM_LICMAN_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Authorization Objects

License Distribution

The authorization object protecting the distribution of licenses over systems is SM_LIC.

Running Background Job REFRESH_ADMIN_DATA_FROM_SUPPORT

The background job is scheduled by the License Management user using transaction SA38, executed by background job user SOLMAN_BTC. For more information, see SAP Note 1280664.

Authorization Group for Authorization Object S_TABU_DIS

The authorization group used is SM_LIC.

Log Authorization

License Management uses transaction SLG1 with object SOLAR for logging information.

3.3.2.5 IT Calendar

The roles `SAP_ITCALENDAR*` contain main authorizations for the IT Calendar.

If you want to use the external IT Calendar application to share in your Intranet, see SAP Note 2616516.

> **Note**
>
> IT Calendar application can be accessed by non - SAP Solution Manager users based on generated URL link that includes pre-selected Technical Scenarios / Systems. The application is launched via a display user.
>
> The IT Administrator generates the URL with the pre-defined login credentials with some pre-selected technical systems and scenarios, which you can then share with external users.

Notification Management Authorization Object SM_CNM_AUTH

The role for *Notification Management* `SAP_NOTIF_ADMIN` contains:

- *Global Recipient Notification* with authorization object `SM_NOTI_TA to maintain recipient lists`
- *Central Notification Management (CNM) - Instant Notification* (as a feature of Gateway services) - enhanced version of *Global Recipient Notification* with authorization object `SM_CNM_AUT` to schedule notifications
- allows access to Data Resource Management (DRM), IT Events (ITE) , Work Mode Management (WMM) and it used in these functions

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.

> **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).

CRM 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*.

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 Process Management and Test Suite

4.1 Document History

The following changes to the specific scenario guide were made for each Support Package:

Support Package Stack (Version)	Description
SP20	Process Management - Selective Data Transfer → Tip • For security recommendations, see the *Security Guide for Selective Data Transfer* on the Service Marketplace. • For online help documentation, see Help Documentation **Test Suite** See the *Menu* tab in the specified roles for information on authorization object changes. • Adapted role `SAP_SM_TSTR_THIRD_PARTY_INT`

Support Package Stack (Version)	Description
SP19	Process Management - Selective Data Transfer → Tip • For security recommendations, see the *Security Guide for Selective Data Transfer* on the Service Marketplace. • For online help documentation, see Help Documentation **Test Suite** See the *Menu* tab in the specified roles for information on authorization object changes. • Adapted role `SAP_SM_TSTR_THIRD_PARTY_INT` • Adapted role `SAP_STWB_2_ALL` • Adapted role `SAP_STWB_2_DIS` • Adapted role `SAP_STWB_WORK_ALL` • Adapted role `SAP_STWB_WORK_DIS` • Adapted role `SAP_STWB_INFO_ALL` • Adapted role `SAP_STWB_INFO_DIS` Additional information on customizing transactions for role `SAP_TM_CONFIG` Added new authorization object `SM_TFLW` (allow test sequence in Test Suite applications)
ST SP18 / ST-PI SP23	**Test Suite** See the *Menu* tab in the specified roles for information on authorization object changes. • Adapted role `SAP_STWB_2_ALL` • Adapted role `SAP_TST_AGENT_RFC` (delivered with *ST-PI SP23*)
SP16	**Test Suite - Third Party Integration** See the *Menu* tab in the specified roles for information on authorization object changes. • Shipped new role `SAP_SM_TSTR_THIRD_PARTY_INT` • Adapted role `SAP_STWB_2_ALL` • Adapted role `SAP_STWB_WORK_ALL` For the integration with Third Party tools, a technical user `SM_TSTR_INT` is required. The user and its role assignment are integrated into the Guided Procedure for Test Suite. For more information, see section on *Third Party Integration*.

Support Package Stack (Version)	Description
SP15	**Test Suite** See the *Menu* tab in the specified roles for information on authorization object changes. • Adapted role `SAP_SM_SUTMAN_ADMIN` • Adapted role `SAP_SM_SUTMAN_EDIT` • Adapted role `SAP_SM_CBTA_ADMIN` **Process Management** • Adapted roles `SAP_SM_SL_ADMIN`
SP14	**Test Suite** See the *Menu* tab in the specified roles for information on authorization object changes. • Adapted role `SAP_STWB_WORK_ALL`
SP13	**Test Suite** • Term adjustment from Test Management to Test Suite • Extended section *Additional Security Measures* for application log information • Removed CRM customizing from section *User Roles for CBTA* as this is not required anymore • Added new section *System Under Test (SUT) Management* to *Additional User Roles* **E-Catt Integration** • Adapted role `SAP_SM_ECET` **Test Management** • Adapted role `SAP_STWB_WORK_DIS` • Adapted role `SAP_STWB_WORK_ALL` • Adapted role `SAP_TM_CONFIG` **CDMC (Process Management)** **⚠ Restriction** The function of CDMC is not allowed in SAP S/4 HANA 2020 systems.
SP12	**Section on Component Based Test Automation (CBTA)** • Added information on file storage for test script files.

Support Package Stack (Version)	Description
SP11	**Role SAP_SM_CBTA_TRANSPORT** Substituted role SAP_SM_CBTA_TRANSPORT with role SAP_SM_GEN_TRANSPORT for the following use case IDs: • TP_CBTA_TC • TP_CBTA_TE • TP_TM_BC adapted role SAP_TST_AGENT_RFC
SP10	**Process Management** • Adapted roles SAP_SM_SL_* **Test Management** • Adapted roles SAP_STWB_2_* • Adapted role SAP_STWB_INFO_ALL • Adapted role SAP_STWB_WORK_ALL with ACTVT **UP**, for testers to be able to upload attachments to test packages • Added section on *Authorizations of Interface Documentation* in section *Additional Functions*.
SP09	**Test Management** • Business partners are created for every creation of a new template user in transaction SOLMAN_SETUP. • Adapted role SAP_STWB_2_ALL **Process Management** • Refined combination of authorization objects SM_GAL_GO (diagram objects) and SM_SDOC (process management access) by adding a new ACTVT 68 (model) to SM_SDOC. For more information, see section *Authorization Objects* in scenario-specific guide *Process Management*. • Adapted roles SAP_SM_SL_EDIT_BPMN and SAP_SM_SL_ADMIN • Adapted role SAP_SL_CONFIG

Support Package Stack (Version)	Description
SP08 Plus	**Process Management** • adapted *Communication Channels* section • removed *Technical Users* section • new *Running Individual Background Jobs with Specific Users* section **BPCA** • adapted *Communication Channels* section • removed *Technical Users* section • new *Technical User for ECatt* section **Test Management and SEA** • adapted *Communication Channels* section • removed *Technical Users* section

Support Package Stack (Version)	Description
SP01	**General** • First general version **General Adaptations to Previous Release 7.1 (Due to new Process Documentation functionality)** • Removed roles SAP_SMWORK_BASIC* and SAP_SM_BI_BILO (obsolete) • Substituted roles SAP_SOL_PROJ_ADMIN_*, SAP_SOLAR_* and SAP_SM_SOLUTION_* with SAP_SM_SL_* • Substituted roles SAP_SOL_KW_* with SAP_SM_KW_* **Obsolete Authorization Objects** • SM_UDA_PRJ • D_SOL_VSBL • D_SOLM_ACT • D_SOL_VIEW • S_PROJECT • S_PROJECTS • S_PROJ_GEN **Additional Security Measures in BPCA** • Authorization group BPCA added to all relevant tables and authorization group S_TABU_DIS. • Authorization object S_RFC confined in all relevant roles • Added roles for Business Partners and Test Management Information System **Test Management** • New composite roles SAP_TEST_*_COMP • Substituted role SAP_SM_SL_EDIT with role SAP_SM_SL_DISPLAY in all composite roles • Substituted role SAP_SM_KW_DIS with role SAP_SM_KW_ALL in all composite roles but display role • Added SAP_SUPPDESK_CREATE to all composite roles • Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_TEST_MAN was transferred into roles: SAP_STWB_*, and SAP_STCE_*. • To call the old work center, use transaction STWB_OLD. You can restrict the views for both work centers within the authorization field help for authorization object SM_WC_VIEW. **SEA** • Removed Maintenance Optimizer roles **Process Documentation** • Roadmap authoring environment is obsolete, therefore corresponding roles SAP_RMDEF_RMAUTH_* are obsolete and removed from delivery **Project Management (ITPPM)**

Support Package Stack (Version)	Description
	• New template users and configuration user • Specific end - user authorization roles for `ITPPM: SAP_SM_ITPPM_*` • Specific configuration role: `SAP_ITPPM_CONFIG` **SAP Fiori Integration** • All users receive authorization for SAP Fiori embedded launchpad (role: `SAP_SM_FIORI_LP_EMBEDDED`)
`SP02`	**BPCA** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted single role `SAP_BPCA_CONFIG` **Process Management** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted single roles `SAP_SM_SL_*` (additional transaction codes `SOLDOC` and `SOLADM`) **Test Management** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted role `SAP_WDA_TST_RFC` **CBTA** All changes within roles are documented in the *Menu* tab of the respective role: • adapted role `SAP_CBTA_DIS_COMP` • adapted role `SAP_TST_AGENT_RFC`

Support Package Stack (Version)	Description
SP03	**Business Process Graphical Modelling within Process Management** • Adapted roles SAP_SM_SL_ADMIN and SAP_SM_SL_DISPLAY with specific BPMN authorization • New additional role for Process Management specifically for BPMN maintenance: SAP_SM_SL_EDIT_BPMN **Process Management** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted single role SAP_SM_SL_ADMIN (additional authorization field value in object SM_SDOCADM - Site) • Adapted single roles SAP_SM_SL_ADMIN and SAP_SM_SL_EDIT for *Custom Interface Maintenance* • Added single role SAP_SM_DSH_DISP to all standard users (Dashboard) **Project Management** • Extended section on ITPPM in regards of E2E process integration with *Issue Management*. • Added single role SAP_SM_DSH_DISP to all standard users (Dashboard) • Added single role SAP_SMWORK_IMPL to Administrator user **Solution Documentation Assistant** • Section removed **Test Management** All changes within roles are documented in the *Menu* tab of the respective role: • According to redesigned BW reports, new BW related role: SAP_BI_E2E_SMT • New roles for *Partner Test Management*, see corresponding section • Removed sections for Partner Test Management products for QC by HP and IBM Rational **Business Process Change Analyzer** All changes within roles are documented in the *Menu* tab of the respective role: • Added SAP_STWB_WORK_DIS to the display user • Substituted role SAP_SM_SL_DISPLAY with SAP_SM_SL_EDIT in composite role SAP_BPCA_ECATT_COMP • New role SAP_SM_BPCA_PTM_INT to integrate Partner Test Management and BPCA for configuration users. They share some configuration steps that are optional on both sides. Therefore, this role contains the delta information for these steps.

Support Package Stack (Version)	Description
SP04	**CBTA** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted role SAP_SM_TST_RFC **Test Management** All changes within roles are documented in the *Menu* tab of the respective role: • Added role SAP_STWB_2_DIS to Tester user • Added role SAP_STCE_DIS to Display user **Process Management** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted single roles SAP_SM_SL_* (added authorization object S_RFC_ADM) • Roles SAP_RMMAIN_* are obsolete in 7.2, only display allowed for Roadmaps resulting from 7.1

Support Package Stack (Version)	Description
SP05	**Test Management** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted role SAP_TM_CONFIG for GP *Test Automation Preparation* in area *Test Suite* in transaction SOLMAN_SETUP • Added template users and roles in SOLMAN_SETUP for Test Suite in GP *Test Suite Preparation*. User default ID: TM_<user description>_<system ID>. For more information, see *Users and Authorizations* in *Test Management* section. • Added role SAP_SM_DSH_DISP to template end- user for display • Added role SAP_SM_DSH_CONF to template end- user for PM • Adapted role SAP_STWB_2_* • Added new section *Main Authorization Objects* • Added roles SAP_SETUP_BASIC_ARCHIVE and SAP_SM_BI_ADMIN to SMC_TM user **CBTA** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted authorization object SM_SUTMNG by extending fields for System ID restriction. Note: the roles SAP_SM_SUTMAN* must either be adapted, or you can adapt the authorization object in your own roles by removing the current one and explicitly adding SM_SUTMNG again. • Adapted roles SAP_SM_SUTMAN* **BPCA** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted role SAP_SM_BPCA_TBOM • Added single role SAP_SMWORK_IMPL to user *Quality Expert* (composite role SAP_BPCA_ALL_COMP) to display *Process Management* tiles in SAP Fiori **ECATT - Integration** All changes within roles are documented in the *Menu* tab of the respective role: • ECATT roles are adapted, see SAP Note 2417261 **Customizing Distribution** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • New template users with Default ID: CD_<user description>_<system ID> added in the system, see the extension in this guide for section *Customizing Distribution.* The users are available in application *Solution Manager User Administration* (SMUA) in work center *SAP Solution Manager Administration* view *Users*. For more information on SMUA, see the corresponding section in the *Secure Configuration Guide*. **Project Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role.

Support Package Stack (Version)	Description
	• Added new dashboard ID (`DSHID`) for Dashboard *Project Analytics* to role `SAP_SM_DSH_DISP_ITPPM`. **Process Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • The following roles are obsolete: • `SAP_SOL_BC_COMP` • `SAP_SOL_TC_COMP` • `SAP_SOL_RE_COMP` Removed the corresponding sections in this guide. For users and roles, see template end users in transaction `SOLMAN_SETUP` or *Solution Manager User Administration* SMUA tool. • Adapted role `SAP_SL_CONFIG` with authorization object `S_DEVELOP` and value `ENBC` for BAdI implementation • Adapted role `SAP_SM_SL_ADMIN` with test plan prompt authorization object `SM_TPLN` • Added roles `SAP_SM_SUTMAN_ADMIN` to `SOLD_ADM` user due to system data container prompts when maintaining solutions or logical components **ITPPM** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. `ACO_SUPER (ACTVT 03)` • adapted roles `SAP_SM_ITPPM_*` with authorization object . **Partner Test Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role `SAP_PTM_CONF` • adapted roles `SAP_TMT*` with authorization object `SM_WD_COMP` value `WDC_ADAPTER_ADMIN_CENTER` to restrict adapter application.

Support Package Stack (Version)	Description
SP06	**Test Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role SAP_STWB_2_ALL (allow the test coordinator to access the tester worklist of a tester and work on his behalf, mass update test Package and Test Plans) **Partner Test Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles SAP_TMT_*** with new authorization object SM_TS_PTM **Process Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role SAP_SM_SL_ADMIN with S_DEVELOP authorization to automatically create system containers in SUT Management **Project Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Adapted role SAP_SM_DSH_ITPPM with a new Dashboard ID for *Cycle Reporting with Dashboard Builder* for ITPPM. **Effort and Scope Management (SEA)** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Redesign of users of SEA, see section on SEA • Template users for SEA: SMC_SEA_***, SEA_ADM_***, SEA_DIS_***
SP06	**Test Suite** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Adapted role SAP_STWB_2_ALL (allow mass update for Test Plans) **Process Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Adapted role SAP_SM_SL_ADMIN Added ACTVT 01 (create) and 02 (change) to S_DEVELOP with object type ECSD (for refresh of system data containers of test workbench when logical component groups are maintained)
SP07	**Process Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Adapted role SAP_SL_CONFIG

Support Package Stack (Version)	Description
SP08	**BPCA** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted role SAP_SM_BPCA_TBOM for managed systems • Adapted roles SAP_SM_BPCA_* for managing systems **Effort and Scope Management (SEA)** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Added role SAP_BI_E2E_BPCA to Use Case IDs SEA_ADM_*** and SEA_DIS_*** **Test Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Adapted role SAP_STWB_2_ALL • Adapted role SAP_STCE_ALL • Adapted section *Main Authorization Object* for Documents Management object S_SMDDOC. **CBTA** All changes within roles are documented in the *Menu* tab of the respective role: • Adapted role SAP_SM_TCE_RFC for managed systems **Process Management** Extended *Technical Users* section on how to trace and run background job with a specified technical user other than SOLMAN_BTC.

4.2 Getting Started

SAP Solution Manager covers a wide range of scenarios that you can use. As a customer, you can start with one scenario and add another scenario to your landscape later on. Therefore, SAP delivers scenario-specific security guides that 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 setting 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:

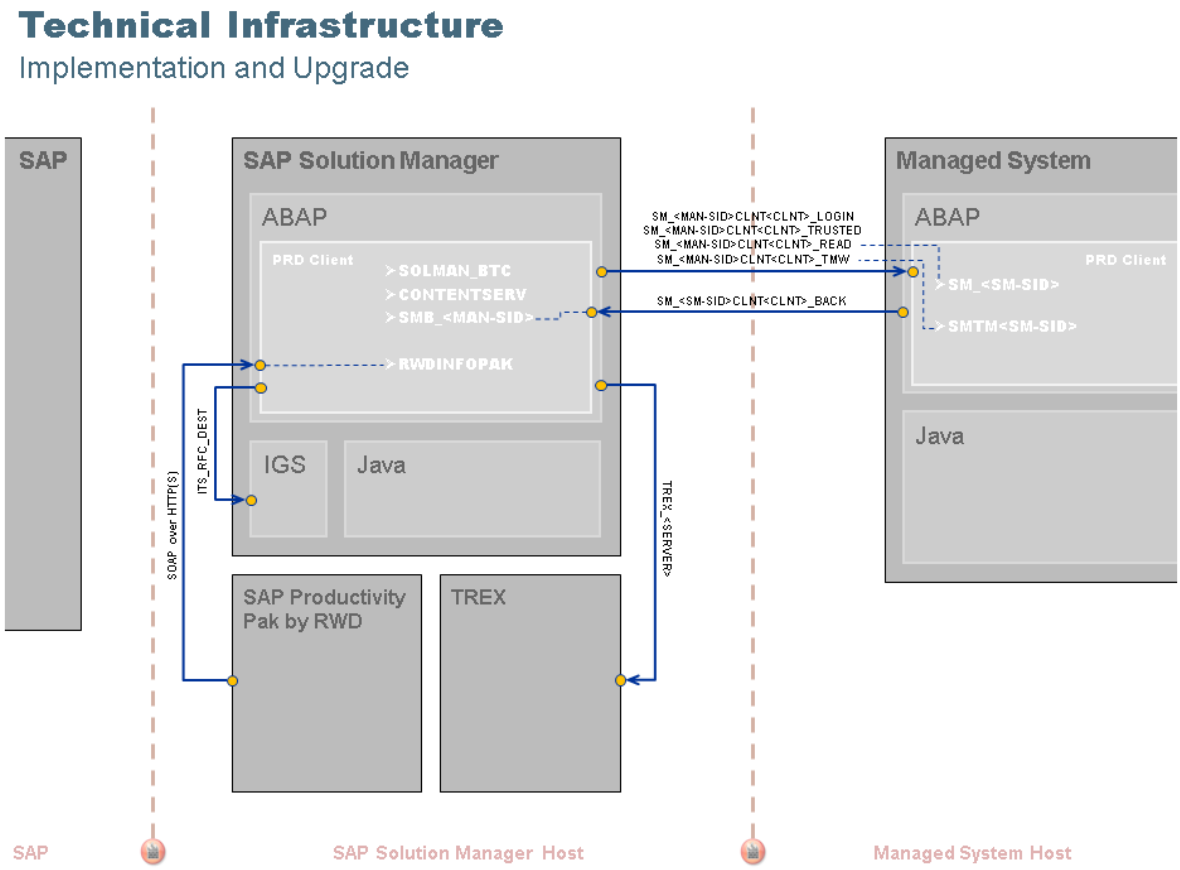
- **Getting Started:** Learn about target groups of this guide. Links for any additional components you can find in the Core Guide.
- **Prerequisites:** Learn about the specific system landscape components such as RFC - destinations and technical users, and how they connect to each other.
- **Users and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

4.3 Scenario-Specific Guide: Process Management

4.3.1 Prerequisites

4.3.1.1 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 the SAP Productivity Pak application by ANCILE to the SAP Solution Manager via specified destinations. For more information on all connections, when they are used, and which technical users are required, see the following sections.



Implementation and Upgrade

4.3.1.2 Configuration User

Basic Configuration SOLMAN_SETUP

You can productively use *Process Documentation* after you have completed the following steps:

1. Migration of solutions/projects from SAP Solution Manager 7.1 to 7.2. For more information about the Solution Documentation content activation procedure, see the corresponding section in the *Secure Configuration Guide*.
2. Configuration procedure for *Process Management* in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`).

Configuration User SMC_SOLD_XXX

Single Role	Help Text
SAP_ESH_CR_ADMIN	No help text ID; The roles are required to configure TREX
SAP_ESH_TRANSPORT	**Note** *Embedded Search* is a main function for document search, which is also used in other scenarios.
SAP_BC_SES_ADMIN	
SAP_SM_ESH_ADMIN	
SAP_SL_CONFIG	AUTH_SAP_SL_CONFIG
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
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
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_DISP	AUTH_SAP_SETUP_BASIC
SAP_SETUP_MANAGED_DISP	AUTH_SAP_SETUP_MANAGED
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP_DISP
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL

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

Critical Authorization Objects

S_DEVELOP

Role `SAP_SL_CONFIG` contains `ACTVT 02` (change) authorization for BAdI implementaions (value `ENBC`).

4.3.1.3 Communication Channels and Technical Users

The tables below show the communication channels and technical users required by SAP Solution Manager in this scenario.

> **Note**
>
> All mentioned `RFC` - destinations are automatically created via transaction `SOLMAN_SETUP`, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to SAP backend system	`HTTPS`	Technical Communication User	Search for SAP Notes
SAP Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide Communication with SAP BW*			Dashboard functionality for Process Management

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to managed systems (Read) `SM_<SID>CLNT<Client>`	`RFC`	`SM_<SID of Solution Manager>`	**Process Management** Read data of objects assigned to processes **Customizing Distribution** Read BC-Set activation log
SAP Solution Manager to managed systems (TMW) `SM_<SID>CLNT<Client>`	`RFC`	`SMTW_<SID of Solution Manager>`	*Custom Development Management Cockpit (CDMC)* for productive systems only. **⚠ Caution** You use the `TMW RFC` - connection for `CDMC` productive systems for analytics activities. For all other nonproductive systems, for example the quality acceptance systems (`QA` systems), development systems (`DEV` systems), or test and upgrade systems (sandbox / reference systems), use a TRUSTED `RFC` connection. See also the *Additional Functions* section in this chapter.
SAP Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	`RFC`	Named End user (customer specific)	Required for *CDMC*, *Customizing Synchronization*, *BC-Sets*, and *Content Activation*.
SAP Solution Manager to managed systems (Login) `SM_<SID>CLNT<Client>_LOGIN`	`RFC`	Named End user (customer specific)	Workaround to using Trusted RFC
Managed systems to SAP Solution Manager (Back) `SM_<SID>CLNT<Client>_BACK`	`RFC`	`SMB_<SID of Solution Manager>`	Help Center Function
SAP Solution Manager to managed systems within customer network	`FTP`		Update route permission table, content: `IP` addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		Graphics inclusion **⚠ Restriction** Manually created in transaction `SM59`

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Productivity Pak by RWD	SOAP over HTTPS	Communication User; RWD *InfoPak* integration user	External Integration on Document Management → Remember This technical user for the web service requires role SAP_RWD_INTERFACE.
Solution Manager to SAP Document Translation service	HTTPS	SAP BTP account user	KW Document
Solution Manager to SAP Machine Translation service	HTTPS	SAP BTP account user	Name of the solution documentation structure elements

4.3.1.4 Running Individual Background Jobs with a Specific Technical User

Most technical users are created automatically or manually during configuration. Technical users are of the type *System User*, if not stated otherwise. For more information on individual technical users, see the *Secure Configuration Guide* in the *Technical Users* section.

Background Jobs Technical User SOLMAN_BTC

The technical user SOLMAN_BTC schedules most of the background jobs relevant for *Solution Documentation (Process Management)*.

Example

You want to run job SMUD_DATTR_CALC* (*calculation of derived attributes* in scenario *Process Management*) with a separate technical user. This means you have to trace authorizations for the job, build a role, and then assign the new role to the new user. The following steps are relevant:

1. Preparation: Make sure you know the following:
   - The specific use case in your system. In this case, you want to trace the following application specific tasks:
     - Create a scenario
     - Create a process
     - Create a process step

    - Create an executable (for example a transaction)
    - Create/Assign a test document
  - The system that you want to trace in. In many cases, especially if the expected authorizations are system-specific or user specific, you have to run a trace in the productive system. However, we recommend running the trace in your test systems if possible. This use case requires you to run the trace in the production system due to the information that needs to be gathered.
  - Make sure that the user doing the tracing has the authorization to do so. During the tracing process, we recommend that you either assign the profile SAP_ALL (remember to unassign it afterwards) or use the SOLMAN_BTC user for this purpose. In this case, use technical user SOLMAN_BTC to run the job and collect all relevant authorizations.
  - Make sure that you also have a user with the authorization to run authorization traces in your system. This user should haveat least the authorization to run transaction STAUTHTRACE. In this case, the system administrator has all relevant authorizations to run this transaction.
2. Run the trace using transaction STAUTHTRACE.
    1. With your system administrator user, call transaction STAUTHTRACE.
    2. Choose *System-Wide Trace*.
    3. Mark all servers for which you want to trace. We recommend marking all of them.
    4. Activate the trace for your user (the user who will run the application). In this case, this user is SOLMAN_BTC.

    > → Tip
    >
    > Best practice is to assign the SAP_ALL profile to your user for the time of tracing. Don't forget to unassign this profile after tracing.

    .
    5. Run your app.
    6. Deactivate the trace.
    7. After deactivation, add the user for which you traced in the user field for *Restriction for the Evaluation*. In this case, the user is SOLMAN_BTC.
    8. In addition, select *Filter Duplicate Entries*.
    9. Choose the *Evaluate* button to get the trace results.
    10. In the *Object* column, all objects are mentioned that have to be added to a role. The columns *Field* and related *Field Values* show all traced values.

    > → Tip
    >
    > The more accurate you trace, the better and more correct values you receive. If you missed some authorizations, you can find log entries with red traffic lights in transaction SLG1. In this case, we check for object SMUD and subobject DATTR_CALC.
3. Create your new role in transaction PFCG.
    1. Go to transaction PFCG and create a role.
    2. Add the authorization objects from the trace to the role manually. In this case, use the following authorization objects:
        - S_RFC_ADM
        - S_ESH_ADM
        - SM_BPCA

- S_SMDDOC

3. Then, choose *Trace*.
4. In the pop-up, add the user for which you executed the trace in the filter for *All Applications*. In this case, user SOLMAN_BTC.
5. Choose *Evaluate*.
6. You receive the trace results for the objects. Choose *Transfer* to add the values from the trace per authorization object to your authorization object.

   > ⚠ Restriction
   >
   > For some fields, no values are added by the trace. You can either check the required value manually and add it, or you can add an asterisk (*). This indicates that all possible values are allowed.

   Do this for all objects and then save the role. This is your new role.

4. Assign the role to your separate technical user.

> ⚠ Caution
>
> Make sure, your new user is of type system user.

4.3.2 Scenario Integration

Implementation refers to the phase in your product lifecycle where you define and refine your business processes with the help of solutions, business processes, and related activities. According to the end-to-end business process lifecycle, this phase has to be integrated with a number of other tasks that emerge in your daily business, such as the handling of problems, and so on. The following sections describe how the implementation integrates with other scenarios in SAP Solution Manager and which user roles are applicable.

> → Tip
>
> For more information on each individual scenario, see the according *Application - Specific Guide*.

Business Process Change Analyzer (BPCA)

Users (for example the *Application Consultant*) can record TBOMs for the *Business Process Change Analysis* (BPCA). To do this, you have to assign the required BPCA single roles to your user: SAP_SM_BPCA_TBOM_ALL (generating TBOMs), and SAP_SM_BPCA_RES_ALL (analyzing results).

In the managed systems, you have 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 have to assign the according single roles of the required Use Case ID of *Incident Management*.

Issue Management

In *Process Management*, users can create *Issues* for your user. To do this, you have to assign the corresponding single role `SAP_ISSUE_MANAGEMENT_EXE` as well as the navigation role `SAP_SMWORK_SERVICE_DEV`, which is required for Use Case IDs of *Service Delivery*, *Issue Management*.

Job Management

You can also integrate *Job Scheduling*. If you assign Job-Scheduling-related objects, you have to assign user role `SAP_SM_SCHEDULER_EXE` to your users (see the application-specific guide for *Job Management*).

Test Management

You have to use the respective Test-Management-relevant roles in the user roles (see the scenario-specific guide for *Test Management*.

Change Request Management

You can use the *Change Request Management* function with *Process Management*. You also have to assign the user role `SAP_SOCM_REQUESTER` (see the scenario-specific guide for *Change Request Management*).

Scope and Effort Analyzer (SEA)

To use the function, you have to assign the according single roles of the required Use Case ID of *SEA*.

RFC Display

If you require your user to read or display RFCs from transaction `SM59`, you have to assign role `SAP_SM_RFC_DIS`.

Dashboard Integration

To allow data to be displayed in dashboards, you have to assign the appropriate display role for dashboards as well as BW authorizations in the respective BW client.

4.3.3 Users and Authorizations

4.3.3.1 User Roles in the SAP Solution Manager

This section provides an overview of the users as recommended by SAP and their respective Use Case ID assignments for *Process Management*.

Administrator/Project Manager SOLD_ADMXXX (Help Text ID: TP_SOLD_ADM)

Single Role	Help Text ID
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
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_DSH_DISP	AUTH_SAP_DSH_DISP
SAP_SM_SUTMAN_ADMIN	AUTH_SAP_SM_SUTMAN_ADMIN
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_DIS

> **Note**
>
> If you require display RFC Destinations, assign role SAP_SM_RFC_DISP.

Execution User/Application Consultant SOLD_EXEXXX (Help Text ID: TP_SOLD_EXE)

Single Role	Help Text ID
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

> **Note**
>
> If you require to display RFC Destinations, assign role SAP_SM_RFC_DISP.

Display User SOLD_DISXXX (Help Text ID: TP_SOLD_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_SMWORK_IMPL	AUTH_SAP_SMWORK_IMPL
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

Dashboard Configuration and Use

To use the dashboard function for Process Management, you require a user in the BW system. If your BW system is the same client as your SAP Solution Manager, you can assign the roleSAP_SM_BI_DSH_CONF for

configuration or SAP_SM_BI_DSH_DISP for display access to your end user. If your BW system/client is not the same as your SAP Solution Manager client/system, you need a user in the BW system who is assigned the above-mentioned roles as well as role SAP_SM_BW_S_RFCACL for trusted RFC communication.

Integration for Business Process Management (BPM) Objects UI

You can grant access to the BPM Object UI for Process Management by assigning the role SAP_SM_SL_EDIT_BPMN.

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

- Data Object
- Data Store
- Free Components
- Roles

The data is contained in database table AGSGBC*. It is 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 the role SAP_SM_SL_EDIT as this role serves as a maintenance role for several scenarios that would not allow the maintenance of global objects. Instead, the role SAP_SM_SL_EDIT_BPMN is to be used for maintaining global objects in the graphical display.

Logging

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

Custom Attribute Maintenance

In the *Interface Documentation* app, 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 provided in the SAP_SM_SL_ADMIN and SAP_SM_SL_EDIT roles.

4.3.3.2 User Descriptions and User Roles in Managed Systems

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

4.3.3.3 Authorization Objects

Solution Documentation SM_SDOC

This object is used to control the Process Documentation maintenance. The object contains the field SLAN, which is used to restrict a complete solution. In addition, branches of a solution can be restricted using the SBRA field. To allow only for a set of objects and attributes to be used within a certain solution and branches of that solution, you can use the SMUDAUTHGR field. With this field, you can 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. Only users who have the authorization for authorization object SM_SDOC with this authorization area name in the authorization area field SMUDAREA can perform activities for this structure element and its children. Authorization areas are defined on a solution-specific basis.
The Solution Documentation root element and all unassigned elements have the implicit authorization area assignment *Default* as standard. If the elements of a solution have not yet been assigned authorization areas, each element has the *Default* authorization area. 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 entire sub tree rooted by the element, excluding all nested sub trees rooted by elements with their own authorization area assignments. Non-structure elements always inherit the authorization area from their parent structures. The authorization area determination is branch-specific, because the inheritance hierarchy is branch-specific. If an element is moved, it may inherit a new authorization area from its new parent. In this case, the authorization area of an element may be different in different branches.

Concept of Authorization Group

Authorization Groups are defined based on the solution. When you assign an object or attribute type to a 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 who can see all objects, but can only maintain test cases. You then 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, the technical objects are invisible.

Combination with Authorization Object SM_GAL_GO

The SM_GAL_GO authorization object protects the following object types: Data Object, Data Store, Free Component, and Role. It is not relevant to control the access mode on a given diagram. The diagram opens in edit mode as soon as the user has sufficient authorization on SM_DOC with ACTVT 02 (change). You can differentiate between edit mode access to Solution Documentation and graphics diagram using ACTVT 68 (modeling) with authorization object SM_SDOC. This allows maintenance mode in Solution Documentation and display mode in the diagram graphics.

Solution Documentation Administration SM_SDOCADM

This object allows restrictions at the administrative level, that is administrative tasks at the process documentation level, the branches level, and logical components. As with SM_SDOC, solutions and branches can be restricted. In addition, the concept of aspect is used to further refine activities. By default, ACTVT 61 (Export) is not set to active because it is crucial to security. If you require this activity for your user, you have to adapt the authorization object in your user role accordingly.

Transport System S_CTS_ADMI

The authorization object is set to 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.

RFC Administration S_RFC_ADM

In the roles SAP_SM_SL_*, the authorization object S_RFC_ADM is included because executables from managed systems have to be read. If this authorization is not active, names of executables for managed systems can't be read and are therefore not displayed. The authorization is restricted to display for RFC connections only.

Document Management authorizations

Authorizations for Document Management in class SMD are set to inactive in roles SAP_SM_SL_*, as roles SAP_SM_KW_* contain these authorizations and others. If you do not require any further scenario integration with Process Management, you can set the authorizations in class SMD to active and remove role SAP_SM_KW_* from your user. If you do have a scenario integration, such as Process Management and Change Request Management, you require roles SAP_SM_KW_*. Make sure that authorizations do not overlap.

Test Plan Prompting SM_TPLN

When maintaining a branch in Process Management, the system prompts you to make changes to the corresponding test plans. To maintain the corresponding test plans, the authorization object SM_TPLN is required. The object is contained in role SAP_SM_SL_ADMIN with ACTVT 03. For full authorization for Test Management, see the according section in this guide.

System Data Container Prompting SM_SUTMAN

When updating solutions or logical components, a System Data Container (SDC) is created by the system in the background. To ease application use, SUT Management is updated simultaneously. This update requires authorizations for SUT Management, which are contained in role SAP_SM_SUTMAN_ADMIN which is optionally assigned to SOLD_ADM user.

Automatic Creation of ECAT System Containers S_DEVELOP

For the system to be able to automatically generate an ECAT container, authorization object S_DEVELOP with object types ECAT and ECSD is required. The object is contained in role SAP_SM_SL_ADMIN. If you do not require the automatic generation of system containers, you can remove the object from the role.

4.3.4 User Roles for Additional Functions

4.3.4.1 User Roles for Activation of Business Functions

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

Authorizations in SAP Solution Manager System

In addition to implementation roles, you have 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 have 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 the section in the *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_FUNCTIONS` to the users. This role contains authorizations to read access necessary function groups as test work bench. objects.

4.3.4.2 User Roles for Custom Development Management Cockpit (CDMC)

Configuration

See SAP Note 1244713

> **⚠ Restriction**
>
> The function of *CDMC* is not allowed in *S/4 HANA 2020* systems. see also the following SAP Notes:
>
> - 2250709 - Solution Manager 7.2: End-User Roles and Authorizations Corrections as of SP01 and higher
> - 2249880 - Dump SYSTEM_ABAP_ACCESS_DENIED caused through Blocklist Monitor in SAP S/4HANA on premise

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: http://help.sap.com *SAP Solution Manager*.

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

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

> **Caution**
>
> If you use a TRUSTED RFC destination, you have to assign to your user in the managed system user role SAP_CDMC_MASTER (with full authorization) or SAP_CDMC_STAT_SYSTEM (with restricted authorization).

Custom Development Management Cockpit

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 *Clearing Analysis*. 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.

> **Note**
>
> To be able to work with the result list, assign an additional role SAP_CDMC_CRITICAL_AUTH that 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.

4.3.4.3 User Roles for Customizing Comparison and Distribution

You have the option to use the *Customizing Distribution* function. To use this, you have to have implementation authorization as described earlier, as well as additional authorizations. For *Customizing Comparison* and

distribution, SAP delivers composite roles for administrator tasks and display users. These composite roles contain several single roles that are outlined underneath.

Template End User

New template users with Default ID: `CD_<user description>_<system ID>` added in the system.

The users are available in the *Solution Manager User Administration* (SMUA) app in work center *SAP Solution Manager Administration* view *Users*. For more information on SMUA, see in the *Secure Configuration Guide* the according section.

> → Tip
>
> If you search for users for Technical Administration in application *SMUA*, filter in column *Scenarios in which used* for the EMPTY entry. This entry filters all users for scenarios and functions, which are not represented in any of the configuration procedures in transaction `SOLMAN_SETUP`, and are therefore **only** available in `SMUA`.

Administrator User CD_ADM_XXX (Help Text ID: TP_CD_ADM)

The roles of this user should be assigned *in addition* to one of the following implementation template users:

- `SOLD_ADMXXX`
- `SOLD_EXEXXX`

Single Role	Help Text ID
`SAP_SCOUT_ALL`	`AUTH_SAP_SCOUT_ALL`
`SAP_SCDT_ALL`	`AUTH_SAP_SCDT_ALL`
`SAP_SCIDM_ALL`	`AUTH_SAP_SCIDM_ALL`

Display User CD_DIS_XXX (Help Text ID: TP_CD_DIS)

The roles of this user should be assigned *in addition* to the implementation template user `SOLD_DISXXX`.

Single Role	Help Text ID
`SAP_SCOUT_DIS`	`AUTH_SAP_SCOUT_DIS`
`SAP_SCDT_DIS`	`AUTH_SAP_SCDT_DIS`

Single Role	Help Text ID
SAP_SCIDM_DIS	AUTH_SAP_SCIDM_DIS

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

4.3.4.4 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

Single Role	Remarks
SAP_BCS_ACTIV	Activate BC Sets See SAP Note 505603.
SAP_BCS_CREAT	Create BC Sets
SAP_BCS_ADMIN	Administration of BC Sets

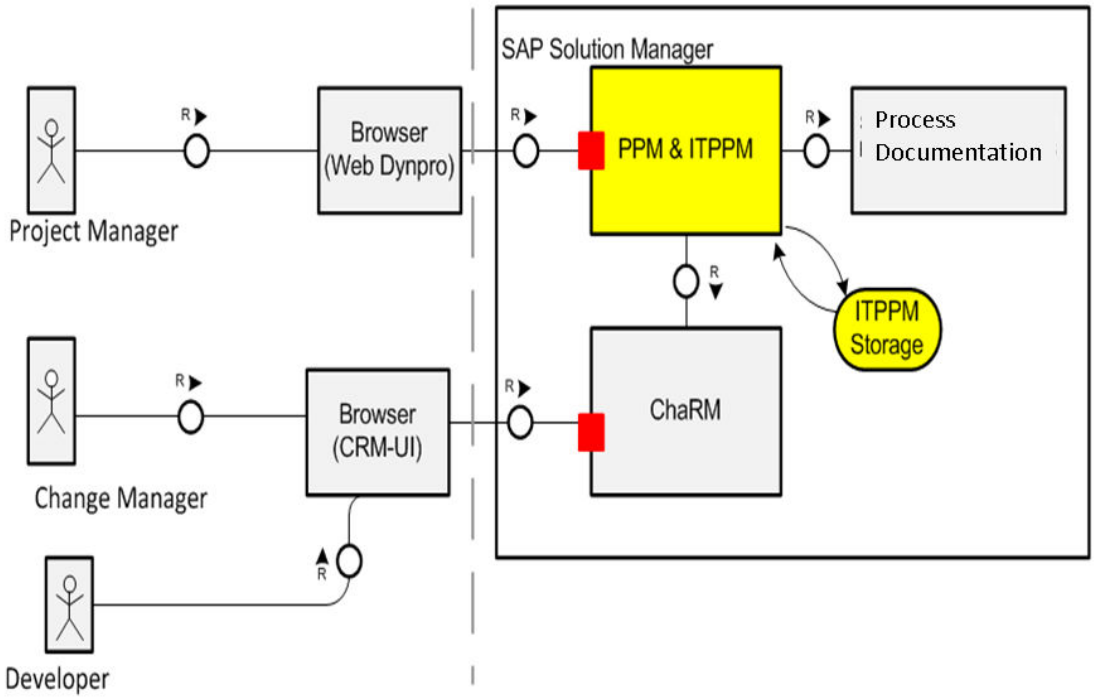
> **Note**
>
> Roles for BC Sets include authorization object S_TABU_DIS with ACTVT 03 for display of all table groups. If you require to restrict which table should be accessible, you have to trace your application and add these authorizations manually or build a new role for your purpose.

4.3.4.5 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 that 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.



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 all single roles listed for user SMC_PPM in SOLMAN_SETUP (see table below).

Single Role	Help Text ID
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN

Single Role	Help Text ID
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_DISP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

End Users

End users can be created as template users within the guided procedure for the scenario in transaction SOLMAN_SETUP.

Project Manager User (Help TXT ID: TP_ITPPM_AM)

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
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_CM_SMAN_CHANGE_MANAGER	AUTH_SAP_CM_SMAN_CM
SAP_ITCALENDAR_DIS	AUTH_SAP_ITCALENDAR_DIS
SAP_RM_ITREQ_MANAGER	AUTH_SAP_RM_ITREQ_MANAGER

Single Role	Help Text ID
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
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	SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	SAP_SM_CRM_UIU_SOLMAN
SAP_SM_CRM_UIU_SOLMANPRO_RM	SAP_SM_CRM_UIU_SOLMAN
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SOCM_CHANGE_MANAGER	AUTH_SAP_SOCM_CM

Project Team Member (Help TXT ID: TP_ITPPM_TM)

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
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

NWBC

> **Note**
>
> ITPPM requires transaction NWBC as a user interface in addition to the SAP Fiori launchpad and tiles. The transaction is included in role SAP_SM_FIORI_LP_EMBEDDED.

Dashboard Configuration and Use

To use the dashboard function for Project Management, you require a user in the BW system. In case your BW system is the same client as your SAP Solution Manager, you can assign the role SAP_SM_BI_DSH_CONF for configuration or SAP_SM_BI_DSH_DISP for display access to your end-user. If your BW system/client is not the same as your SAP Solution Manager client/system, you require a user in the BW system who is assigned the above-mentioned roles as well as role SAP_SM_BW_S_RFCACL for trusted RFC communication.

Transaction Types

The transaction type for `ITPPM` is `SMCP`.

Authorization Group for S_TABU_DIS

The authorization group for all integration-relevant tables for `ITPPM` is `SMCP`. The authorization object is checked when the integration is ON, which can be checked in table `SMCP_CUST_TABLOG`.

Integration with Change Request Management: Change Manager

If you use PPM with Change Request Management, you have 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 the scenario-specific guide for *Change Request Management.*

Integration with Change Request Management and Requirement Management: Developer User

If you use PPM with Change Request Management and Requirement Management, you have 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 the scenario-specific guide for *Change Request Management* or *Requirement Management*.

Integration with Requirement Management: Requirement Manager

If you use PPM with Requirement Management, you have 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 the scenario-specific guide for *Requirement Management*.

Issue Management

If you use `ITPPM` with *Issue Management*, you have to additionally assign the composite role for the *Issue Management* user: `SAP_ISSUE_MANAGEMENT_*_COMP`. For more information on Issue Management, see the 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).

4.3.4.6 Authorizations for Interface Documentation

The *Interface Documentation* app includes the authorizations to view and maintain processes in Process Management (Solution Documentation). The *Interface Documentation* app, although closely linked to Solution Documentation, is a standalone app with separate data persistency. It acts as external app to Solution Documentation and can be called from there as an element of an interface object in the Interface Library.

User Roles

In general, all roles relevant for Process Management are required for Interface Documentation. To maintain customer-specific content, you require authorization to run transaction `AGS_DCM_CUST_IFDOCU`. The authorization is included in roles `SAP_SM_SL_*`

.

Value Help for Managed System Values

To make full use of the value helps that are available for most attributes, you require destination TMW or at least READ.

Integration SAP PI / PO Enterprise Service Repository (ESR)

If you want to import interface data from an *SAP PI / PO Enterprise Service Repository (ESR)* via transaction `AGS_DCM_EXT_IMPORT`, you have to provide an additional HTTP(s) destination to the relevant PI / PO system in transaction `SM59`. This destination must have the naming convention `SOL_DIR_ESR_<SID>` with `<SID>` as the extended system ID of the PI / PO system as maintained in SAP Solution Manager's LMDB. Provide the Target Host and the Service Number of the system, and enter /rep in the Path Prefix field of the destination. Finally, enter basic authentication data (user and password). The technical user for this destination must have at least role `SAP_XI_DISPLAY_USER_J2EE` to be authorized to call the ESR.

4.3.5 External Integration

4.3.5.1 Introduction

You can integrate external products with SAP Solution Manager. The term *External Product* refers to either third-party products or SAP products, which can be used to complement a function in SAP Solution Manager.

4.3.5.2 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 SAP Solution Manager project.

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

4.3.5.3 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.

4.3.5.4 SAP Productivity Pak App by ANCILE

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

4.3.5.5 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 SAP 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 SAP Support Portal: *SAP Components* > *SAP Solution Manager* > *Additional Guides*.

4.4 Scenario-Specific Guide: Business Process Change Analyzer

4.4.1 Introduction

The business process lifecycle stretches across 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. The Business Process Change Analyzer supports this implementation and upgrade process in various use cases, for instance:

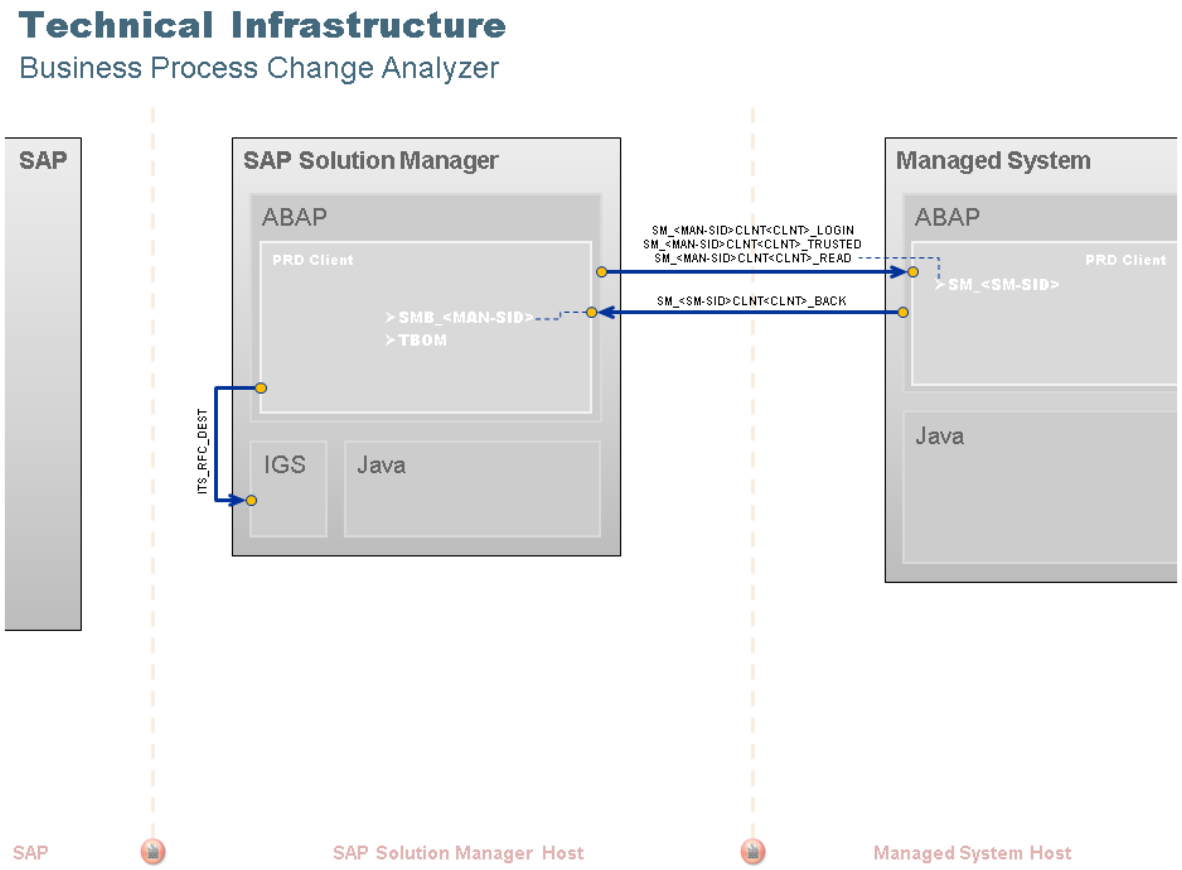
- Dynamic TBOM (Technical Bill of Material) Recording
- TBOM Creation via 3rd party Test Tool /Test Cases
- Web Services for External Test Tool integration

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

4.4.2 Prerequisites

4.4.2.1 Technical System Landscape

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



Infrastructure

4.4.2.2 Scenario Configuration User

You configure the *BPCA* scenario in SAP Solution Manager Configuration (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, you have to assign the following single roles:

Single Role	Help Text ID
SAP_BPCA_CONFIG	AUTH_SAP_BPCA_CONFIG

Single Role	Help Text ID
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_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SM_BPCA_PTM_INT	AUTH_SAP_SM_BPCA_PTM_INT
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN

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

> **Note**
>
> To create users and assign user roles in a managed system, you also have to assign role SAP_SM_S_RFCACL.
>
> Remove this role after configuration from the SMC user.

> **Caution**
>
> SAP role SAP_BCPA_CONFIG contains the following critical authorization objects:

- S_ICF_ADM
- S_C_FUNC
- S_RFC
- S_DEVELOP
- PLOG: Make sure that you maintain the authorization on organization unit level according to your requirements. If not required, we recommend that you deactivate the authorization object.

Due to the high number of critical authorization objects in this role, we highly recommend that you deactivate the role after successful updates of the SOLMAN_SETUP procedure.

Scenario Configuration

To configure the *Business Process Change Analyzer* and its *Third-Party Integration*, you have to configure it in SAP Solution Manager (transaction SOLMAN_SETUP). During the specific guided configuration, you can create *Standard Template Users*. The system automatically adds all relevant user roles (see the corresponding sections about *Users and User Roles*).

4.4.2.3 Communication Channels and Technical Users

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

> **Note**
>
> All mentioned RFC destinations are automatically created via transaction SOLMAN_SETUP (view: managed systems). For more information, see the *Secure Configuration Guide*.

> **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 roles and authorizations recommended by SAP.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to SAP Backend system	HTTPS	Technical Communication User	Search for SAP Notes

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			
MDX Parser			Used for the creation of semi-dynamic `TBOM`s
Solution Manager to managed systems (Read) `SM_<SID>CLNT<Client>`	`RFC`	`SM_<SID of Solution Manager>`	To read data such as business functions, transport requests, Support Packages, repository objects, and so on from the managed systems for `BPCA` analysis
Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	`RFC`	Named End-user (customer specific)	Recording TBOMs in managed systems **→ Tip** Alternatively, the Login RFC can be used.
Solution Manager to managed systems (Login) `SM_<SID>CLNT<Client>_LOGIN`	`RFC`	Named End-user (customer specific)	Optional as Login `RFC` - Connection can also be used. Needed for `TBOM` recording of automatic test cases (traces)
Managed systems to Solution Manager (Back) `SM_<SID>CLNT<Client>_BACK`	`RFC`	`SMB_<SID of Solution Manager>`	For recording of automated test cases to receive trace information about which functions in which managed systems were analyzed
Solution Manager to managed systems within customer network	`FTP`		Update route permission table, content: `IP` addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		Graphics inclusion **▲ Restriction** Manually created in transaction `SM59`

4.4.2.4 Technical User for ECatt

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

Users in Managed System

User Name	User ID
Test Automation Framework Technical User	ECATT_ET_USR

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 with 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 to create TBOMs via a trusted RFC connection.

User in SAP Solution Manager System

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

4.4.3 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 have to add the changed values in the according CRM - authorization objects for the scenario.

- For CRM authorizations, see the *Authorization Concept Guide*
- For maintenance of authorization objects, see the *How-to Guide on how to maintain authorization objects*

Transaction Types

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>.

4.4.4 Scenario Integration

BPCA refers to the phase in your product lifecycle 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 lifecycle, this phase needs to integrate with a number of other tasks that occur in your daily business, such as handling problems. 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 corresponding scenario-specific guide.

Test Management: Create Test Plans

BPCA is used to prepare the test phase. You can create test plans. To create test plans, also assign 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 directly jump to the CRM WebUI. In addition to the basic BPCA role, you require the following single roles:

- 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 the scenario-specific guide for *Change Request Management*.

4.4.5 Users and Authorizations

4.4.5.1 Users and User Roles

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

Authorization for Trusted RFC Between SAP Solution Manager and BW System

When using 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 the corresponding application authorization in the managed system and role SAP_SM_BPCA_TBOM for recording activities.

For Business Process Change Analyzer, you have 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 have 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)

Single Roles	Help Text ID
SAP_SM_BPCA_TBOM_ALL	AUTH_SAP_SM_BPCA_TBOM_ALL
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

Single Roles	Help Text ID
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_SMWORK_IMPL	SAP_SMWORK_IMPL
SAP_BPCA_CRM_INTEGRATION	AUTH_SAP_BPCA_CRM_INTEGRATION
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

If you use a remote BW scenario, these roles must be assigned to the user with the same user ID and password in the BW system.

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)

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_EXE	AUTH_SAP_SM_KW_EXE
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

If you use a remote BW scenario, these roles must be assigned to the user with the same user ID and password in the BW system.

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)

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_ECAT)

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

Single Roles	Help Text ID
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.

Authorization Object SM_BPCA

The main authorization for BPCA is `SM_BPCA`. It is also required in role for scenario CDMC (for example `SAP_SM_CDMC_INT`).

4.4.6 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 app does not ensure that access to this file is only allowed with the correct authorization. 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 you 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.

4.5 Scenario-Specific Guide: Test Suite

4.5.1 Prerequisites

4.5.1.1 Technical System Landscape

The following graphic provides an overview over the basic technical system landscape that is needed to run the complete *Test Management* scenario. SAP Solution Manager is connected to your managed systems via READ - RFC . Optionally, you can connect a third-party product to the SAP Solution Manager via specified connections. For more information on all connections, when they are used, and which technical users are required, see the following sections.

4.5.1.2 Scenario Configuration User SMC_TM_XXX

> ⓘ Note
>
> For information about the following concepts, see the corresponding sections in this guide:
>
> - Configuration users in SAP Solution Manager: chapter *Configuration Users*
> - BW integration concept: chapter on BW integration

Creating Configuration Users for Running Configuration in SAP Solution Manager Configuration

You have the following options for creating the configuration user in SAP Solution Manager Configuration (transaction SOLMAN_SETUP):

- Use default user SMC_TM_XXX:
  When you configure your scenario using the appropriate configuration procedure in SAP Solution Manager Configuration (transaction SOLMAN_SETUP), the system asks you to create a specific configuration user with a default user name. You can use user SMC_TM_XXX to configure the following *Test Suite* procedures: *Test Suite Preparation* and *Test Automation Preparation*.
  - *Test Management*: SMC_TM_<systemID> (help text ID: USER_CONFIG_TM)

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_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_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_APPLOG	AUTH_SAP_SETUP_BASIC
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONF

> **Note**
>
> To activate BW content, you need the role SAP_SM_BI_ADMIN in the BW system/client.

- Use the user SOLMAN_ADMIN and add additional user roles. Enter the user ID for user SOLMAN_ADMIN in the popup and assign the roles.
- Do not use the default user, create your own configuration user in transaction SU01: Set the flag for *Manual Maintenance* in the popup in SAP Solution Manager Configuration, and create your user in transaction SU01.

→ Recommendation

If you want to create the configuration users manually, we recommend that you assign them the following roles:

- All roles referenced by use case ID `SMC_TM_***`
- All roles referenced by use case ID `SMC_CBTA_***`

> ⓘ Note
>
> To perform the following tasks, you need have to assign additional roles:
>
> - To create users and assign user roles, assign role `SAP_SM_USER_ADMIN`.
> - Use a trusted RFC connection between SAP Solution Manager and the managed systems, you need to assign role `SAP_SM_S_RFCACL` in the SAP Solution Manager system and in the managed system.

Additional Customizing Authorizations

To allow all customizing transactions for this user, you need to add manually values `SMT_CUST*` which includes transaction codes `SMT_CUST_0` to `SMT_CUST_15`, `SMT_SET_KW_DOC_CATEG`, and `SMT_SET_OTPK_REST_DF` in authorization object `S_TCODE` to role `SAP_TM_CONFIG`.

4.5.1.3 Communication Channels and Technical Users

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

> ⓘ Note
>
> All mentioned RFC destinations are automatically created in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`) under *Managed Systems*. For information, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to SAP backend system	HTTPS	Technical communication user	Search for SAP Notes

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to/ from SAP BW system/client **Note** See the Secure Configuration Guide section *Communication with SAP BW*			Dashboard usage
SAP Solution Manager to managed systems (Read) `SM_<SID>CLNT<Client>`	RFC	`SM_<SID of SAP Solution Manager>`	To read data from the managed system in *Test Management* and *CBTA*
SAP Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	RFC	Named end-user (customer-specific)	Required for CBTA. For more information, see section *User Roles for CBTA (Component-Based Test Automation)* in this guide.
SAPSolution Manager to managed systems (Login) `SM_<SID>CLNT<Client>_LOGIN`	RFC	Named end-user (customer-specific)	**CBTA** Workaround to using trusted RFC. Integration with BPCA
Managed systems to SAP Solution Manager (Back) `SM_<SID>CLNT<Client>_BACK`	RFC	`SMB_<SID of Solution Manager>`	Required for CBTA. For more information, see section *User Roles for CBTA (Component-Based Test Automation)* in this guide.
SAP Solution Manager to managed systems (SUT) `TST_<SUTSID>_CLNT<Client>`	RFC	`TST_SUT_<SolutionManager SID>` in the managed system	Required for CBTA. For more information, see section *User Roles for CBTA (Component-Based Test Automation)* in this guide.
SAP Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		Graphics inclusion **Restriction** Manually created in transaction `SM59`
Solution Manager to/from Quality Center by HP	SOAP over HTTP(S)	Communication User	Test requirements (send and receive data)
Third Party Test Tools	SOAP over HTTP(S)		Depends on the individual application

4.5.2 Scenario Integration

Test Management refers to the phase in your product lifecycle where you test and validate your business processes through projects. Following the end-to-end business process lifecycle, this phase has to be integrated with a number of other functions that come into play in your daily business, such as problem handling, 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.

> ⓘ Note
>
> For more information about each individual scenario, see the corresponding *Scenario-Specific Guide*.

Business Process Change Analyzer (BPCA)

In SAP Solution Manager process documentation, users (for example, the Basis Development Consultant) can record TBOMs for the Business Process Change Analysis. To do this, you have to assign the required BPCA role to your user: `SAP_SM_BPCA_TBOM_ALL` (creating TBOMs), and `SAP_SM_BPCA_RES_ALL` (analyzing results).

In the managed systems, you have to assign the appropriate app-specific authorizations to your user.

Process Management

In the *Process Documentation* app, users can add test cases. To do this, you have to assign user roles for Process Management. For more information, see the relevant section.

Change Request Management

Process documentation can be integrated with Change Request Management. In this case, test cases are assigned to testers in Change Request Management. To perform and document test, you must assign test suite roles to the appropriate users.

CBTA

CBTA is tightly integrated with Test Suite and also refers to test suite. For more information, see the section about CBTA and check the template users for CBTA in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`).

4.5.3 Users and Authorizations

4.5.3.1 Users and User Roles

This section provides an overview of users recommended by SAP and their corresponding user role assignments for *Test Suite*. All users are assigned a composite role that contains a number of single roles.

Authorization for Trusted RFCs Between SAP Solution Manager, Managed Systems, and BW System

Trusted authorizations are required between SAP Solution Manager and its managed systems, and between SAP Solution Manager and a remote BW system.

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

Both roles are not included in the respective composite roles due to their high security relevance.

Application-Specific Authorizations in Managed Systems

For Test Suite, you have to assign authorizations in the managed system depending on the application you are using in the managed system. In addition, if you are using the trusted RFC connection, you have to assign the authorization object S_RFCACL to your user. This authorization object is not included in the SAP_ALL profile.

Users in the SAP Solution Manager System

Tester (help text ID: TP_TM_TM)

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

Single Role	Help Text ID
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_STWB_2_DIS	AUTH_SAP_STWB_2_DIS
SAP_SUPPDESK_CREATE	AUTH_SAP_SUPPDESK_CREATE
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

Project Manager/Test Organizer (Help Text ID: TP_TM_PM)

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
SAP_SM_DSH_CONF	AUTH_SAP_SM_DSH_CONF

> **Note**
>
> - If you want to use the *Test Suite Dashboard*, you also have to assign the single role SAP_SM_DASHBOARDS_DISP_TWB.

If you use the remote BW scenario, these roles have to be assigned to the user with the same user ID in the BW system.

Single Roles	Help Text ID
SAP_BI_E2E_SMT	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DIS

Basis Development Consultant (Help Text ID: TP_TM_BC)

Single Role	Help Text ID
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_SM_GEN_TRANSPORT	AUTH_SAP_SM_CBTA_TRANSPORT
SAP_STWB_INFO_ALL	AUTH_SAP_STWB_INFO_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_RMMAIN_EXE	AUTH_SAP_RMMAIN_EXE
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

If you use the remote BW scenario, these roles have to be assigned to the user with the same user ID in the BW system.

Single Roles	Help Text ID
SAP_BI_E2E_SMT	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DIS

Display User (Help Text ID: TP_TM_RO)

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_DIS	AUTH_SAP_SM_KW_DIS
SAP_STWB_INFO_DIS	AUTH_SAP_STWB_INFO_DIS

Single Role	Help Text ID
SAP_STWB_2_DIS	AUTH_SAP_STWB_2_DIS
SAP_STCE_DIS	AUTH_SAP_STCE_DIS
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

> **Note**
>
> If you want to use the Test Suite Dashboard, you also have to assign the single role SAP_SM_DASHBOARDS_DISP_TWB.

If you use the remote BW scenario, these roles have to be assigned to the user with the same user ID and password in the BW system.

Single Roles	Help Text ID
SAP_BI_E2E_SMT	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DIS

Authorization Objects

SM_TPCK and SM_TPLN

Use these authorization objects to access and manage test packages and test plans in SAP Solution Manager. They are included in the role SAP_STWB_2_*.

Authorization Groups for Tables (S_TABU_DIS)

Test Suite uses authorization group TSTM to protect tables. The group is added to the authorization object S_TABU_DIS in the corresponding roles.

SM_WC_VIEW

The work center was redesigned in Release 7.2, although you can still open the old work center using transaction STWB_OLD. You can restrict the views for both work centers in the authorization field help. Assign only entries with the suffix OLD to the old work center views.

C_SIGN

This object is maintained in roles SAP_STWB_2_* specifically for the purpose of digital signatures on test plans.

4.5.4 Additional User Roles

4.5.4.1 User Roles for Test Suite Workflow

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

User Roles

The user role for the Test Suite workflow has to be assigned to the user in addition to the respective single roles.

Test Suite Workflow

User role	Restriction on
`SAP_STWB_WORKFLOW_ADMIN`	Full authorization
`SAP_STWB_WORKFLOW_DIS`	Display authorization

CRM Standard Customizing

> **⚠ Restriction**
>
> This section applies only to incident-related workflows. For workflows related to test plan or test automation execution, SMARTFORMS are used.

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 provides an overview of the transaction types used.

> **⚠ Caution**
>
> If you copy SAP standard customizing, you have to add the changed values in the corresponding CRM authorization objects for the scenario. See also the how-to guide for maintaining authorization objects.

Transaction Types

Authorization Objects

The most important CRM authorization objects are contained in the corresponding roles. For more information, see the *Authorization Concept Guide*, section about CRM integration.

4.5.4.2 User Roles for Extended Capabilities

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

User Roles

Role	Restriction on
SAP_STWB_WITC_CREATE	Authorization for creating or maintaining work items
SAP_STWB_WITC_EXE	Authorization to maintain work items as the person responsible, but not to create new work items
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 and action profiles. SAP delivers a standard CRM customizing, which is also maintained in the individual CRM authorization objects for workflow. The following table provides an overview of the transaction types used.

> ⚠ Caution
>
> If you copy SAP standard customizing, you have to add the changed values in the corresponding CRM authorization objects for the scenario. See also the *How-to Guide* for maintaining authorization objects.

Transaction Types

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 more information, see the *Authorization Concept Guide*, section about CRM integration.

4.5.4.3 User Roles for CBTA (Component-Based Test Automation)

Component-Based Test Automation is an optional SAP software component that can be installed on SAP Solution Manager. Use it to create, deploy, and maintain, 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,, and Web Dynpro ABAP.
- SAP SUT based on 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 third-party servers running Web technology, and so on.

You use CBTA use cases in one of the following ways:

- Without TBOM creation (BPCA integration)
- With TBOM creation

Configuration

Configuration Procedure

You can configure CBTA in transaction SOLMAN_SETUP.

> **Note**
>
> The system to be tested must not be a productive system.

Configuration User

The configuration can be performed using the user SMC_CBTA_>SID>, which you can create when calling the CBTA configuration procedure in transaction SOLMAN_SETUP.

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

Single Role	Help Text ID.
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
>
> The 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 SMT_DV_ECCUST_ET, which is used to register the CBTA tool. For information on how to maintain a specific authorization group for the table, see SAP Note 1976897.

Temporary File Storage

During CBTA processing, the following files are stored on the local machine:

- The system records the test scripts as temporary files. These files are stored on the user's machine for the CBTA.

  > ⓘ Note
  >
  > You can delete the temporary files as needed using the CBTA configuration. Choose the appropriate option on the *Others* tab.

- When CBTA is installed on a machine, the system stores C-base files locally.

RFC Connections and Users Used

> ⓘ Note
>
> For detailed information, see SAP Note 1763697.

In general, the scenario uses the RFCs as defined in SOLMAN_SETUP. For more information, see transaction SOLMAN_SETUP.

To enable automated testing, information has to be persisted in SAP Solution Manager so that the CBTA app can communicate with the SUT. To do this, you can set the following parameters in the SUTManagement app:

1. The System Under Test to be tested.
   - The SUT that is based on ABAP technology: RFC destination (with technical user)
     .

- The SUT that is not based on ABAP technology: URL is to be provided to identify the SUT.

2. User ID for the scenario execution
   - The SUT that is based on ABAP technology: The provision is mandatory.
   - SUT that is not based on ABAP technology: The provision is optional.

   User credentials are persisted in the *Secure Password Storage*.

Regardless of which scenario you use, the following RFC connections exist between your SAP Solution Manager system (TCE) and your managed system (SUT):

- 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

Create/Maintain Test Profiles (Design Time) User: Test Coordinator/Administrator

1. Select the system data container (SDC) to be used
2. Import the selected SDC definition into the SUT Management app.
   This creates an enhanceable structure *SDC – Target Systems – Branches - System Roles*.
3. Define SDC enhancements in SUT Management for each available system role.

Usage of Test Profiles in Test Scripts (Runtime)

1. Create tests in test composition environment (TCE).
   - Select the underlying SDC and the target system.
   - Select the appropriate test profile.
   - Run the recording wizard.
     (The recording wizard records the business scenario processed on the SUT and automatically creates the test script components from the recorded scenario. It persists in the test repository.)
2. Execute previously created tests from the TCE.
3. Maintain previously created tests from the TCE.

> **Note**
>
> Both recording and execution scenarios require opening sessions on the SUT. This session opening retrieves data from tables of the SUT Management app. Authorization is required to access this data at runtime .

Technical System User on the Managed System: TST_<SolutionManagerSID>

Technical User Roles

To work with CBTA, you must have a TST_<SolutionManagerSID> system user in place for the corresponding RFC TST_<SUTSID>_CLNT<Client>. This user requires the following roles:

Technical User Roles

Role	Help Text ID
SAP_TST_AGENT_RFC	AUTH_SAP_TST_AGENT_RFC
SAP_CRM_TST_RFC (optional) **Note** If your managed system is a CRM-based system, you have to add role SAP_CRM_TST_RFC. Download this role from your SAP Solution Manager system to your PC, and then upload it to your CRM system. You have to maintain the authorization objects, generate the profile, and run the user comparison.	AUTH_SAP_CRM_TST_RFC
SAP_WDA_TST_RFC **Note** Use if your managed system is a WD-ABAP-based system.	AUTH_SAP_WDA_TST_RFC
SAP_SM_TCE_RFC	AUTH_SAP_SM_TCE_RFC

Specific Authorizations for Role SAP_TST_AGENT_RFC

Additional security measures are enforced when the technical user accesses content-related data. Therefore, the following authorization objects are also checked:

- /SDF/E2E with ACTVT 03 (display)
- S_ADMI_FCD with ACTVT 03 (display) for field value ST0R

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

In the case of BPCA integration, the trusted authorization object S_RFCACL (role SAP_SM_S_RFCACL; help text ID: AUTH_SAP_S_SM_RFCACL) is assigned to the end user in the SAP Solution Manager system and in the managed system.

Test Engineer: CBA_TE_>SID> (Help Text ID: TP_CBTA_TE)

User Roles in the SAP Solution Manager System

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_GEN_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: CBA_TC_<SID> (Help Text ID: TP_CBTA_TC)

User Roles in the SAP Solution Manager System

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_GEN_TRANSPORT	AUTH_SAP_SM_CBTA_TRANSPORT
SAP_STCE_ALL	AUTH_SAP_STCE_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Read Only User: CBA_DIS_<SID> (Help Text ID: TP_CBTA_DIS)

User Roles in the SAP Solution Manager System

Role	Help Text ID
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST

Role	Help Text ID
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)

Role	Help Text ID
Business Relevant Application Role	

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 Manager.

The RTL Manager is a client-side tool for customizing the VBScript 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 SAP/PUBLIC/CBTA folder in transaction SE80 (MIME Repository) contains the official runtime library (CBASE.zip) provided by SAP. Additional files are stored in this location when the customization is transferred.

The RTL Manager provides the ability to write additional custom functions that the test scripts may need to automate the testing of certain business scenarios where the common approach (based on default components) is not sufficient. When running a CBTA test script, the VBScript code corresponding to the test is sent from the SAP Solution Manager MIME Repository to the client computer and executed using the VBScript interpreter. The Runtime Library is a set of VBScripts that provide helper classes, functions and procedures that are necessary to simulate actions that are normally performed by a regular user. Default Components are components that perform atomic operations on user interface elements. The Runtime Library (RTL) is delivered with default components for all the user interface technologies supported by CBTA. Using the RTL Manager, developers can perform the following tasks:

- Developers can check out the Runtime Library to their local file system to modify it. They can add custom code to the specified locations.
- When developers have completed the custom code, they can save the modifications back to the SAP Solution Manager MIME Repository. This makes the libraries available to other testers.
- By transporting the changes, the libraries can also be updated on other SAP Solution Manager systems in the landscape.

BPCA TBOM Integration

If you integrate CBTA with BPCA based on TBOMs, assign the user roles for BPCA (SAP_SM_BPCA_TBOM and SAP_SM_SL_DISPLAY) to your users. For more information, see the security guide for *Business Process Change Analyzer* in this document, chapter *User Description and User Roles*.

Critical Authorization Objects

S_TABU_NAM

The authorization object S_TABU_NAM allows the display of the table RFC_READ_TABLE (in the configuration role for the 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. Activities are checked for SUT management definitions for the explicitly listed system data containers and system IDs:

- Perform: Use SUT Management test profiles and the defined user credentials in test cases.
- Maintain: Create, modify, and delete definitions in SUT Management
- Check: Verify definitions in SUT Management (credentials, technical destination)
- Import: Enables all SDC import activities in SUT Management.

The activities have no dependencies and can be granted independently.

The Test Profile field has no value help. To find out the values for this field, proceed as follows: On the SAP Solution Manager launchpad, choose *Administration - Test Suite* > *Test Automation Framework* > *System Under Test Management*.

SM_SUT_LCN

In addition to authorization object SM_SUTMNGT, the authorization object SM_SUT_LCN is used as a fallback. The fallback is called in case there is no authorization assignment of authorization object SM_SUTMGNT in place. The authorization fields of the two objects are different.

Scenario Integration

SUT Management is integrated with the CBTA capability of SAP Solution Manager, and CBTA is integrated with Test Suite as an external tool. It can be accessed as follows:

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

> **Note**
>
> CBTA is also closely related to scenario BPCA in terms of TBOM. For more information, see the scenario-specific guide for BPCA.

Additional Security Related Information

SSL Communication Security

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

4.5.5 Partner Integration

4.5.5.1 Tool with BC — ECATT- Integration

You can integrate an external test tool with eCatt.

Role for eCatt - Integration

Role	Remarks
SAP_ECET	Authorization for saving and loading of test scripts with eCatt. This role is automatically assigned during technical user generation.

4.5.5.2 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.

Data Flow

In Process and Project Management

1. Solution is created by a user.
2. Solution Documentation is updated via a Branch.

In Test Suite/Partner Test Management

1. Associations are created for the Production branch in SAP Solution Manager to Production project HP ALM
2. Associations are created for the Development branch in SAP Solution Manager to Development project in HP ALM.

3. Solution Documentation is pushed from the Development branch in the SAP Solution Manager to the Development project in HP ALM. Elements of type Documentation and executables are transferred.

In HP ALM

1. Test Cases are created in the Test Plan for the new requirements in HP ALM by the Test Engineer.
2. Test Sets are created and testing is executed in HP ALM by the Test Co-ordinator.
3. Test Status is updated for the Test Cases in the Test Set, and Defects are created in HP ALM. SAP - related defects are marked in HP ALM by the Tester.
4. Test Results are pushed to the SAP Solution Manager by the Tester.
5. SAP - related Defects are pushed to the SAP Solution Manager, and corresponding Incident are created in Incident Management by the Tester.

In Test Suite/Partner Test Management

1. The user launches the Partner Test Management Application in SAP Solution Manager, selects the relevant association, and launches the Test Results User Interface. This is done by the Project Manager or Business Process Experts.

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 the single roles mentioned in the table below manually.

> ⚠ 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.

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

Single Role	Help Text ID
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
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP

> **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)

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_ADMIN	AUTH_SAP_TMT_ADMIN
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS

Maintenance User (Help TXT ID: TP_PTM_EXE)

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

Single Role	Help Text ID
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)

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

Roles	Help Text ID
SAP_SUPPDESK_INTERFACE	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

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.

4.5.5.3 Third Party Test Management Integration

You can integrate Test Suite with a third party test tool.

SM-TSTR partners are integrated to Solution Manager through the SM-TSTR/BC-eCATT certified interface.

For this integration, two communication channels are available:

- *Test package synchronization*: communication is initiated from the SAP Solution Manager to the Third Party tool.
  Third party tests creation, maintenance, and execution are initiated from the Test Suite and orchestrated by the ECATT engine.
- *Result integration*: communication is initiated from the Third Party tool to SAP Solution Manager.
  Mass execution of Test Packages is enabled within Third-Party tools. The execution process is fully delegated to and triggered from the Third-Party tools. The Test Suite test packages are outsourced, and their execution is fully externalized, delegated to the Third Party.

  > ⓘ Note
  >
  > The Third-Party must rely on a secure storage for critical data such as credentials.

Test Package Synchronization

Precondition:

- The eCatt configuration is executed.
- To use the integration synchronization, you need to assign two roles to the technical user ECATT_ET_USER

  > → Tip
  >
  > You can rename the user to your own convenience.

  :

  - SAP_ECET
  - SAP_SM_TSTR_THIRD_PARTY_INT
    This role substitutes role SAP_SM_ECET, which is obsolete as of SP14.

Result Integration

Precondition:

- You have executed the relevant step for creating the technical user `SM_TSTR_INT` in transaction `SOLMAN_SETUP` for the Test Suite.

  > ⓘ Note
  >
  > For security reasons, the specific technical user is used. You can rename the user to your own convenience.

  The system assigns two roles to the technical user:
  - `SAP_ECET`
  - `SAP_SM_TSTR_THIRD_PARTY_INT`
    This role substitutes role `SAP_SM_ECET`, which is obsolete as of SP14.

Log

In SAP Solution Manager, the application log as described for Test Suite is relevant.

4.5.6 Additional Security Measures

4.5.6.1 Application Log Information

Test Suite

A user can access the application log in transaction `SLG1`. The according object is `SMT_TWB`. The following sub-object are available:

- `DEFAULT` Default Log
- `OTPK_INBOUND_SYNC` Transfer test results from external tool to test package
- `OTPK_OUTBOUND_SYNC` Transfer test package content to external test tool
- `OTPK_PREREQ_CHK` Prequisite check for inbound test package synchronization
- `SM_TSTA_MIGT` Test Status Migration Object
- `TPLN_DS` Digital Signature for Test Plan

CBTA - TAO

A user can access the application log in transaction `SLG1`. The according object is `SOLAR` with sub-object `TST`.

4.5.6.2 System Under Test (SUT) Management

SUT Management - Additional Password Management Application (Mass Update)

SUT Management allows you to control passwords for your tester categories in a flat list.

> ⚠ Caution
>
> Due to the security critical nature of this scenario, we strongly advice the following security measures:
>
> - The System Under Test (SUT) should be of type *Test System* or *Quality System*. Do not run SUT management on a development system or even a productive system.
> - Only register recognizable test user IDs instead of a Business user IDs.
> - Make sure, that any test user for this scenario has limited authorizations to solely verify exactly the scenario to be tested.

4.6 Main Authorization Objects

Authorization Objects Test Suite

Authorization Object SM_TPCK

The authorization objects allow to access and to manage the test packages in SAP Solution Manager. It is included in roles `SAP_STWB_2_*`.

Authorization Object SM_TPLN

The authorization objects allow to access and to manage test plans in SAP Solution Manager. It is included in roles `SAP_STWB_2_*`.

> → Recommendation
>
> How to best maintain the object field `BO_SERVICE`: Use the value help (F4) for the *Query* tab. Here, enter the BO name and node name you require. The system returns a *Query Name List*. Here you can select your required query.

Authorization Object SM_TFLW

The authorization objects allow to access and to manage the test sequences in SAP Solution Manager. It is included in roles `SAP_STWB_*`.

Run Archiving Reports

To be able to run specific archiving reports, you require authorization object S_PROGNAM with report names. This object allows specific authorization for named reports only. It is contained in the standard role SAP_STWB_2_ALL.

User Interface Work Center

Authorization Object SM_WC_VIEW

Within release 7.2, the work center is redesigned, though you can still open the old work center using transaction STWB_OLD. You can restrict the views for both work center within the authorization field help.

Basic Authorizations

Authorization Groups for Tables (S_TABU_DIS)

Test Suite uses authorization group TSTM to protect tables. The group is added to authorization object S_TABU_DIS in the relevant roles.

Protection RFC Connections (S_ICF)

Test Suite uses Trusted RFCs. The RFCs are protected by authorization object S_ICF with value TST_*. Make sure to assign this authorization only to dedicated users.

Knowledge Warehouse / Document Management Authorization

Document (S_SMDDOC)

Test Suite uses document folders that are specific for Test Suite, as users create test notes, test results, test plan, and test package attachments from test documents. The relevant authorization object S_SMDDOC is contained in roles SAP_SM_KW_* allowing values that are contained in table SMDFLDGRP. By default, all folder groups are allowed. Test notes, test results, test plan, and test package attachments are stored in a KW folder that has the name of the solution added by naming convention TWB. If you want to restrict folders specifically for Test Suite documents, make sure that you need to add this naming convention <.TMW> as addition to the solution, <technical solution name>.TWB.

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

4.7.1 Introduction

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.

4.7.2 Getting Started

What is this guide about? SAP Solution Manager covers a wide range of divers 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.

4.7.3 Prerequisites

4.7.3.1 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
7. SAP Backend

4.7.3.2 Scenario Configuration

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

- Custom Code Management
- Business Process Change Analyzer

You should configure at least Custom Code Management to use SEA successfully. For configuration information and users, see the respective scenario-specific guides for both scenarios. Both scenarios are configured in SAP Solution Manager Configuration (transaction SOLMAN_SETUP).

Configuration User SMC_SEA_***

Single Roles	Restriction on
SAP_SEA_CONFIG	AUTH_SAP_SEA_CONFIG
SAP_SM_SMUA_ALL	AUTH_SAP_SM_KW_DIS

Single Roles	Restriction on
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_ITEST
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC_ARCHIVE
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY

Dialog S-User Assignment

If you use SEA together with the *Maintenance Planner*, you must assign the relevant S-users in table AISUSER in transaction AISUSER. In addition, in the SAP Solution Manager system in SAP Solution Manager Configuration (transaction SOLMAN_SETUP) under *System Preparation* > *Set Up Connections to SAP*, check section *S-User Assignment for AISUSER Table*.

Additional Authorizations for the Configuration Procedure

If you need to transport specific settings during the configuration, you need to assign authorization object S_TRANSPRT with DTRA and ACTVT 01 (create) and 02 (change) together with authorization object S_SYS_RWBO as well as S_DEVELOP for BAdI implementation.

4.7.3.3 Communication Channels and Technical Users

During the guided activity for SEA analysis, systems are selected that are used during the analysis run. For these systems, RFC connections and access to a BW system are required.

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

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to SAP backend system	HTTPS	Technical Communication S-User	Search for SAP Notes
SAP Solution Manager to/ from SAP BW system/client **Note** Check the Secure Configuration Guide section *Communication with SAP BW*			Analysis runs
`MDX PARSER` for `ODBO BAPI`			Used for the creation of semi-dynamic TBOM
SAP Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	RFC	Named end-user (customer specific)	Required for TBOM recording
SAP Solution Manager to managed systems (Login) `SM_<SID>CLNT<Client>_LOGIN`	RFC	Named end-user (customer specific)	Workaround to using trusted RFC. Optional as login RFC connection can also be used. Needed for TBOM recording of automatic test cases (traces)
Managed systems to SAP Solution Manager (Back) `SM_<SID>CLNT<Client>_BACK`	RFC	`SMB_<SID of Solution Manager>`	For recording of automated test cases to receive trace information about which functions in which managed systems were analyzed
SAP Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		Graphics inclusion **Restriction** Manually created in transaction `SM59`

4.7.4 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.

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 SEA_ADM_*** (Help Text ID: TP_SEA_ADMIN)

Single Roles	Restriction on
SAP_SEA_ALL	AUTH_SAP_SEA_ALL
SAP_SM_BPCA_RES_ALL	AUTH_SAP_SM_BPCA_RES_ALL
SAP_SM_BPCA_TBOM_EXE	AUTH_SAP_SM_BPCA_TBOM_EXE
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
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_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

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.

Single Roles	Remarks
SAP_BI_E2E_BPCA	AUTH_SAP_BI_E2E

Display User SEA_DIS_*** (Help Text ID: TP_SEA_DISPLAY)

Single Roles	Restriction on
SAP_SM_BPCA_TBOM_DIS	AUTH_SAP_SM_BPCA_TBOM_DIS

Single Roles	Restriction on
SAP_SM_BPCA_RES_DIS	AUTH_SAP_SM_BPCA_RES_DIS
SAP_SEA_DISPLAY	AUTH_SAP_SEA_DISPLAY
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_SMWORK_ITEST	AUTH_SAP_SMWORK_ITEST
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BPCA_CRM_INTEGRATION	AUTH_SAP_BPCA_CRM_INTEGRATION

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.

Single Roles	Remarks
SAP_BI_E2E_BPCA	AUTH_SAP_BI_E2E

4.7.5 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

S_DEVELOP

In case you require to implement BAdIs in your own name space, you need to adapt authorization object S_DEVELOP, specifically your own package.

5 Application Operations and Business Process Operation

5.1 Introduction

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

5.2 Document History

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

Support Package Stacks (Version)	Description
SP19	**Job Management - Third Party Tool Integration Redwood** • Updated role `SAP_SM_SCHEDULER_ADMIN` • Updated role `SAP_SM_SCHEDULER_TOP` • Updated authorization object `SM_JSM_SDL` with new activity `ACTVT 07` (copy scheduling) • Updated role `SAP_SM_REDWOOD_COMMUNICATION`
SP13	**Business Process Operations** • updated role `SAP_SM_DSWP_OP_BPM` • updated role `SAP_SM_DSWP_OP_BPM_DIS` **Technical Monitoring** • adapted role `SAP_SMWORK_TECH_MON` (added transaction code for easier handling, no update required)
SP12	**Job Management - Third Party Tool Integration Redwood** • Reworked section on External Integration - Third Party • Shipped new role `SAP_SM_REDWOOD_COMM_EXT_SDL`
SP11	**Business Process Operations** • added new section on *Integration Repository* in chapter *User Roles for Additional Functions* • added role `SAP_SM_BPOINR_EXE` to use case ID `BPO_ADM`. • updated roles `SAP_SM_DSWP_OP_BPM` and `SAP_SM_DSWP_OP_BPM_DISP` • updated role `SAP_BPO_CONFIG` **New: Automation Rate Cockpit** *Automation Rate Cockpit* subsection as part of chapter *Business Process Improvement*. **Job Management** • added new user *Requester* (use case ID `JM_REQ`) • removed obsolete users template users L1 and L2 from transaction `SOLMAN_SETUP`. **BI Monitoring** Updated roles: • `SAP_SM_BIM_LEVEL02` • `SAP_SM_BIM_LEVEL01`

Support Package Stacks (Version)	Description
SP10	**Job Management** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • `SAP_SM_SCHEDULER*` • Added optional user information for Third Party • Adapted third party relevant role `SAP_SM_REDWOOD_COMMUNICATION` **Business Process Operations** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • adapted roles `SAP_OP_DSWP_BPM` and `SAP_OP_DSWP_BPM_DIS` • adapted authorization object `S_TABU_DIS` for new authorization groups `SMSDS` (SDS) and `SMDO` (Digital Operations) **System Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • adapted role `SAP_SM_SYM_CONF` • adapted roles `SAP_SM_SYM_LEVEL01` and `SAP_SM_SYM_LEVEL02` **PI Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • adapted roles `SAP_BI_E2E` and `SAP_BI_E2E_PIM` for PI-relevant queries
SP09	**Job Management** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • `SAP_SM_SCHEDULER*` **Interface Connection Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • adapted role `SAP_SM_IC_LEVEL01` • adapted role `SAP_SM_IC_LEVEL02`
`SP08` Plus	**Technical Monitoring** • adapted section on *Communication Channels* • removed section *Technical Users* • new section *Java Data Collector User* • moved sections *Message Flow Monitoring*, *User Experience Monitoring* to *SAP Fiori Apps Security Guide*. **Business Process Operations and Job Management** • adapted section on *Communication Channels* • removed section *Technical Users*

Support Package Stacks (Version)	Description
SP08	**CDC** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles `SAP_CDC_INSTANCE_CREATOR, SAP_CDC_ADMIN` (new authorization object `SM_CDC_GRP`)
SP07	**BI HANA Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles `SAP_SM_BIMON_*` **Job Management** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Added role `SAP_SM_JMON_LEVEL02` to Job Management use case ID `JM_TOP` **Job Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role `SAP_SM_JMON_LEVEL02`

Support Package Stacks (Version)	Description
SP06	**Business Process Operations** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_MANAGED_BPOANA_ALL **End-User Experience Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_EEM_LEVEL* **Job Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_JMON_LEVEL02 with authorization object SM_GPACUST for Advanced Monitoring purpose **Data Readiness Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_BIMON_*** **Job Management** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Substituted role SAP_SM_JMON_LEVEL02 with role SAP_SM_JMON_LEVEL01 • Adapted roles SAP_SM_SCHEDULER_***, added new business transaction types SMCR, SMIN, SMRQ, removed business transaction type SLFJ in authorization object CRM_ORD_PR, which is obsolete in Release 7.2.

Support Package Stacks (Version)	Description
SP01	**Adaptations with Release 7.2 Relevant for all Subscenarios** • Roles SAP_SMWORK_BASIC_* and SAP_SM_BI_BILO obsolete • All roles for *Technical Monitoring* have been adapted to SAP_BASIS 7.40. • Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_* has been transferred into Core Roles. • Added to all L2 users role SAP_SM_MAI_REPORTING • Removed from all L2 users role SAP_SM_BI_BILO **Adaptations Business Process Operations** • Role SAP_SMWORK_BPM obsolete • Roles SAP_SM_SOLUTION_* and SAP_SOLMAN_DIRECTORY_* are removed from user roles, substituted by new roles SAP_SM_SL_* accordingly, see section on *Users and Authorizations*. • Removed section on *Solution Maintenance* • Added new authorization objects according to Software Components SAP BASIS and ST • Deleted roles SAP_CDC_ADMIN and SAP_CDC_DIS • Additional role assignment for integration with Job Monitoring and Interface Channel Monitoring for template users. **Adaptations Job Management** • Role SAP_SM_SOLUTION_* is removed from user roles, substituted by new roles SAP_SM_SL_* accordingly, see section on *Users and Authorizations*. • Substituted role SAP_BPMJSM_BW_ALL_REPORTING with role SAP_SM_BPMON_REPORTING • All core roles SAP_SM_SCHEDULER_* and role SAP_SMWORK_JOB_MAN adapted • Removed section on *Solution Maintenance* • New authorization objects added from SAP_BASIS • Substituted authorization object SM_JSM_SCH with SM_JSM_SDL **Adaptations System Monitoring** • Work Center for System Monitoring is obsolete, according Work Center role SAP_SMWORK_SYS_MON is not delivered anymore. **Adaptations Interface Channel Monitoring** • Added role SAP_SM_SYM_LEVEL01 to Level 2 user. **SAP Fiori Integration** • All users receive SAP Fiori Embedded Launchpad authorizations, role SAP_SM_FIORI_LP_EMBEDDED

Support Package Stacks (Version)	Description
SP02	**Business Process Operations** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_BP_OPERATIONS_ADMIN_COMP **System Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_SYM_LEVEL* • Added role SAP_DBA_DISP to composite role SAP_SM_L2_COMP **Interface Channel Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_IC_CONF • Added BW authorizations to Level 1 User: SAP_BI_E2E_SM, SAP_SM_BI_DISP **PI Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_PIM_LEVEL* **End-User Experience Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_EEM_LEVEL02

Support Package Stacks (Version)	Description
SP03	**Job Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_JMON_LEVEL* **End - User Experience Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_EEM_LEVEL* • Adapted role SAP_SM_EEM_CONF • Adapted technical names of User IDs from <EEM> to <UXM> • Integration of new SAP Fiori App, see separate section **PI Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_PIM_CONF • Adapted roles SAP_SM_PIM_LEVEL* **BP Operations** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SMWORK_BPO and added Fiori Catalogue for *Data Consistency Management* • New roles SAP_SM_BPOIMP_* for *Business Process Improvement*, see according new section **CDC** Adaptations of terminology for roles. **Message Flow Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Delivered new roles for SAP Fiori App: Message Flow Monitoring, see new section • Adapted roles SAP_SM_MFM_LEVEL* **Interface Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_IC_LEVEL* • Adapted role SAP_SM_IC_CONF **System Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_SYM_LEVEL* **Exception Management** • new section for scenario *Exception Management*.

Support Package Stacks (Version)	Description
SP04	**System Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_SYM_LEVEL* **Business Process Operations** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_CDC_* **BI - Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_BIM_LEVEL* **PI - Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_PIM_LEVEL01 **EE - Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_EEM_LEVEL02

Support Package Stacks (Version)	Description
SP05	**EE - Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted role SAP_SM_EEM_CONF • Adapted roles SAP_SM_EEM_LEVEL* with new values for authorization objects (specifically with ACTVT DL for download in authorization object AI_EEM in level 02 role) and object status adaptations **Job - Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_JMON_LEVEL* and SAP_SM_JMON_CONF with authorization object SM_JSM_DOC due to integration **Job Scheduling Management** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Adapted roles SAP_SM_SCHEDULER_ADMIN and SAP_SM_SCHEDULER_AM with authorization object SM_MOAL_TC due to integration **System - Monitoring** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role Adapted roles SAP_SM_SYM_LEVEL* **Business Process Operations** Adaptations of authorization objects in roles are described in *Menu* tab of the respective role • Added dashboard configuration role SAP_SM_DSH_CONF to BPO Administrator user • Added dashboard display role SAP_SM_DSH_DISP to all BPO end users • Adapted role SAP_BPO_CONFIG (maintained authorization object S_TABU_DIS with appropriate authorization groups, see Description text in the role)

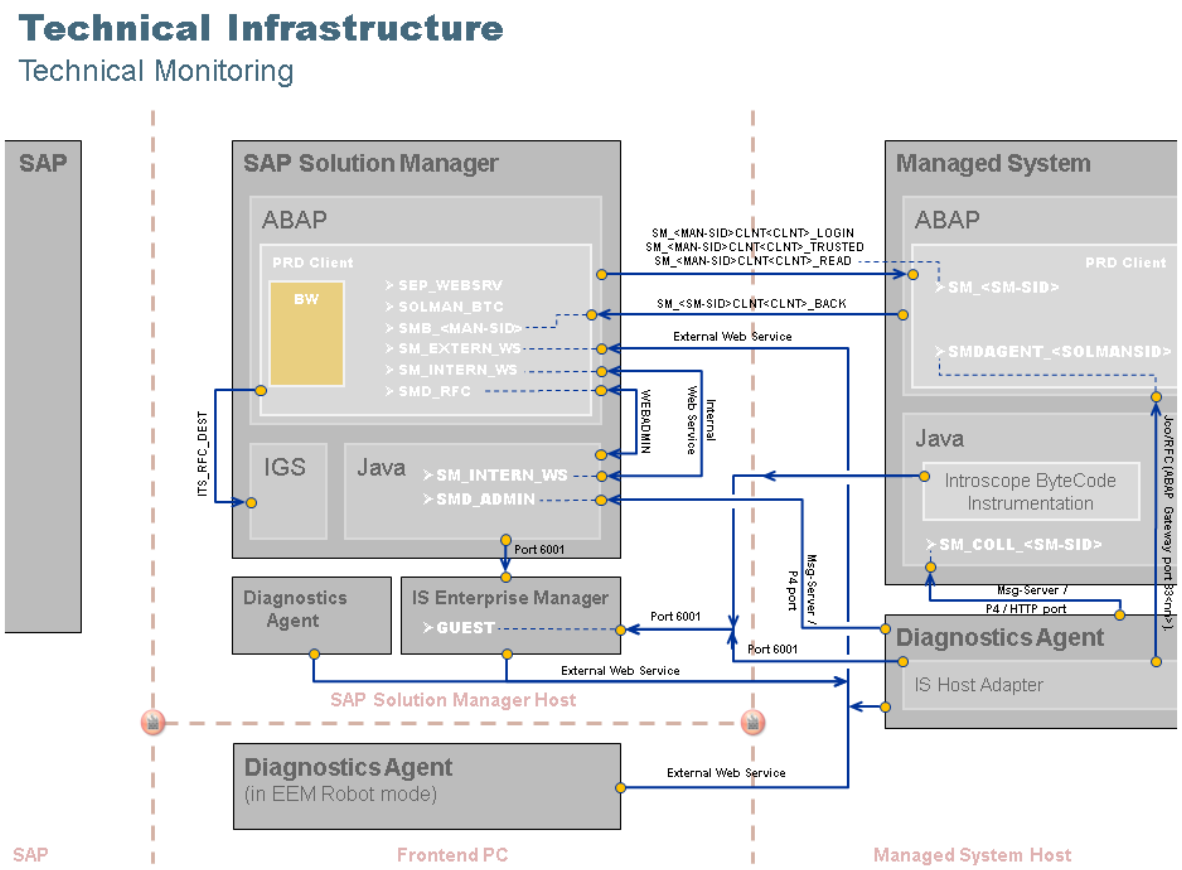
5.3 Scenario-Specific Guide: Technical Monitoring

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 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.



Infrastructure

> ### 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.

5.3.1.2 Scenario Configuration Users

> ### Note
>
> For conceptual information, see the following sections in the *Authorization Concept Guide*:
>
> - Configuration users in SAP Solution Manager, see section *Configuration Users*.
> - BW integration concept

You configure the technical monitoring scenarios using the automated guided procedure in SAP Solution Manager Configuration (transaction SOLMAN_SETUP).

To configure the scenarios, proceed as follows:

Creating Configuration User in SAP Solution Manager Configuration

After you have performed the basic configuration for SAP Solution Manager, you can use 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>`)

  > ⓘ 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`)

  > ⓘ Note
  >
  > To be able to use Infrastructure Monitoring, you must configure:
  >
  > 1. SAP IT Infrastructure Management
  > 2. Infrastructure Monitoring
  >
  > As a prerequisite, you need to have applied the corresponding 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`: Select the *Manual Maintenance* checkbox in the `SOLMAN_SETUP` pop-up and create your user in transaction `SU01`.

  > → Recommendation
  >
  > If you want to create the configuration users manually both for your SAP Solution Manager system and for your BW system, you must assign all single roles as mentioned in SAP Solution Manager Configuration.

- Note

  - To create users and assign user roles, you need to assign as well role `SAP_SM_USER_ADMIN`.
  - To use a trusted RFC connection between the SAP Solution Manager and the managed systems, you must assign role `SAP_SM_S_RFCACL` in the SAP Solution Manager system and the managed system.

- Note

  To use a trusted RFC connection between SAP Solution Manager and the BW system, you must assign role `SAP_SM_S_RFCACL` in the SAP Solution Manager system and role `SAP_SM_BW_S_RFCACL` in the BW system.

Scenario Configuration

To configure the individual scenarios, you need to configure them in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`.

In the specific configuration scenario, you can create standard template users. The system automatically adds all relevant user roles, see the corresponding sections about *Users and User Roles*.

5.3.1.3 Communication Channels and Technical Users

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

Note

All mentioned `RFC` - destinations are automatically created via transaction `SOLMAN_SETUP`, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to SAP Backend system	`HTTPS`	Technical Communication User	Search for SAP Notes

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			
Solution Manager to managed systems (Read) `SM_<SID>CLNT<Client>`	`RFC`	`SM_<SID of Solution Manager>`	**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_<SIDof SolMan>`.
Managed systems to Solution Manager (Back) `SM_<SID>CLNT<Client>_BACK`	`RFC`	`SMB_<SID of Solution Manager>`	
Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	`RFC`	Named End-user (customer specific)	Required for *Message Flow Monitoring*
Solution Manager to managed systems within customer network	`FTP`		Update route permission table, content: `IP` addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		

Communication Channel	Protocol	User	Type of Data Transferred / Function
		`CSMREG` (customer-specific);	
`CCMSPING.<server>` `<SystemNr.>`	Registered Server Program (program `ccmsping.00`)	User created during configuration of Central Monitoring (`CCMS`)	Service Level Reporting with `CCMSPING`; system availability overview in System Monitoring work center; IT Performance Reporting

5.3.1.4 Java - Related Users

Users

User Name	System	Use Case ID
Java data collector user	in managed systems	`SM_COLL_<SIDof SolMan>`
Java - ABAP Connection	in Solution Manager system	`SMD_RFC`

5.3.2 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 all single roles as listed for IT Service Management `TP_IM_PROC` Processor User.

> **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_DSWP_EWA` to your user.

5.3.3 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.

5.3.4 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.

> **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)

5.3.5 User Roles for System, Database, Host Monitoring, and Self - Monitoring

5.3.5.1 First Level User Role

The table underneath gives you a further overview, which single roles are assigned in transaction SOLMAN_SETUP.

First Level User (Help Text ID: TP_SM_L1)

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

5.3.5.2 Second Level User 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 additional 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)

Single Roles	Help Text ID
SAP_SM_SYM_LEVEL02	AUTH_SAP_SM_SYM_LEVEL02

Single Roles	Help Text ID
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_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

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.

Single Roles	Help Text ID
SAP_BI_E2E_SM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

5.3.6 User Roles for Process Integration - Monitoring

5.3.6.1 First Level User 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)

Single Roles	Help Text ID
SAP_SM_PIM_LEVEL01	AUTH_SAP_SM_PIM_LEVEL01

Single Roles	Help Text ID
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

5.3.6.2 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 additional 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)

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

Single Roles	Help Text ID
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

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.

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

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

5.3.7 User Roles for Message Flow Monitoring

5.3.7.1 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

5.3.7.2 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

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

5.3.7.3 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 additional 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)

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

Single Roles	Help Text ID
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_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

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.

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

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

5.3.7.4 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.

5.3.7.5 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

5.3.8 User Roles for End-User Experience Monitoring

5.3.8.1 First Level User 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)

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

5.3.8.2 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 additional 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)

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
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

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.

Single Roles	Help Text ID
SAP_BI_E2E_EEM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

5.3.9 User Roles for HANA and Business Intelligence Monitoring

5.3.9.1 First Level User 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)

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

5.3.9.2 Second Level User 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 additional 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)

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

Single Role	Re
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
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

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.

Single Roles	Help Text ID
SAP_BI_E2E_BIM	AUTH_SAP_BI_BIM
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

5.3.9.3 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.

Application Log

Logging can be accessed using transaction SLG1 with authorization object S_APPL_LOG using field Object E2E_ALERTING with subobject AUTOCONFIG.

5.3.10 User Roles for Interface (Channel) Monitoring

5.3.10.1 First Level User Role

The table underneath gives ywqou 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)

Single Roles	Help TXT ID
SAP_EM_DISPLAY	AUTH_SAP_EM_DISPLAY
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_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

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.

Single Roles	Help Text ID
SAP_BI_E2E_SM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

5.3.10.2 Second Level User Roles

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 additional 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)

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
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
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

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.

Single Roles	Help Text ID
SAP_BI_E2E_SM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

5.3.11 End-User Roles for Job Monitoring

5.3.11.1 First Level User 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)

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
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

5.3.11.2 Second Level User 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 additional 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)

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

Single Role	Remarks
SAP_SYSTEM_REPOSITORY_DIS	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_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_MAI_REPORTING	AUTH_SAP_SM_MAI_REPORTING
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_CENTRAL_JOB_OVERVIEW	AUTH_SAP_SM_CENTRAL_JOB

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.

Single Roles	Help Text ID
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

5.3.11.3 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.

5.3.12 User Roles for Infrastructure Monitoring

5.3.12.1 Introduction

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*.

5.3.12.2 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)

Included 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_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

5.3.12.3 Second Level User 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 additional 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)

Included Single Roles	Help Text ID
SAP_SM_SYM_LEVEL02	AUTH_SAP_SM_SM_LEVEL02
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
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_RCA_DIS	AUTH_SAP_RCA_DIS

5.3.13 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)

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

Role	Help Text-ID
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONF

Cockpit User: EXM_EXE_<SID> (Help TXT: TP_EM_EXE)

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

5.3.14 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.

> **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:

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: • configure IV Discovery settings and to manage flow definitions • navigate to whole “Integration Visibility” User Interface • configure Data Collector execution

Single Role	User Type	Remarks
SAP_IV_DC_SUPPORTER		Corresponds to Technical Supporter. Users assigned to this role, will be able to: • read data from all Integration Visibility tables in NWA Open SQL Data Browser (without BC_IV_DC_EVENT – contains business sensitive information) • navigate to whole "Integration Visibility" User Interface with read-only rights • have full access to: WS Navigator/ Log Viewer/Log Configurator/ WS Log Viewer/ WS Log Configurator/ GET operations from all IV web services
SAP_IV_DC_ADMIN		Composite role. Includes: • SAP_IV_DC_SUBSCRIBE • SAP_IV_DC_EXECUTE • SAP_IV_EVENT_CONSUMER • SAP_IV_DC_CONFIG

5.3.15 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.

5.3.16 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. As all three monitoring areas oberlap in their functionality, application values can overlap as well, such as SAP_SM_BIM_* roles contain authorization for applications *Job Monitoring* and *BI - Monitoring*.

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 objects 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 SAP Support Portal 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 objects 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.

> → Recommendation
>
> The authorization is given by default in role `SAP_SM_EEM_LEVEL02`. If you do not require downloads from the system, we recommend removing it.

Job Documentation: SM_JSM_DOC

This authorization is required in *Job Monitoring* as with every scheduled job also job documentation is required. Roles `SAP_SM_JMON***` include this object.

5.3.17 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`.

You can find details of the jobs in the in the *Self-Monitoring - SAP Solution Manager* app (in the *SAP Solution Manager Administration* launchpad group).

5.4 Scenario-Specific Guide: Business Process Operations

5.4.1 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.

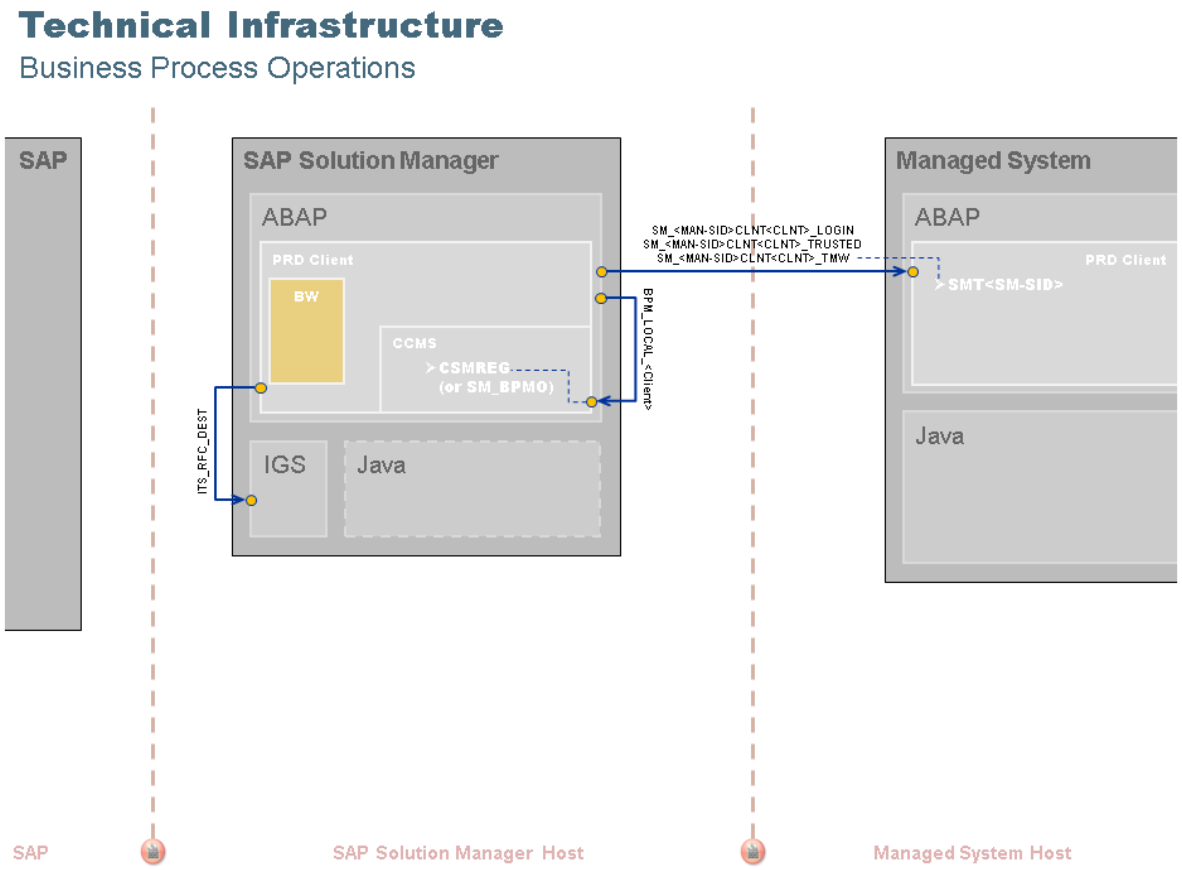
This guide covers the following topics:

- **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 relevant roles that represent them. Here, you also find information on the relevant launchpad groups and apps.
- **User Roles for Additional Functions**: Find out about additional authorization for the launchpad group.
- **Scenario Integration**: In accordance with 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.

5.4.2 Prerequisites

5.4.2.1 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.



Infrastructure

5.4.2.2 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_<XXXClient>` 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.

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
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_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP

If you want to create the configuration user manually, you need to assign all single roles as mentioned in the table above:

- > **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.

Required single roles fort he configuration user in the BW-sytem are:

- - SAP_SM_BI_ADMIN
- - SAP_BI_E2E_BPO

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*.

5.4.2.3 Communication Channels and Technical Users

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

> **Note**
>
> All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP`, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to SAP Backend system	HTTPS	Technical Communication User	Search for SAP Notes
Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to managed systems (TMW) `SM_<SID>CLNT<Client>TMW`	`RFC`	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 **Note** Specific data collectors write log information and details list information into table `/SSA/PTAB` in the managed system. 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. Data collection for monitoring objects that are scheduled to be collected asynchronously will not work. This may result in problems for lasting data collections.
Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	`RFC`	Named End-user (customer specific)	• Mandatory for `CDC` functionality setup, due to necessity of code generation in managed system; • Mandatory for Business Process Monitoring to use according value help from managed systems. Login `RFC` can be used instead, but then the value help must be maintained manually.
`SM_<SID>CLNT<Client>_LOGIN` (`ABAP` connection)	`RFC`	Named End-User (customer-specific)	to be used instead of trusted `RFC`
Solution Manager to managed systems within customer network	`FTP`		Update route permission table, content: `IP` addresses, see section *File Transfer Protocol (FTP)*

Communication Channel	Protocol	User	Type of Data Transferred / Function
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		
`BPM_LOCAL_<Client>`	RFC	`SM_BPMO`(customer-specific) with assigned composite role `SAP_SM_BPMO_COMP`	Logon client is 000. **⚠ Restriction** `RFC` is created during Business Process Operations setup session, not in transaction `SOLMAN_SETUP`.

5.4.3 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.

> **ⓘ 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.

5.4.4 Users and Authorizations

5.4.4.1 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.

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 additional 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_RFACL (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)

Single Roles	Help Text ID
SAP_BC_FDT_ADMINISTRATOR	This role gives access to the *BRFplus Workbench* 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_SCHEDULER_BPO	AUTH_SAP_SM_SCHEDULER_BPO
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
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
SAP_CDC_INSTANCE_EXECUTER	AUTH_SAP_CDC_INSTANCE
SAP_CDC_INSTANCE_ANALYZER	AUTH_SAP_CDC_INSTANCE

Single Roles	Help Text ID
SAP_SM_DSH_CONF	AUTH_SAP_SM_DSH_CONF
SAP_SM_BPOINR_EXE	AUTH_SAP_SM_BPOINR_EXE

> **Note**
>
> If you need to create users in a managed system, single role SAP_SM_S_RFCACL is required.
>
> Remove this role after configuration.

> **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.

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*.

Single Roles	Help Text ID
SAP_BI_E2E_BPO	AUTH_SAP_BI_E2E
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR

> **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.

Assigned Role	Help Text-ID
SAP_MANAGED_BPOANA_ALL	AUTH_SAP_MANAGED_BPOANA_ALL

Analytics/Reporting User (Help Text ID: USER_TP_BPO_REP)

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
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
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP

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*.

Single Roles	Help Text ID
SAP_BI_E2E_BPO	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP
SAP_SM_BI_EXTRACTOR	AUTH_+SAP_SM_BI_EXTRACTOR

> **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.

Assigned Role	Help Text-ID
SAP_MANAGED_BPOANA_DISP	AUTH_SAP_MANAGED_BPOANA_DISP

Alert User (Help Text ID: USER_TP_BPO_ALERT)

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
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORT
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_IC_LEVEL02	AUTH_SAP_SM_IC_LEVEL02
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP

> ### 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)

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

Single Roles	Remarks
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_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP

Display User (Help Text ID: USER_TP_BPO_DIS)

Single Roles	Remarks
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SYM_LEVEL01
SAP_OP_DSWP_BPM_DIS	AUTH_SAP_OP_DSWP_BPM_DIS
SAP_SM_JMON_LEVEL01	AUTH_SAP_SM_JMON_LEVEL01
SAP_SM_GP_DIS	AUTH_SAP_SM_GP_DIS
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_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_DSH_DISP	AUTH_SAP_SM_DSH_DISP

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.

5.4.5 User Roles for Additional Functions

5.4.5.1 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

Main Authorization Objects

SM_CDC_OBJ and SM_CDC_INS

New Role	Authorization object SM_CDC_OBJ "CDC Comparison Object"	Authorization object SM_CDC_INS "CDC Comparison Instance"
SAP_CDC_OBJECT_MODELER "Cross-Database Comparison (Object Modeler)"	01 Create or generate 02 Change 03 Display 06 Delete 07 Activate, generate	03 Display
SAP_CDC_INSTANCE_CREATOR "Cross-Database Comparison (Instance Creator)"	03 Display 36 Extended maintenance	01 Create or generate 02 Change 03 Display 06 Delete
SAP_CDC_INSTANCE_EXECUTER "Cross-Database Comparison (Instance Executer)"	03 Display	03 Display 16 Execute 65 Reorganize
SAP_CDC_INSTANCE_ANALYZER "Cross-Database Comparison (Instance Analyzer)"	03 Display	03 Display 35 Output

CDC - Authorizations Overview

5.4.5.2 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
  This user is also relevant for *Automation Rate Cockpit (RCA)*.
- Analytics User: SAP_SM_BPOIMP_EDIT
- Display User: SAP_SM_BPOIMP_DIS
  This user is relevant for ARC.

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). It protects objects in table AGS_BPA_OBJ, which can be accessed using the *Persistence Manager*. Additional object types for ARC are:

- ARC_SIM_VARIANT
- ARC_DASHBOARD

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.

Logging of Changed Objects

In the Persistence Browser, logging is done for any changed object. This browser can be accessed running report AGS_BPA_PERSISTENCE_BROWSER.

Automation Rate Cockpit

In general, the roles relevant for Business Process Improvement are also relevant for this function. See above.

Additonal notes:

- The display user can create, change and delete simulation variants
- Private variants are only visible for the user who created them
- Public variants are checked by the authorization object `SM_BPA_OBJ` for object type `ARC_SIM_VARIANT`.
- Each simulation variant is directly referring to one AR Dashboard. Therefore, you must assign the correct dashboard authorization to the individual user.

Authorization Group for S_TABU_DIS

Table access is protected by authorization group `SBPO`.

5.4.5.3 Integration Repository and Interface Discovery

The Integration Repository and Interface Discovery function is part of the Business Process Operation Application. It can be used in managed systems.

Users and User Roles in the Managed System

Configuration User

You can assign to the configuration user in the managed system role `SAP_BPM_INT_CONF`.

- Can execute the Interface Discovery for IDoc, qRFC and Web service.
- Can check the status of the qRFC Table Shadowing.
- Can activate the qRFC Table Shadowing.
- Can execute the evaluation for qRFC.

Display User

You can assign to the display user in the managed system role `SAP_BPM_INT_DIS`.

- Can check the status of the qRFC Table Shadowing.

Users and User Roles in the SAP Solution Manager System

User Roles for End-Users. There is no use case ID available in the SAP Solution Manager. You need to assign the following roles manually to your end-.users.

End-User

Single Role	Help Text ID
SAP_SYSTEM_REPOSITORY_EDIT	AUTH_SAP_SYSTEM_REPOSIORY_EDIT
SAP_SMWORK_BPO	AUTH_SAP_SMWORK_BPO
SAP_SM_BPOINR_EXE	AUTH_SAP_SM_BPOINR_EXE
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT

Display User

Single Role	Help Text ID
SAP_SYSTEM_REPOSITORY_DISP	AUTH_SAP_SYSTEM_REPOSIORY_DISP
SAP_SMWORK_BPO	AUTH_SAP_SMWORK_BPO
SAP_SM_BPOINR_DISPLAY	The role allows display of the Integration Repository application.
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

Main Authorization Objects

Screen Restriction SM_BPM_DET

The object restricts access to Solution Manager applications for BPM in the managed systems. In Interface Discovery, it is used to restrict the access to the Interface Discovery execution from the selection screen of program.

Table Protection S_TABU_DIS

Tables `/SDF/IFR_TRFCQIN` und `/SDF/IFR_TRFCQOU` are protected by authorization group `STPI` in the managed system.

Integration Repository Protection SM_INR

The authorization object `SM_INR` is used in the SAP Solution Manager system to protect the application Integration Repository.

SAP Cloud Platform Integration

The functions allows an integration into the SAP Cloud Platform. Here, all security measures for the backend system SAP Solution Manager remain consistent. For more information on the SAP Cloud Platform

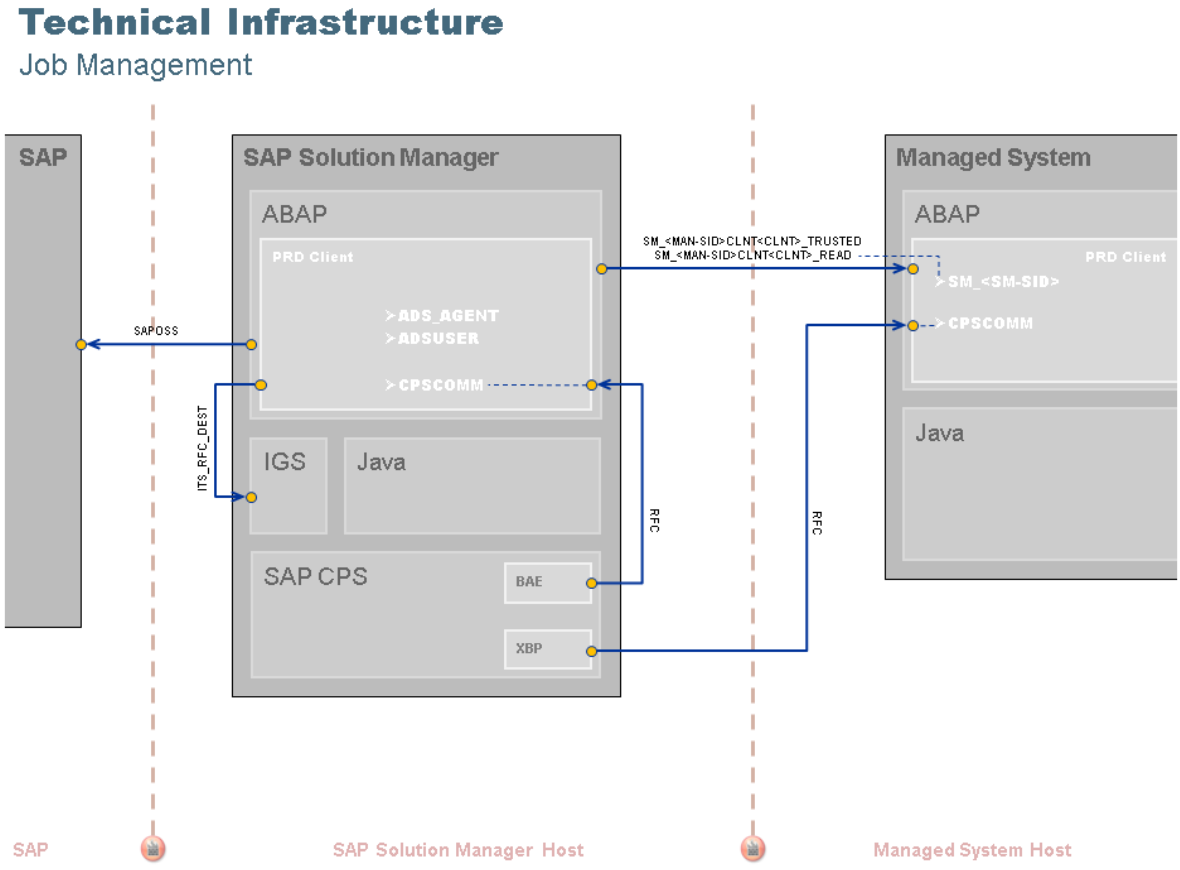
security, check the following document:https://help.sap.com/doc/e4ecfa7accb642ffad68328130244d69/Cloud/en-US/SAP_CloudIntegration_SecurityGuide_External.pdf.

5.5 Scenario-Specific Guide: Job 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 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.



Infrastructure

5.5.1.2 Scenario Configuration User

> **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_JM_<XXXClient>) for Job Management (Help Text ID: USER_CONFIG_JM) 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.

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

Single Roles	Help Text ID
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_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP

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

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 all sibgle roles as mentioned in the table above.

- ⓘ 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.

- ⓘ 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.

5.5.1.3 Communication Channels and Destinations

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

> **Note**
>
> All mentioned RFC - destinations are automatically created via transaction SOLMAN_SETUP, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to SAP Backend system	HTTPS	Technical Communication User	Search for SAP Notes
Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			
Solution Manager to managed systems (Read) SM_<SID>CLNT<Client>	RFC	Default user: SM<SID of Solution Manager system>	Necessary for all functions in implementation and upgrade
Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) ITS_RFC_DEST	Activation Type Registered Server program (program: IGS.<SID>)		

Communication Channel	Protocol	User	Type of Data Transferred / Function
		CPSCOMM **Note** for communication between SAP `CPS` and SAP Solution Manager, assigned roles `SAP_SM_REDWOOD_COMMUNICATION` and `SAP_BC_REDWOOD_COMM_EXT_SDL`	
SAP CPS	RFC		See SAP Note 1037903 and section *External Integration → SAP Central Process Scheduler*.

5.5.2 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.

5.5.3 Users and Authorizations

5.5.3.1 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)

Single Role	Help Text ID
SAP_BC_BATCH_ADMIN_REDWOOD	AUTH_SAP_BC_REDWOOD
SAP_BC_REDWOOD_COMM_EXT_SDL **Note** Both roles are only needed for managing external schedulers.	AUTH_SAP_BC_REDWOOD
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING
SAP_CM_SMAN_CHANGE_MANAGER	AUTH_SAP_CM_SMAN_CHANGE_MANAGER
SAP_CM_SMAN_DEVELOPER	AUTH_SAP_CM_SMAN_DEVELOPER
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_REPOSIORY_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

Single Role	Help Text ID
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 **Note** The administration user receives role SAP_SM_RFC_ADMIN due to administration tasks. If this is not required, assign SAP_SM_RFC_DISP instead.	AUTH_SAP_SM_RFC_ADMIN
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

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)

Single Role	Help Text ID
SAP_BC_BATCH_ADMIN_REDWOOD	AUTH_SAP_BC_REDWOOD
SAP_BC_REDWOOD_COMM_EXT_SDL **Note** Both roles are only needed for managing external schedulers.	AUTH_SAP_BC_REDWOOD
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING

Single Role	Help Text ID
SAP_CM_SMAN_DEVELOPER	AUTH_SAP_CM_SMAN_DEVELOPER
SAP_SOCM_DEVELOPER	AUTH_SAP_SOCM_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_PROC	AUTH_SAP_SM_CRM_UIU_PROC
SAP_SM_CRM_UIU_SOLMANPRO_CHARM	AUTH_SAP_SM_CRM_UIU_CHARM
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
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
SAP_SM_JMON_LEVEL02	AUTH_SAP_SM_JMON_LEVEL02

In the BW - System

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

Single Role	Help Text ID
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING
SAP_CM_SMAN_CHANGE_MANAGER	AUTH_SAP_CM_SMAN_CHANGE_MANAGER

Single Role	Help Text ID
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_REPOSIORY_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

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

Single Role	Help Text ID
SAP_SM_BPMON_REPORTING	AUTH_SAP_SM_BPMON_REPORTING

Single Role	Help Text ID
SAP_SOCM_REQUESTER	AUTH_SAP_SOCM_REQUESTER
SAP_SM_SCHEDULER_AM	AUTH_SAP_SM_SCHED_AM
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSIORY_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_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

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) Obsolete as of SP11

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

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_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

Level 1 User (Technical User Name: JM_L1_XXX) Obsolete as of SP11

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_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_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
SAP_SM_SOLUTION_DIS	AUTH_SAP_SM_SOLUTION_DIS

Single Role	Help Text ID
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

type

Requester User (Use Case ID: JM_REQ; Help Text ID: TP_JM_REQ)

This user is introduced as of SP11 and substitutes template users JM_L1 and JM_L2.

> ### ⚠ Restriction
>
> By default in transaction SOLMAN_SETUP, the user is assigned two core scenario roles. If you create this template user via SOLMAN_SETUP, both roles are assigned to your end user. You have the following possibilities to proceed:
>
> 1. Keep both roles to be able to access and execute *Request Batch Job* via *Job Request* (simple and detailed UI) and *Request Batch Job* via *Job Document* (simple UI).
> 2. Deassign role SAP_SM_SCHED_REQ_JD from your user, if you prefer to execute *Request Batch Job via Job Request* (simple and detailed UI) only.
> 3. Deassign role SAP_SM_SCHED_REQ_JR from your user, if you prefer to execute *Request Batch Job via Job Document* (simple UI) only.

The offered core scenario roles differ in their authorization objects as follows:

- SAP_SM_SCHED_REQ_JD
  - full authorization for authorization object SM_JSM_DOC (01 create, 02 change, 03 display, and 06 delete.

    > ### ⚠ Caution
    >
    > Due to security reasons, valu e07 *Import Job* has to be assigned, manually.

    Value
  - read authorization (value 03) for authorization object SM_JSM_REQ (Request Batch Job via Job Request)
- SAP_SM_SCHED_REQ_JR
  - full authorization for authorization object SM_JSM_REQ (01 create, 02 change, 03 display, and 06 delete).
  - read authorization (value 03) for authorization object SM_JSM_DOC (Request Batch Job via Job Document)

Single Role	Help Text ID
SAP_SM_SCHED_REQ_JR	AUTH_SAP_SM_SCHED_REQ_JD

Single Role	Help Text ID
SAP_SM_SCHED_REQ_JD	AUTH_SAP_SM_SCHED_REQ_JR
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_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_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

Display User (Technical User Name: JM_DIS_XXX)

In the Solution Manager

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
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

Single Role	Help Text ID
SAP_TASK_INBOX_DIS	AUTH_SAP_TASK_INBOX_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_SOLUTION_DIS	AUTH_SAP_SM_SOLUTION_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY

In the BW - System

Single Role	Help Text ID
SAP_BI_E2E_JSM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

Authorization Objects

SM_MOAL_TC

Job Monitoring can be accessed from three entry points:

- System and Application Monitoring
- Job Management Work Center
- BPO Work Center

The object restricts access to Job Monitoring from all three access points. It is therefore included in the according roles for BPO, Job Monitoring, and System Monitoring.

5.5.4 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

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

5.5.5 External Integration

5.5.5.1 SAP Business Process Automation - SAP Central Process Scheduler (SAP CPS) and SAP BPA by Redwood

SAP Business Process Automation by Redwood is a job scheduling tool you can use to automate business processes across your SAP landscape. You can integrate SAP BPA with SAP Solution Manager Job Documentation / Job Management.

> ⓘ Note
>
> 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.

SAP CPS / SAP BPA

Using SAP CPS / SAP BPA, 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.

Name	Type	Remarks
SAP_SM_REDWOOD_COMMUNICATION	ABAP	Role assigned to the technical user (for instance REDWOOD) to communicate from SAP Central Process Scheduler to the SAP System to schedule background jobs with a link to the Solution Manager Job Documentation; applied to technical user in managed SAP system / SAP Solution Manager as a managed system
SAP_BC_REDWOOD_COMMUNICATION	ABAP	Role assigned to the technical user (for instance REDWOOD) in the managed system to communicate from SAP Central Process Scheduler to the SAP System to schedule background jobs.
SAP_BC_REDWOOD_COMM_EXT_SDL	ABAP	Role assigned to the technical user (for instance SM_REDW) in the SAP Solution Manager system to communicate from SAP Central Process Scheduler to SAP Solution Manager for configuration of parameter SAP_EnableRfcServer on the process server.
SAP_SM_REDWOOD_COMM_EXT_SDL	ABAP	Authorization for a user to communicate from SAP Solution Manager to SAP Central Process Scheduler to hand over job information and to fetch job execution information. For information on user type, see underneath.

Background Information

You can run the external integration with Redwood with two different options:

- Schedule jobs directly using Redwood with an ABAP system
  Using Redwood, you can schedule background jobs in your SAP systems, for instance you can define a job in Redwood together with the job schedule in SAP Solution Manager. Then, Redwood regularly triggers the job execution. For this, you need to create a technical user in the ABAP system and assign role SAP_BC_REDWOOD_COMMUNICATION to this user.
- Schedule jobs using SAP Solution Manager. This option allows also for job documentation integration.
  With SAP Solution Manager you can manage your job scheduling. For instance, you can document your background jobs in SAP Solution Manager and hand them over to regular execution to the managed SAP system. For this, you need to link your managed SAP System to SAP Solution Manager via RFC connection. You can integrate SAP Solution Manager job management with Redwood job scheduling via SMSE interface. For instance, you hand over from SAP Solution Manager job information to Redwood, and Redwood triggers the job execution together with a link to the job documentation. For this, you need to create a technical user in the ABAP system and assign role SAP_SM_REDWOOD_COMMUNICATION to this user.

Job scheduling using SAP Solution Manager

For this option, you require different users and roles in the SAP Solution Manager system, which you need to create manually:

- Technical User of type System to communicate with Redwood (e.g. `SM_REDW`). This user is assigned role `SAP_BC_REDWOOD_COMM_EXT_SDL`. You need to create the user manually in the SAP Solution Manager system.
- **Alternatives for reading information from Redwood**
  - **Dialog User:** to hand over and read (administer) the job scheduling information. We recommend using the use case ID user JMT and assign additionally role `SAP_SM_REDWOOD_COMM_EXT_SDL`

    > ⓘ Note
    >
    > In the Redwood system, you need to create a user with the same ID. If you use a user with a different user ID, you can assign this user ID as ALIAS user in SAP to the dialog user. An ALIAS user can only be assigned to one SAP dialog user. Therefore, if you use Alias user IDs, you require for every SAP Solution Manager user a dedicated user in the Redwood system.

  - **Generic User:** If you want to allow reading data from the Redwood system with one generic technical user, such as `SMSE_DISPLAY` or a named user, you need to:
    - create the user manually in both, SAP Solution Manager system and the Redwood system
    - assign role `SAP_SM_REDWOOD_COMM_EXT_SDL` to this user in the SAP Solution Manager system
    - enter the technical user `SMSE_DISPLAY` in table `AGS_JOB_CONFIG` with the added parameter `CPS_FALLBACK_UNAME`
    - If you like to start the process by using a dialog user, such as the Requester dialog user for Job Scheduling, you need to assign role `SAP_SM_REDWOOD_COMM_EXT_SDL`, and substitute in authorization object `S_BTCH_EXT ACTVT 01` with `ACTVT 33`.
      Then, the system transfers the information from the dialog user automatically to the technical user `SMSE_DISPLAY`, which in turn fetches the information from Redwood.

  Make sure, to create as well a technical user in the ABAP managed system and assign role `SAP_BC_REDWOOD_COMMUNICATION`.

  > → Tip
  >
  > For this option, remove authorization object `S_BTCH_EXT`.

Security Information

To be able to read or write in/from Redwood, authorization object `S_BTCH_EXT` is checked by the system. For instance, technical user `SMSE_DISPLAY` is allowed to write (`ACTVT 01`), while dialog user Requester is only allowed to display (`ACTVT 33`).

6 Change Control and IT Service Management Scenarios

6.1 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 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.

6.2 Document History

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

Support Package Stacks (Version)	Description
SP21	IT Service Managament Text adaption in section *Scenario Integration* (Monitoring Requirement)
SP20	**IT Service Managament** Reference to authorization object `CRM_ORD_TE` added for technical user `SM_ITSM` **Change Request Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • `SAP_CM_SMAN_DEVELOPER`
SP19	**IT Service Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. `SAP_SM_ITSM` **Change Request Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • `SAP_CM_MANAGED_DEVELOPER` (as of ST-PI 740 SP23) • `SAP_CM_MANAGED_TESTER` (as of ST-PI 740 SP23) • `SAP_CM_MANAGED_OPERATOR` (as of ST-PI 740 SP23) • `SAP_CM_MANAGED_CHANGEMAN` (as of ST-PI 740 SP23) • `SAP_CM_MANAGED_RELEASEMAN` (as of ST-PI 740 SP23) • `SAP_CM_MANAGED_ADMIN` (as of ST-PI 740 SP23)
SP16	**Change Request Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • `SAP_CM_SMAN_DEVELOPER` • shipped new role for Change Request Management and Test Suite integration `SAP_SM_CM_TEST_INT`. For more information, see section *E2E Integrations* → *Solution Manager Scenario Integrations*.

Support Package Stacks (Version)	Description
SP15	**Change Request Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted authorization object `S_RFC` for ATC check function in role `SAP_SOLMAN_TMW_702` for TMW - user `SMT<SID>`, for more information see section *Main Authorization Objects Change Request Management* and update the role via SAP Note 2257213 • `SAP_CM_SMAN_DEVELOPER` • `SAP_CM_SMAN_OPERATOR` • `SAP_CM_SMAN_ADMINISTRATOR` • `SAP_SOCM_CHANGE_MANAGER` • `SAP_SOCM_ADMIN` • `SAP_SM_CHM` • `SAP_CM_MANAGED_DEVELOPER` (as of ST-PI 740 SP18) • `SAP_CM_MANAGED_TESTER` (as of ST-PI 740 SP18) • `SAP_CM_MANAGED_OPERATOR` (as of ST-PI 740 SP18) • `SAP_CM_MANAGED_CHANGEMAN` (as of ST-PI 740 SP18) • `SAP_CM_MANAGED_RELEASEMAN` (as of ST-PI 740 SP18) • `SAP_CM_MANAGED_ADMIN` (as of ST-PI 740 SP18) **IT Service Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. -`SAP_SM_ITSM`

Support Package Stacks (Version)	Description
SP14	**Change Request Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted authorization object `S_DEVELOP` for ATC check function in role `SAP_SOLMAN_TMW_702` for TMW - user `SMT<SID>`, for more information see section *Main Authorization Objects Change Request Management* and update the role via SAP Note 2257213 • adapted role `SAP_CHARM_CONFIG` • adapted role `SAP_CM_MANAGED_CTS_DEV` • adapted role `SAP_CM_SMAN_OPERATOR` • removed role `SAP_SM_GCTS_TWM` for user `SMT<***>` (technical user for TMW RFC - Connection) • new roles: • `SAP_CM_MANAGED_CTS_OPERATOR` • `SAP_CM_MANAGED_CTS_CHANGEM` • `SAP_CM_MANAGED_CTS_TESTER` • `SAP_CM_MANAGED_CTS_ADMIN` *Section: Integration with Git-enabled CTS (GCTS)* • The use case requirements have changed due to security protection measures. GCTS is enabled for individual business users on the managed systems. • Added additional information concerning TMW user authorization changes. The following function modules have been removed from role SAP_SOLMAN_TMW_702: • `TMW_CREATE_TRANSPORT` • `TMW_GET_REPO_CURRENT_COMMIT` • `TMW_GET_DEPLOY_HISTORY` • `TMW_GET_IMPORT_LOG` • `TMW_GET_REPOSITORY_BRANCH` • `TMW_RELEASE_TRANSPORT` • `TMW_VERIFY_GCTS_CFG` • `TMW_GET_COMMIT` • added new additional roles for managed systems business users
SP13	**Change Request Management** • adapted role `SAP_CM_SMAN_ADMINISTRATOR`

Support Package Stacks (Version)	Description
SP12	**Change Request Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • Restructured section *E2E Integration*. • Added *Best Practice Recommendation* to section *Users for Retrofit* *New section: Integration with Git-enabled CTS* • adapted role `SAP_SM_CHM` • adapted roles SAP_CM_SMAN* and SAP_SOCM* (for Git-enabled integration) • extended section on *End-to End Integration* for *Integration with Git-enabled CTS* • delivered additional role `SAP_SM_GCTS_TWM` (authorizations for Git-enabled CTS integration (SMTM<SID> user))
SP11	**Change Request Managament** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role `SAP_SM_CHM` • adapted section *Communication Channels and Users* for TMW User • adapted section *E2E Integration* with information on *SAP Cloud Platform* integration • adapted role `SAP_SOCM_CHANGE_MANAGER` • adapted role `SAP_CM_QGM_MANAGED_SETUP` **Incident Management** New technical background job user `SM_ITSM`.
SP10	**Change Request Managament** • adapted roles `SAP_CM_SMAN_TESTER`, `SAP_CM_SMAN_CHANGE_MANAGER`, `SAP_CM_SMAN_ADMINISTRATOR` • adapted role `SAP_SM_CHM` • adapted role `SAP_SOCM_REQUESTER`

Support Package Stacks (Version)	Description
SP09	**Incident Managament** • old transaction types are no longer supported **Quality Gate Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role `SAP_QGM_CONFIG` to access new step *Background Jobs* in guided procedure for *Change Request Management* (`SM_SETUP`). For more information, see section • substituted role `SAP_SM_ESH_ADMIN` with `SAP_SM_ESH_DISP` for configuration user `SMC_QGM*`. For more information, see section **Change Request Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role `SAP_CHARM_CONFIG` • adapted role `SAP_SOCM_ADMIN` • adapted role `SAP_CM_SMAN_DEVELOPER, SAP_CM_SMAN_CHANGE_MANAGER, SAP_CM_SMAN_ADMINISTRATOR` • additional BACK RFC user authorizations, see section *Communication Channels and Relevant Users* • extended background jobs scheduled by technical user SM_CHM, see section *Technical User for Background Jobs SM_CHM* **Requirements Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role `SAP_RM_CONFIG`
SP08 Plus	**Quality Gate Management, Incident Management** • adapted section on *Communication Channels* • removed section *Technical Users* **Change Request Management** • adapted section on *Communication Channels* • removed section *Technical Users* • new section *Technical User for Background Jobs SM_CHM*

Support Package Stacks (Version)	Description
SP08	**Incident Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. adapted role SAP_SUPPDESK_CONFIG **Quality Gate Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted all SAP_SM_QGM* roles **System Recommendation** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. adapted roles SAP_SYSREC_* **Change Request Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles SAP_CM_SMAN* • added a new technical user SM_CHM and according user role SAP_SM_CHM for Back RFC specific to Change Request Management. It runs an event triggered backgrond job after every import into a managed system. • adapted roles SAP_SOCM_ADMIN, SAP_SOCM_CHANGE_MANAGER, SAP_SOCM_TESTER, SAP_SOCM_DEVELOPER • adapted role SAP_SM_UIU_SOLMANPRO_ADMIN • adapted role SAP_CHARM_CONFIG **Requirements Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted role SAP_RM_ITREQ_ADMIN • adapted role SAP_RM_ITREQ_MANAGER • adapted roles SAP_RM_BP_EXPERT and SAP_RM_BUSINESS_MANAGER • adapted role SAP_RM_CONFIG • removed role SAP_RM_ADD_CONF from configuration Use Case ID SMC_RM*

Support Package Stacks (Version)	Description
SP07	**General** Introduced generic role for Transport Management for all configuration scenarios (use case IDs `SMC_*`) **Configuration Validation** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles `SAP_CV_*` (new authorization object `AI_CCDB_CU`) **Quality Gate Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles `SAP_SM_QGM_ALL` and `SAP_SM_QGM_CHANGE` **Requirements Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • added roles `SAP_SETUP_INFRASTR_DISP, SAP_SETUP_BASIC_DISP, SAP_SETUP_BASIC_APPLOG` to `SMC_RM*` Use Case ID • adapted role `SAP_RM_CONFIG` (with critical authorization objects `S_NUMBER, S_TABU_NAM`) **System Recommendation** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles `SAP_SYSREC*`

Support Package Stacks (Version)	Description
SP06	**Incident Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles SAP_SUPPDESK* due to new Transaction Type SMDT (Incident for Damaged Test Cases) **Quality Gate Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles SAP_QGM_CONFIG • adapted roles SAP_SM_QGM_CM_ALL, SAP_SM_QGM_CM_TRANSPORT, • removed authorization object SM_CM_DGP from roles SAP_SM_QGM_CM_QAB and SAP_SM_QGM_CM_QM. For more information on the authorization object, see section on *Specific Authorization Objects* in this guide **Requirements Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted all roles SAP_RM* with authorization object SM_CM_FUNC • extensive adaptation of configuration role SAP_RM_CONFIG to run the GP in transaction SOLMAN_SETUP. For more information, see according section in this guide. • added role SAP_SETUP_BASIC_ARCHIVE to user SMC_RM_*** **Change Request Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted roles SAP_SOCM_* for instance SAP_SOCM_ADMIN with inactive authorization object SM_SUTMNGT. For more information, see section on *Main Authorization Objects* in this guide. • adapted roles SAP_CM_SMAN_*** with new values for authorization object SM_CM_FUNC • adapted role SAP_CHARM_CONFIG for user SMC_CH_*** with SM_SETUP authorization to sub-GP for ChaRM as well as read access to JSM steps in the GP for the integration of Job Scheduling Management • adapted roles SAP_SM_*UIU*_SOLMANPRO* • ship new role SAP_CM_SMAN_BACK for BACK user SMB_*** in case of usage of CCTS, see section on *Technical Users* for ChaRM and QGM in this guide. • adapted all managed system roles SAP_CM_MANAGED_* • new role SAP_CM_SMAN_BACK for new *Back User for cCTS*, see section on Technical Users and Communication Channels and Destinations in this guide. **Configuration Validation** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • authorization objects AI_CCDB_*** are obsolete as of SP05. The according section has been removed from this guide. • adapted role SAP_CV_DIS for report application Configuration Validation Reporting • adapted role SAP_SMWORK_DIAG for the new tile

Support Package Stacks (Version)	Description
	• substituted SAP_SMWORK_CHANGE_MAN with role SAP_SMWORK_DIAG for template users CV_ADM*** and CV_DIS_*** **Change Request Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • TMW User SMT* requires BC-Set authorization for function *Retrofit* • adapted role SAP_CM_MANAGED_ADMIN • adapted roles SAP_CM_SMAN_CHANGE_MANAGER, SAP_CM_SMAN_ADMINISTRATOR, SAP_CM_SMAN_OPERATOR

Support Package Stacks (Version)	Description
SP05	**System Recommendation** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • New template users with Default ID: `SYR_<user description>_<system ID>` added in the system, see the extention in this guide for section *System Recommendation.* The users are available in application *Solution Manager User Administration* (SMUA) in work center *SAP Solution Manager Administration* view *Users*. For more information on SMUA, see in the *Secure Configuration Guide* the according section. **Configuration Validation** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • New template users with Default ID: `CV_<user description>_<system ID>` added in the system, see the extention in this guide for section *Configuration Validation.* The users are available in application *Solution Manager User Administration* (SMUA) in work center *SAP Solution Manager Administration* view *Users*. For more information on SMUA, see in the *Secure Configuration Guide* the according section. **Requirement Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted all relevant Requirement Management roles with User Interface authorization object `SM_PPF`. More information on the object, see according section for *Main Authorization Objects*. • adapted role `SAP_RM_SOL_ARCHITECT` • adapted role `SAP_RM_CONFIG` **Quality Gate Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • new section: *Specific Authorization Objects* • new authorization group for QGM tables `SQGM` (referenced in authorization object `S_TABU_DIS`) • all `SAP_SM_QGM*` roles adapted to usage in transaction `SOLMAN_SETUP` (all fields in authorization objects delivered with field values) • adapted roles `SAP_SM_QGM_STATUS_QM` and `SAP_SM_QGM_STATUS_QAB` with OData Service for SAP Fiori App (more on SAP Fiori APP, see Security Guide for SAP Fiori App for Solution Manager) • adapted role `SAP_QGM_CONFIG` due to substitute of BAdI-Implementation transaction `SE18` with transactions `AGS_BADI_IMPL_NEW` (new implementation), `AGS_BADI_IMPL_OVERV` (Overview with full functional approach), and `AGS_BADI_IMPL_CLASSI` (classic implementation) for call in transaction `SOLMAN_SETUP` via GUI HTML • adapted role `SAP_QGM_CONFIG` • added authorization object `S_IWB` to QGM core roles **Incident Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role.

Support Package Stacks (Version)	Description
	• adapted role SAP_SUPPDESK_CONFIG with S_DEVELOP (ENBC for BAdI Implementation) • added role SAP_SETUP_BASIC_ARCHIVE to SMC_CM* user to display archived entries • adapted role SAP_SUPPDESK_CONFIG due to substitute of BAdI-Implementation transaction SE18 with transactions AGS_BADI_IMPL_NEW (new implementation), AGS_BADI_IMPL_OVERV (Overview with full functional approach), and AGS_BADI_IMPL_CLASSI (classic implementation) for call in transaction SOLMAN_SETUP via GUI HTML • adapted role SAP_SUPPDESK_CONFIG with additional CRM authorizations • adapted CRM UIU Framework role SAP_SM_UIU_FRAME with additional link authorizations for C_LL_TGT • adapted role SAP_SUPPDESK_DISPATCH **Change Request Management** All changes of authorization objects for a role are documented in the *Menu* tab of the specific role. • adapted all relevant SAP_SM_CM* roles with User Interface authorization object SM_PPF. More information on the object, see according section for *Main Authorization Objects*. • adapted roles SAP_CM_SMAN_ADMINISTRATOR, SAP_CM_SMAN_OPERATOR, SAP_CM_SMAN_DEVELOPER with new authorization object SM_CM_RFIT to allows access to retrofit function. For more information on the authorization object, see section *Main Authorization Objects*. • added role SAP_SETUP_BASIC_ARCHIVE to SMC_CM* user to display archived entries • added new roles SAP_SM_GEN_TRANSPORT and SAP_SM_CH_TRANSPORT to the SMC_CM* configuration user. For more information on the security - criticality of these roles, see section on *Configuration User* for this scenario. • adapted roles SAP_SOCM*with authorization object values for SM_PPF • adapted roles SAP_CHARM_CONFIG due to substitute of BAdI-Implementation transaction SE18 with transactions AGS_BADI_IMPL_NEW (new implementation), AGS_BADI_IMPL_OVERV (Overview with full functional approach), and AGS_BADI_IMPL_CLASSI (classic implementation) for call in transaction SOLMAN_SETUP via GUI HTML • Complete recheck of all roles for managed systems SAP_CM_MANAGED* • added role SAP_CM_MANAGED_IMPORT to user *Release Manager* • new CTS integration role SAP_BC_CCTS_CHARM_CH_MGR_TMPL for *Release Manager* • adapted CRM UIU Framework role SAP_SM_UIU_FRAME with additional link authorizations for C_LL_TGT

Support Package Stacks (Version)	Description
SP04	**Change Request Management** Changes in roles are documented on the Menu tab of the respective role • Adapted all roles SAP_SOCM* • Adapted all roles SAP_CM_MANAGED_* (note: SAP_CM_MANAGED_OPERATOR includes values requires EPS1, IMPA, IMPS and PROJ in authorization object S_CTS_ADMI which is specific for Quality Gate Management) • Added role SAP_SM_ITPPM_DIS to all ChaRM template users for Solution Manager • Adapted role SAP_CHARM_CONFIG **Incident Management** Changes in roles are documented on the Menu tab of the respective role • Adapted composite role SAP_SUPPDESK_CONF_COMP (added role SAP_SM_KW_ALL and substituted role SAP_SM_SL_DISPLAY with SAP_SM_SL_ADMIN) • Adapted role SAP_SUPPDESK_CONFIG **Quality Gate Management** Changes in roles are documented on the Menu tab of the respective role • Adapted role SAP_QGM_CONFIG • Adapted all roles SAP_CM_MANAGED_* (note: SAP_CM_MANAGED_OPERATOR includes values requires EPS1, IMPA, IMPS and PROJ in authorization object S_CTS_ADMI which is specific for Quality Gate Management) • Added roles SAP_SETUP_BASIC_DISP, SAP_SETUP_BASIC_ARCHIVE, SAP_CM_QGM_MANAGED_SETUP, and SAP_SETUP_INFRA_DIS to Configuration User SMC_QGM*** • Adapted roles SAP_SM_QGM_STATUS_QM, SAP_SM_QGM_STATUS_QAB , SAP_CM_QGM_SETUP

Support Package Stacks (Version)	Description
SP03	**Quality Gate Management** • Adapted section QGM, due to configuration of QGM in transaction SOLMAN_SETUP. • Following authorization objects are obsolete and substituted in all relevant roles • /TMWFLOW/D • /TMWFLOW/O • /TMWFLOW/P • /TMWFLOW/R • /TMWFLOW/S Substitute authorization object: SM_CM_TASK. It allows differentiation from which User Interface the task can be triggered. • Template users and roles for Guided Procedure *QGM* in transaction SOLMAN_SETUP • Additional role SAP_CM_QGM_MANAGED_SETUP for Managed System Setup procedure for *QGM* and *Change Request Management* • Adapted all roles SAP_SM_QGM* **Change Request Management** • Following authorization objects are obsolete and substituted in all relevant roles • /TMWFLOW/D • /TMWFLOW/O • /TMWFLOW/P • /TMWFLOW/R • /TMWFLOW/S Substitute authorization object: SM_CM_TASK. It allows differentiation from which User Interface the task can be triggered. • Adapted all roles SAP_SOCM* • Adapted all roles SAP_CM_SMAN * • Removed transaction codes: /TMWFLOW/REPORTINGN; /TMWFLOW/REPORTING; /TMWFLOW/LOCKMON; /TMWFLOW/MAINT; /TMWFLOW/MAINTENANCE; /TMWFLOW/CMSCONF • Deactivated in all relevant roles authorization object PLOG (organization level for HR) • Adapted role SAP_CHARM_CONFIG • Added roles SAP_ITCALENDER and SAP_SETUP_BASIC_ARCHIVE to user SMC_CH (Configuration User) • Additional role SAP_CM_QGM_MANAGED_SETUP for Managed System Setup procedure for *QGM* and *Change Request Management* **Requirement Management** Changes in roles are documented on the Menu tab of the respective role • Adapted role SAP_RM_CONFIG • Deactivated in all relevant roles authorization object PLOG (organization level for HR) **Incident Management**

Support Package Stacks (Version)	Description
	Changes in roles are documented on the Menu tab of the respective role • Adapted roles SAP_SUPPDESK* **CTS Plug Managed System** • New role SAP_CM_MANAGED_CTS_ADOP (Administrator and Operator) • New role SAP_CM_MANAGED_CTS_DEV (Developer)
SP02	**Change Request Management** • adapted all composite roles (from SP01) • adapted SAP_SOCM_REQUESTER • adapted roles SAP_CM_SMAN_* (authorization object SM_CM_TASK) **Quality Gate Management** • adapted roles SAP_*QGM* (authorization object SM_CM_TASK) **Requirements Management** • adapted roles SAP_RM_ITREQ_ADMIN and SAP_RM_SOL_ARCHITECT **Incident Management** • adapted all composite roles (from SP01) • adapted SAP_BI_E2E (due to data activation in ITSM) **Release Management** • adapted roles SAP_SM_CRM_UIU_RM_DISPLAY, SAP_RM_BUSINESS_MANAGER, SAP_RM_ITREQ_ADMIN, SAP_ITREQ_MANAGER, SAP_RM_SOL_ARCHITECT **Note** see SAP Note 2250709

Support Package Stacks (Version)	Description
SP01	**General** Transaction `CRM_DNO_SERVICE_MONITOR` and associated authorization objects are not supported anymore with Release 7.2. For more information, see CRM application guides. **Adaptations for Incident Management** • Roles `SAP_SM_BI_BILO`, `SAP_DNOTIFWL_DIS`, and `SAP_SMWORK_BASIC_INC_MAN` obsolete. • Added new roles for Process Documentation integration `SAP_SM_SL*` and Systems `SAP_SYSTEM_REPOSITORY_*` to users • All roles for *Incident Management* have been adapted to the new functionality of *Process Documentation* and `SAP_BASIS 7.40`. • Authorization object `SM_WC_VIEW` from role `SAP_SMWORK_BASIC_INC_MAN` has been transferred into roles: `SAP_SUPPDESK_*`. • Roles for *Service Provider* `SAP_SUPPDESK_SP*` and `SAP_SUPPCF_*` are not supported anymore. The authorization object `SM_SP` is added to roles `SAP_SUPPDESK_*`, see section *Authorization Objects*. • Added new Transaction Types, see section *CRM Customizing*. **Adaptations for Change Request Management** • Roles `SAP_SOCM_PRODUCTION_MANAGER`, `SAP_SM_BI_BILO`, and `SAP_SMWORK_BASIC_CHANGE_MAN` obsolete. • Roles `SAP_SOLAR01_DIS` and `SAP_SOL_PROJ_ADMIN_ALL` are removed from user composite roles. • All roles for *Change Request Management* have been adapted to the new functionality of *Process Documentation* and `SAP_BASIS 7.40`. • 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_*`. • New authorization objects due to new Process Documentation: `SM_CM_FUNC` and `SM_CM_DGPN.` • Roles for cPro are removed from composite roles, as cPro is no longer supported in Change Request Management • Introduction of new user definition *Release Manager* in Change Request Management process, see section on users. • Adapted authorization object `S_RFC` in all relevant roles for use of Function Modules • Obsolete application *Schedule Manager* removed from role `SAP_SMWORK_CHANGE_MAN` • All users allowed to call cProject Navigation (Role `SAP_BPR_BPM`) • Obsolete Transaction Types `SMMM, SMMN, SMDV` removed in according authorization objects • New Transaction Types `SMAI, SMIM, SMRE` added in according authorization objects **New Functions and Users** • New users and roles for *Release Management*, see section in *Change Management* • New users and roles for *Requirement Management*, see section in *Change Management* • Additional roles `SAP_SM_TREX_ADMIN` and `SAP_SM_ESH_ADMIN` for TREX and Embedded Search administration assigned to all `SMC*` (configuration) users

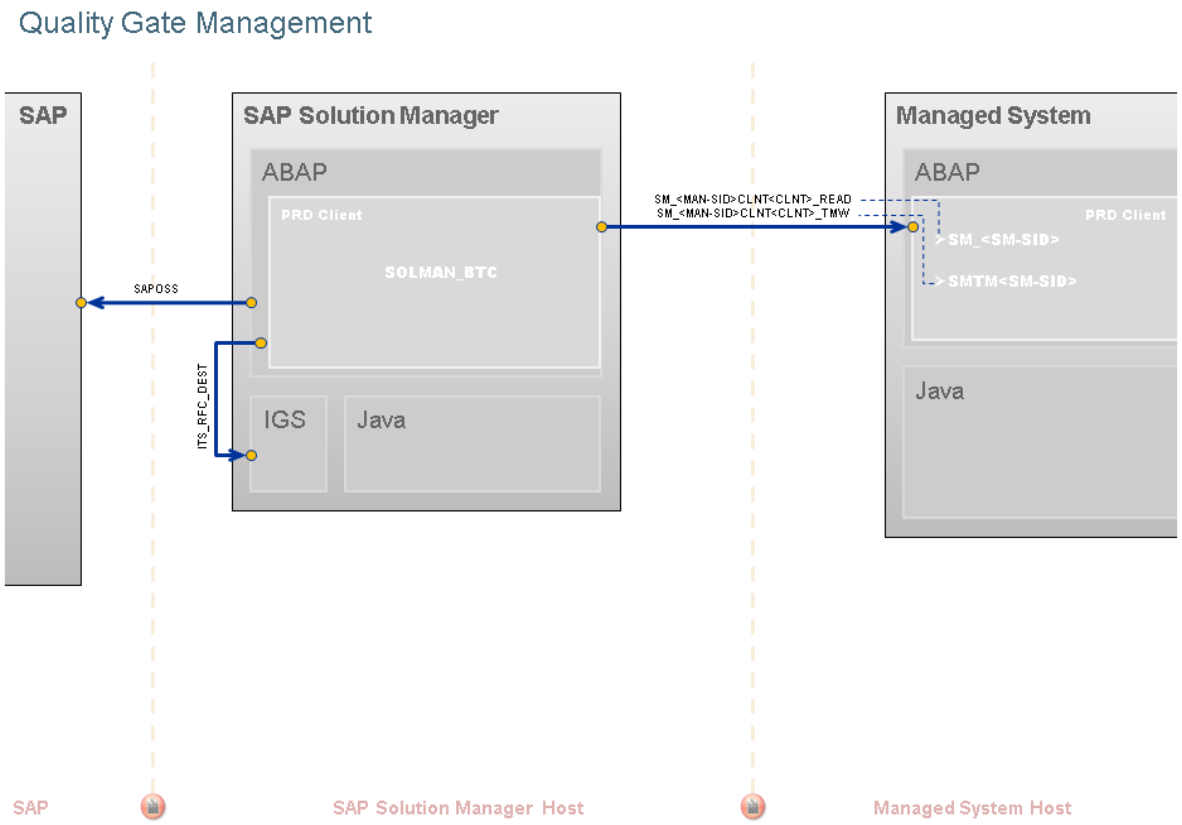
Support Package Stacks (Version)	Description
	Adaptations for Quality Gate Management • Roles SAP_SM_BI_BILO, and SAP_SMWORK_BASIC_CHANGE_MAN obsolete. • Roles SAP_SOLAR* and SAP_SOL_PROJ_ADMIN_ALL are removed from user roles. • All roles for *Quality Gate Management* have been adapted to the new functionality of *Process Documentation* and SAP_BASIS 7.40. • Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_CHANGE_MAN has been transferred into roles: SAP_*QGM*. • New authorization objects due to new Process Documentation: SM_CM_FUNC and SM_CM_DGPN. **SAP Fiori Launchpad Integration** • All users receive SAP Fiori Launchpad authorization role SAP_SM_FIORI_LP_EMBEDDED.

6.3 Scenario-Specific Guide: Quality Gate Management

6.3.1 Prerequisites

6.3.1.1 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.



Infrastructure

6.3.1.2 Scenario Configuration User

> ⓘ 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>) forQGM (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:

Single Role	Help Text ID
SAP_QGM_CONFIG	AUTH_SAP_QGM_CONFIG
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_BASIC
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_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBEDDED
SAP_SM_ESH_DISP	AUTH_SAP_SM_ESH_DISP
SAP_CM_QGM_MANAGED_SETUP	AUTH_SAP_QGM_CONFIG
SAP_SETUP_BASIC_DISP	AUTH_SAP_SETUP_BASIC
SAP_SETUP_INFRA_DISP	AUTH_SAP_SETUP_INFRASTR
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC
SAP_SM_GEN_TRANSPORT	AUTH_SAP_SM_GEN_TRANSPORT

If you want to create the configuration user manually, you need to assign all single roles as mentioned in the table above.

- > **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:

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_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Specific Authorization Objects

S_TABU_DIS and S_TABU_NAM

In role SAP_CM_QGM_MANAGED_SETUP both authorization objects are set active. If your security policy requires to restrict directly to tables, you can set authorization object S_TABU_DIS inactive.

SM_SETUP with ACTVT 03 for other guided procedures

The role SAP_QGM_CONFIG contains authorization object SM_SETUP. The object has various maintenances in the role. It allows acccess to other guided procedures than QGM; for instance Change Request Management. The access allows display only to these steps in other guided pocedures.

> ⚠ Caution
>
> If you allow change authorization ACTVT 02 in authorization object SM_SETUP for another guided procedure step, the system opens a pop-up and asks you for full assignment of roles for this guided procedure.We recommend to ignore or set the user profile parameter to suppress the pop-up.

6.3.1.3 Communication Channels and Technical Users

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

> ⓘ Note
>
> All mentioned RFC - destinations are automatically created via transaction SOLMAN_SETUP, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to SAP Backend system	HTTPS	Technical Communication User	Search for SAP Notes
Managed systems to Solution Manager (Back) SM_<SID>CLNT<Client>_BACK	RFC	SMB_<SID of Solution Manager>	**Using CCTS** If you are using CCTS, you require an additional authorization role for the Back User SMB_*** in the SAP Solution Manager system. For this use, role SAP_CM_SMAN_BACK is shipped. The role is shipped with all authorization objects inactive, as these objects are security-critical. We recommend you to closely inspect and maintain the authorization objects in this role: • S_SYS_RWBO • S_CTS_SADM • S_TRANSPRT • S_DATASET **Locally creating transport requests with implicit change document assignment** For more information on additional authorization assignments to this user, check KBA 2745405.
Solution Manager to managed systems (Trusted) SM_<SID>CLNT<Client>_TRUSTED	RFC	Named End-user (customer specific)	Check section *User Descriptions and User Roles in the Managed Systems* in this guide.
Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) ITS_RFC_DEST	Activation Type Registered Server program (program: IGS.<SID>)		Graphics inclusion **⚠ Restriction** Manually created in transaction SM59
TMS Deploy Destination TMSDPL@SID:DOMAIN			CCTS Integration

6.3.2 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

Transaction Type	Usage	Remarks
`SMQC`	Quality Gate Management	supported

6.3.3 Users and Authorizations

6.3.3.1 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 Quality Gate Management.

IT Operator (Help Text ID: TP_QGM_ITO)

Single Roles	Help Text ID
`SAP_SM_QGM_TRANSPORT`	`AUTH_SAP_SM_QGM_TRANSPORT`
`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_CM_TRANSPORT`
`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_SM_BP_DISPLAY`	`AUTH_SAP_SM_BP_DISPLAY`

Development Lead (Help Text ID: TP_QGM_DL)

Single Roles	Help Text ID
SAP_SM_QGM_CHANGE	AUTH_SAP_SM_QGM_CHANGE
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
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_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_QGM_CM_CHANGE	AUTH_SAP_SM_QGM_CM_CHANGE

Quality Manager (Help Text ID: TP_QGM_QM)

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_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY

Quality Advisory Board Member (Help Text ID: TP_QGM_QAB)

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_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_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_QGM_CM_QAB	AUTH_SAP_SM_QGM_CM_ALL

QGM Project Administrator (Help Text ID: TP_QGM_PM)

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_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_SMDOC`.

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_*`.

6.3.3.2 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`)

> **Note**
>
> All users need authorization object `S_RFCACL` additionally assigned to be able to use the trusted - connection between systems.

6.3.3.3 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`.

6.3.4 Specific Authorization Objects

Here, you find specific authorization objects which are relevant in QGM.

Authorization Object S_TABU_DIS

Authorization object `S_TABU_DIS` restricts tables on the basis of a common authorization group. This is relevant for all tables that can be called by the following transactions: `SM31, SM30, SE16`.

QGM uses the authorization group `SQGM`.

Authorization Object SM_CM_AUTH

Using authorization object `SM_CM_AUTH`, you can restrict, which applications within QGM an end-uder is allowed to use or not.

Authorization Object S_IWB

To view and display all documents related to QGM as created within Release 7.1, the object `S_IWB` is required. As soon as you have migrated any documents into Release 7.2, you can use the new Document Management authorization objects.

Authorization Object SM_CM_DGPN

Authorization object `SM_CM_DGPN` is used to control functions SCOL and Downgrade Protection (DGP). Only the Adminnistrator, IT Operator, Change Manager, and Developers are allowed perform actions in regard to these functionalities.

Authorization Object S_DEVELOP

Authorization object `S_DEVELOP` is required for BAdI Implementations in the managed system as well as in the Solution Manager system. In addition, it is required to allow SCOL Lock mechanism. If you do not require both functionalities, we advice to remove `S_DEVELOP` for both functions from role `SAP_QGM_CONFIG`.

6.4 Scenario-Specific Guide: IT Service 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 *ITSM 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 destination for the SAP Backend is 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.

6.4.1.2 Scenario Configuration User

> **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_<XXXClient>`) 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.

- 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.

- 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*.

6.4.1.3 Communication Channels and Technical Users

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

Mandatory Connections and Users

> **Note**
>
> All mentioned RFC - destinations are automatically created via transaction SOLMAN_SETUP, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to SAP Backend system	HTTPS	Technical Communication User	Search for SAP Notes
Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			ITSM Reporting and ITSM Dashboard
Solution Manager to managed systems (Read) SM_<SID>CLNT<Client>	RFC	SM_<SID of Solution Manager>	Used during setup of incident management, and during operations when generating business partners
Managed systems to Solution Manager (Back) SM_<SID>CLNT<Client>_BACK	RFC	SMB_<SID of Solution Manager>	Generating Support Messages from managed systems (table: BCOS_CUST)
Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) ITS_RFC_DEST	Activation Type Registered Server program (program: IGS.<SID>)		Graphics inclusion **Restriction** Manually created in transaction SM59
Third Party Service Desk	SOAP over HTTP(S)	DEFECTMAN	Data Exchange **Note** User for web service; assigned roles SAP_SUPPDESK_ADMIN and SAP_SUPPDESK_INTERFACE

TREX RFC Connections

RFC Destination Name	Activation Type	How Created
TREX_<server> (ABAP connection)	Registered Server Program (program TREXRfcServer_<instance number>)	Manually in transaction SM59 TREX can be administered using the TREX admin tool, see IMG activity *Information and Configuration Prerequisites for TREX Setup* (technical name: SOLMAN_TREX_INFO)
IMSDEFAULT	Start on explicit host (program: ims_server_admin.exe)	
IMSDEFAULT_REG	Registered Server Program (program: rfc_sapretrieval)	

Technical User SM_ITSM

The technical user SM_ITSM is used to run background jobs which are only relevant for *Incident Management* scenario. It is assigned role SAP_SM_ITSM (Help Text-ID: AUTH_SAP_SM_ITSM). You can create this user automatically using transaction SOLMAN_SETUP.

> → Remember
>
> If you have activated the *Territory Check*, you need to add authorization object CRM_ORD_TE to the role SAP_SM_ITSM manually. It can be only used in sales and service order basic (CRM) transaction types. For more information, see Territory Determination in the Business Transaction.

6.4.1.4 SAP Support Portal Contact in SAP Solution Manager (Table: AISUSER)

Users who communicate with the SAP Support Portal via the RFC destination 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 https://help.sap.com/viewer/p/SAP_Solution_Manager.

6.4.1.5 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

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

6.4.2 CRM Standard Customizing for Solution Manager

The Incident 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 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)

> ⚠ Restriction
>
> The following transaction types are no longer supported.

Transaction Type	Usage	Remarks
SLFN	Standard Service Desk	not supported
SIST	Standard Service Desk	not supported
SIVA	Service Request for Service Provider (VAR)	not supported
SISV	Service Request for Software Partners (ISV)	not supported

Transaction Types (new)

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
SMDT	Incident for Damaged Test Cases	supported

6.4.3 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.*

> ⚠ Caution
>
> As of SP21, the link to the application *Monitoring Requirement* is set to invisible in the standard application. To set it to **`visible`**, follow the customizing for the *business role* `SOLMANPRO` in transaction `SPRO`.

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 all single roles for user Requester `TP_CM_REQ` (Change Request Management). For more information about the Change Request Management scenario, see the according *Scenario-Specific Guide*.

6.4.4 Users and Authorizations

6.4.4.1 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.

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 additional 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)

Single Roles	Help Text ID
SAP_SUPPDESK_ADMIN	AUTH_SAP_SUPPDESK_ADMIN
SAP_SMWORK_INCIDENT_MAN	AUTH_SAP_SMWORK_INCIDENT_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME

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

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

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
SAP_SM_BI_DSH_CONF	AUTH_SAP_SM_BI_DSH_CONF

Processor (Help Text ID: TP_IM_PROC)

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

Single Roles	Help Text ID
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

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

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
SAP_SM_BI_DSH_DISP	AUTH_SAP_SM_BI_DSH_DISP
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR

Key User (Help Text ID: USER_TP_IM_CREATE)

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

> **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)

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
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

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

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
SAP_SM_BI_DSH_DISP	AUTH_SAP_SM_BI_DSH_DISP
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTACTOR

Dispatcher User (Help Text ID: TP_IM_DSPTCH)

Single Roles	Help Text ID
SAP_SUPPDESK_DISPATCH	AUTH_SAP_SUPPDESK_DISPATCH

Single Roles	Help Text ID
SAP_SMWORK_INCIDENT_MAN	AUTH_SAP_SMWORK_INCIDENT_MAN
SAP_SM_CRM_UIU_FRAMEWORK	AUTH_SAP_SM_CRM_UIU_FRAME
SAP_SM_CRM_UIU_SOLMANDSPTCH	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
SAP_SM_BI_INCMAN_REPORTING	AUTH_SAP_SM_BI_INCMAN_REP

6.4.4.2 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_*.

> **Note**
>
> To be able to use this function, you need to maintain an organizational model.

Authorization Object: S_DEVELOP

Configuration user SMC* is assigned S_DEVELOP with value ENBC to allow for BAdI Implementation.

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.

6.4.5 External Integration

6.4.5.1 External Service Desk

Roles

Service Desk Interface

Name	Type	Remarks
SAP_SUPPDESK_INTERFACE 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 SAP_SUPPDESK_ADMIN
		User for data exchange; assigned roles SAP_SUPPDESK_ADMIN and SAP_SUPPDESK_INTERFACE

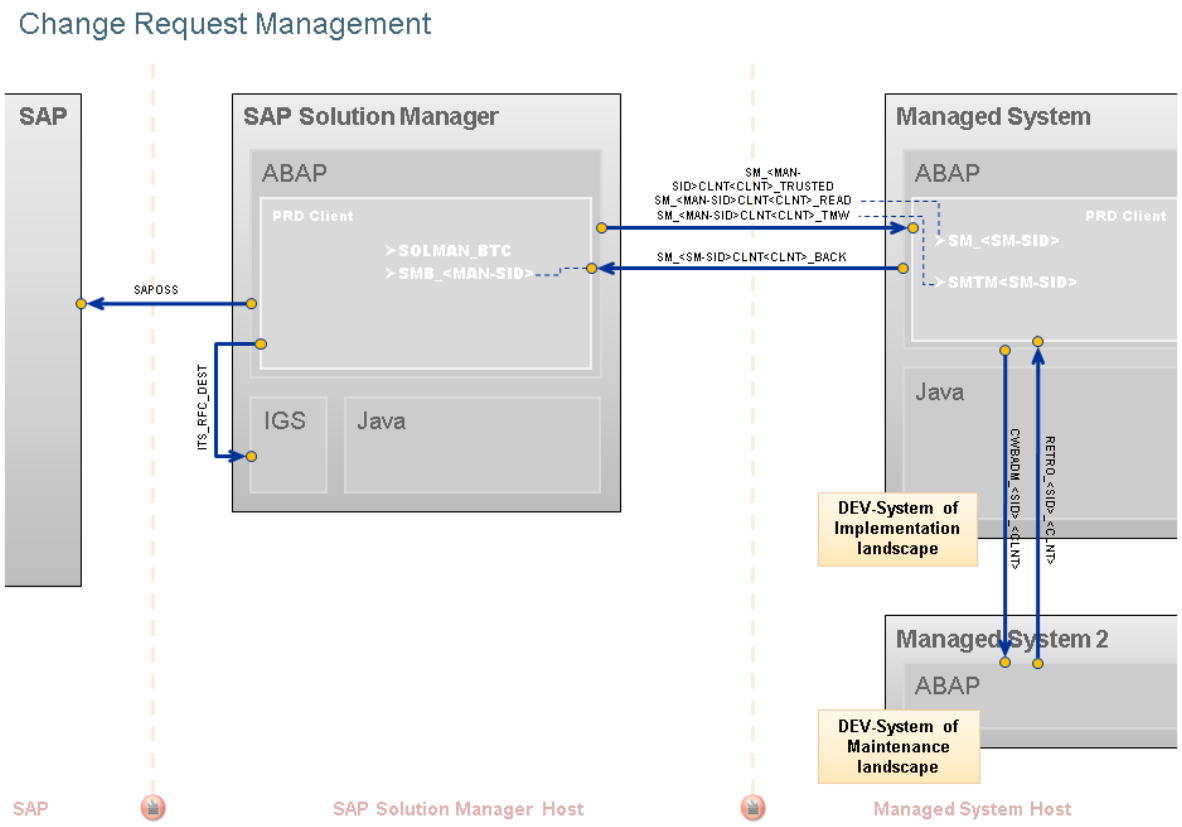
6.5 Scenario-Specific Guide: Change Management

6.5.1 Prerequisites

6.5.1.1 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.



Infrastructure

6.5.1.2 Scenario Configuration User

> ⓘ 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_<XXXClient>) 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.

- 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.

- 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.

Transaction Authorization Object S_TCODE for Transaction SPRO

In case you require to configure individual activities contained in the *Implementation Guide (IMG)* for the scenario, you need to assign transaction authorization object S_TCODE for SPRO to your user. Note, that this is only the access authorization for the Implementation Guide. Any additional authorizations that may be required for individual activities need to be assigned additionally to the current roles.

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:

Single Role	Help Text ID
SAP_CM_QGM_MANAGED_SETUP	AUTH_SAP_CM_QGM_MANAGED_SETUP
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*.

Critical Authorizations

Critical Roles Assignment

The configuration user is assigned a role SAP_SM_GEN_TRANSPORT. This role includes all relevant transport authorization objects which are required for the general Change Request Management configuration. In addition, the user is assigned role SAP_SM_CH_TRANSPORT in case *Downgrade Protection (DGP)* is also configured with this user. DGP requires additional authorization object S_CTS_ADMI with value TADM (execute tp commands). The authorization combination of both roles is highly security - critical.

> → Recommendation
>
> We recommend to disable role SAP_SM_CH_TRANSPORT as soon as you have finished the configuration or update configuration of DGP.

Authorization Object S_TCODE

In case you require to configure individual activities contained in the *Implementation Guide (IMG)* for the scenario, you need to assign transaction authorization object S_TCODE for SPRO to your user. Note, that this is only the access authorization for the Implementation Guide. Any additional authorizations that may be required for individual activities need to be assigned additionally to the current roles.

Authorization Object S_DEVELOP

This authorization object is contain in various maintenance profiles in role SAP_CHARM_CONFIG. Check the *Description Tab* of the role for details, in case your security departments needs additional information for assigning the authorization.

In Solution Manager Setup

Within the configuration of ChaRM in the Solution Manager, the object is required for CSOL and DGP setup implementation CSOL BAdI. It allows to define custom methods for plugging into the processing logic of CSOL, and thus customize its behavior.

In Managed System Setup

Within the configuration of ChaRM in the managed system setup, the object is required for the function *Retrofit* to activate BAdIs within the Managed System. This Business Add-In BADI CTS_EXPORT_FEEDBACK allow to activate the BAdI implementation RETRO_STANDALONE. It ensures that in the managed system during the release of transport requests, the transport requests are registered in Change Request Management.

6.5.1.3 Communication Channels and Relevant Users

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

> **Note**
>
> All mentioned RFC - destinations are automatically created via transaction SOLMAN_SETUP, see *Secure Configuration Guide*.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to SAP Backend system	HTTPS	Technical Communication User	Search for SAP Notes
Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			Dashboard functionality and ChaRM reporting.
Solution Manager to managed systems (Read) SM_<SID>CLNT<Client>	RFC	SM_<SID of Solution Manager>	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.

Communication Channel	Protocol	User	Type of Data Transferred / Function
Solution Manager to managed systems (TMW) `SM_<SID>CLNT<Client>`	`RFC`	`SMTW_<SID of Solution Manager>`	**Change Request Management** Required: • when *Transport Management* is in place; allows for creating and releasing of transport requests via remote pattern. • **Project Status Switches** **Note** Check SAP Note 807228 for additional authorizations in case of control of project status switches and request releases for Change Managers. • **Retrofit** For additional information on the RFC connection for Retrofit, see the according section on *User Roles for Retrofit* in the guide. • **cCTS Integration** • Retrofit for S/4 HANA checks • ATC checks
Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	`RFC`	Named End-user (customer specific)	The `RFC` is used for the following functions: • Retrofit • Git-enabled CTS • ATC checks fallback, if TMW RFC does not exist . Within the *Task List Framework* the login prompt is avoided.
Solution Manager to managed systems (Login) - connection is mandatory for all tasks that involve system changes due to transports - `connection isSM_<SID>CLNT<Client>_LOGIN`	`RFC`	Named End-user (customer specific)	Workaround to using Trusted RFC

Communication Channel	Protocol	User	Type of Data Transferred / Function
Managed systems to Solution Manager (Back) `SM_<SID>CLNT<Client>_BACK`	RFC	`SMB_<SID of Solution Manager>`	1. To display check results with the change document information including ID, description and URL when saving transport-related checks and for F4 help search results to assign change documents. This use case requires you to manually add the following authorization objects to the user role for the `SMB*` user: • `SM_CM_FUNC` • `SM_SDOC` • `CRM_TXT_ID` • `S_RFC` with function module `/TMWFLOW/CREATE_FROM_FEEDBACK` For more information, see KBA 2745405. **⚠ Restriction** This is only relevant for this specific use case and not required in productive systems. 2. Help Center Function
Solution Manager to managed systems within customer network	FTP		Update route permission table, content: `IP` addresses, see section *File Transfer Protocol (FTP)*
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		Graphics inclusion **⚠ Restriction** Manually created in transaction `SM59`
`SM_<SID>CLNT<Client>_BACK_CSOL` (ABAP connection)	RFC	Technical User of type *Service*	Manually created in transaction `SOLMAN_SETUP` (assigned role `<namespace>SAP_SOLMANTMWCOL`) For function *Cross System Object Lock* `CSOL` **ⓘ Note** SAP Solution Manager manages the lock information.
Back RFC for cCTS	RFC	Technical User of type System	**cCTS** Manually created Back RFC User for a *cCTS Back RFC*. It is required in case, that ChaRM/QGM are used and Transport Requests are created locally in the development system, and not from within the Solution Manager system (assigned role `SAP_CM_SMAN_BACK`) For more information, see underneath.

Communication Channel	Protocol	User	Type of Data Transferred / Function
RETRO_<SID>_<CLNT>	RFC	Technical User of type System	**Retrofit** ⚠ Caution This is a trusted RFC - connection used for transport of copies. Used in managed systems, development system (Implementation landscape)
CWBADM_<SID>_<CLNT>	RFC	Technical User of type System	**Retrofit** ⚠ Caution This is a trusted RFC - connection used for comparison and merge of coding according to ToDo list in *Correction Workbench* Used in managed systems, development system (Implementation landscape)
TMS CI RFC	RFC	Technical User of type System	**TMS CI** ⚠ Caution This is a trusted RFC - connection used for TMS CI. For more information, see SAP Note 1384598.

cCTS Back Destination User Role

If you are using cCTS, you require an additional authorization role for the Back User SMB_*** in the SAP Solution Manager system. For this use, role SAP_CM_SMAN_BACK is shipped.

Usage

The role is used for developers, who need to assign change documents to create transport requests in a managed development system. Inm detail, a Transport Request is created locally in development system by an end user such as developer. The request information is sent then to the Solution Manager system containing the following information:

- the transport request is assigned to Change Request Management / Quality Gate Management tables
- in case of cCTS, the new transport request is also assigned to respective cCTS collection.

Maintenance of Role

The role is shipped with all authorization objects inactive, as these objects are security-critical. We recommend you to closely inspect and maintain the authorization objects in this role:

- S_SYS_RWBO

- S_CTS_SADM
- S_TRANSPRT
- S_DATASET

Assignment to Technical User SMB_***

Assign the role to the Technical User SMB_*** user manually. This user has already authorization assigned in role SAP_SOLMAN_BACK.

Application Log Information

Authorization object S_APPL_LOG for application log transaction SLG1 is required with the following values:

- Object: /TMWFLOW/CMSCV
- Sub-object: CHNG_ASSI_TR_CREATE

6.5.1.4 Technical User for Background Jobs SM_CHM

Help Text-ID: USER_SM_CHM

This technical user is specific for *Change Request Management*. The user is assigned role SAP_SM_CHM.

The following jobs are scheduled by this user:

- SM:TMWFLOW_CMSSYSCOL (Help Text: CHM_SM_TMWFLOW_CMSSYSCOL)
- SM:AI_CRM_CM_COM_IMPORT_FEEDBACK (Help Text: CHM_SM_IMPORT_FEEDBACK)
  The *active import feedback* feature is an enhancement which transfers import information from managed systems to the SAP Solution Manager. To achieve immediate import reporting, the managed system actively informs the SAP Solution Manager about finished imports via the BACK-RFC. This triggers a new collector job to be started in the SAP Solution Manager, which might also act upon the newly collected import information, like sending emails or changing the change document status.
- SM:AI_CRM_CM_COM_WLO_CRO_MAIL_NO (Help Text: CHM_SM_WLO_CRO_MAIL_NO)

> ⓘ Note
>
> For more information, see also SAP Note 894279.

6.5.2 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

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
SMGH	Git-enabled CTS

6.5.3 Users and Authorizations

6.5.3.1 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.

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_RFACL (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 in the SAP Solution Manager System

Role	Help Text-ID
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_REQUESTER	AUTH_SAP_SOCM_REQ
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
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

Change Manager (Help Text-ID: TP_CH_CM)

Single Roles for Change Manager in the SAP Solution Manager System

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

Role	Help Text-ID
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
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS
SAP_CPR_USER	AUTH_SAP_CPR_USER

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

Single Roles	Help Text ID
SAP_BI_E2E_CHARM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP
SAP_BW_SPR_REPORTING	AUTH_SAP_BW_SPR_REPORT
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR
SAP_SM_BI_DSH_DISP	AUTH_SAP_SM_BI_DSH_DISP

Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Assigned Role	Help Text-ID
SAP_CM_MANAGED_CHANGEMAN	AUTH_SAP_CM_MANAGED_CHANGE
SAP_CM_MANAGED_IMPORT	AUTH_SAP_CM_MANAGED_IMPORT

Developer (Help Text-ID: TP_CM_DEV)

> **Note**
>
> For import authorizations, see SAP Note 807228.

Single Roles for Developer in the SAP Solution Manager System

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
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

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

Authorization Object S_TABU_NAM

In role SAP_CM_MANAGED_DEVELOPER_RETRO authorization object S_TABU_NAM is shipped in an inactive status. To be able to use retrofit in managed systems, you need to activate the object and add all relevant table entries you require. You can also use object S_TABU_DIS using the according authorization groups.

Tester (Help Text-ID: USER_TP_CH_TESTER)

> **Note**
>
> For import authorizations, see SAP Note 807228.

Single Roles for Tester in the SAP Solution Manager System

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
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Assigned Role	Help Text-ID
SAP_CM_MANAGED_TESTER	AUTH_SAP_CM_MANAGED_TESTER

Assigned Role	Help Text-ID
SAP_CM_MANAGED_IMPORT	AUTH_SAP_CM_MANAGED_IMPORT

IT-Operator (Help Text-ID: TP_CM_OPERATOR)

Single Roles for IT-Operator in the SAP Solution Manager System

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
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
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

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

Single Roles	Help Text ID
SAP_BI_E2E_CHARM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR

Single Roles	Help Text ID
SAP_BW_SPR_REPORTING	AUTH_SAP_BW_SPR_REPORT
SAP_SM_BI_DSH_DISP	AUTH_SAP_SM_BI_DSH_DISP

Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Assigned Role	Help Text-ID
SAP_CM_MANAGED_OPERATOR	AUTH_SAP_CM_MANAGED_OPERATOR
SAP_CM_MANAGED_CTS_ADOP	AUTH_SAP_CM_MANAGED_ADMIN

Administrator (Help Text-ID: TP_CH_ADMIN)

Single Roles for Administrator in the SAP Solution Manager System

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
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_CONF	AUTH_SAP_SM_DSH_CONF
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_SYSTEM_REPOSITORY_EXE	AUTH_SAP_SYSTEM_REP_ALL
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_SM_KW_DIS	AUTH_SAP_SM_KW_DIS
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

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

Single Roles	Help Text ID
SAP_BI_E2E_CHARM	AUTH_SAP_BI_E2E
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN
SAP_BW_SPR_REPORTING	AUTH_SAP_BW_SPR_REPORT
SAP_SM_BI_DSH_CONF	AUTH_SAP_SM_BI_DSH_CONF
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR

Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

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 in the SAP Solution Manager System

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
SAP_SM_ITPPM_DIS	AUTH_SAP_SM_ITPPM_DIS

Role in the Managed System

The role must be assigned to the user with the same user ID in the managed system.

Assigned Role	Help Text-ID
SAP_CM_MANAGED_RELEASEMAN	AUTH_SAP_CM_MANAGED_RELEASE
SAP_CM_MANAGED_IMPORT	AUTH_SAP_CM_MANAGED_IMPORT

6.5.3.2 Best Practice: Manage Import Authorizations in Managed Systems

Use

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.

6.5.3.3 User Roles for Additional Functions

6.5.3.3.1 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*.

Additional Roles for TMW-User SMT*

TMW User SMT* you require BC-Set relevant authorizations. To find out about BC-Set roles that you can assign, check section *User Roles for BC-Set Activities* in chapter *Process Management → User Roles for Additional Functions*.

Best Practice Recommendation

> ⚠ Caution
>
> This recommendation is an example on how to handle roles and authorizations if you implement retrofit as a stand-alone application.

SAP Solution Manager

In the SAP Solution Manager system, you would require two users with at least the following roles. We do however recommend always fully assigning the complete role set as suggested for the template user in the Guided Procedure in transaction SOLMAN_SETUP for this scenario: Developer: SAP_CM_SMAN_DEVELOPER

Managed Systems

In the managed systems, the following roles would be relevant to be assigned:

- SAP_CM_MANAGED_CTS_DEV
- SAP_CM_MANAGED_DEVELOPER
- SAP_CM_MANAGED_DEVELOPER_RETRO
- SAP_CM_MANAGED_IMPORT (see also section *Best Practice Import Authorizations* in this guide)

Specific Security-Critical Authorizations

> ⚠ Caution
>
> The following is a list of authorizations, you may require for Retrofit in certain use cases. Combined with other authorization objects, these authorizations can pose a security risk. We therefore recommend using them with restricted value assignments by first tracing your applications using transaction STAUTHTRACE.
>
> - Calling transaction SCWB requires authoriztion object S_DEVELOP with full authorization in the managed system and display authorization in the SAP Solution Manager system.
>   We recommend to always work with transport of copies. Then the authorization is not required. If you cannot work with this recommendation, then we advise to add authorization object TMWFLOW/Ato your developer user.

- Calling *Object Comparison* may require full authorization for the following authorization objects:
  - `S_RFC`
  - `S_TABU_DIS`
  - `S_USER_AUT` and `S_USER_AGR` with `ACTVT03` (display)

6.5.3.3.2 User Roles for Communication Systems

In the communication systems, you require the same roles as for your managed systems. See section *Users and Authorizations*.

6.5.3.3.3 User Roles for CTS-Integration in SAP Solution Manager

You can use `cCTS` with *Change Request Management*. To be able to use this integration, assign the following roles to your SAP Solution Manager users.

Within cCTS:

- systems with same system role definition, such as development system, QA system, and so on, from different landscapes are configured into one cluster
- transport requests from development systems of different landscapes are linked to the same transport collection
- transport routes are defined between clusters
- due to the import transport collection from the development cluster into target cluster, the related transport requests are imported into the target systems in the target cluster, respectively

> ⚠ Caution
>
> You are required to maintain some of the values in authorization objects `S_SYS_RWBO` and `S_CTS_SADM` due to security-reasons.

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)

Release 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)

6.5.4 E2E Integrations

6.5.4.1 Solution Manager Scenario Integrations

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 additional security measures are applicable.

> **Note**
>
> For more detail on each individual scenario mentioned below, see the according *Application-Scenario—Specific Chapter* in this guide.

Customizing Synchronization

Customizing Synchronization is part of scenario *Process Management*, for more information see the *Application Scenario - Specific Guide for Process Management* as well as SAP Note 1061644.

ITSM Service 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 IT Service Management key user (`USER_TP_IM_CREATE`) roles.

Test Suite

- To allow for smooth Test Automation integration with Change Request Management, you need to assign role `SAP_SM_CM_TEST_INT` to the technical eCatt user `ECATT_ET_USR`.

  > → Remember
  >
  > The role must be adapted for all relevant modified transaction type values. If you have copied SAP transaction types in your own namespace, these values need to be added to the relevant CRM authorization objects in the role.

- In the assignment block *Test Management*, you can create and 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`.

Business Process Change Analyzer

For BPCA integration, you need to add additional BPCA roles, depending on which BPCA functionality, see *Application Scenario-Specific Guide for Business Process Change Analyzer*.

Configuration Validation

See *Application 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 *Application Scenario-Specific Guide for Process Management* section *Project Management*.

6.5.4.2 Integration with Git-enabled CTS

1. In the SAP Solution Manager system, the Change Manager user creates a Git-enabled Change (transaction type `SMGH`).
2. In the SAP Solution Manager system, the developer user creates a transport request from the Git-enabled Change.
3. In the managed system of type development, the developer user executes the development and releases the task. A Transport of Copies (ToC) commit to Git platform is set.
4. In the SAP Solution Manager system, the developer user sets the Git-enabled Change to the status *To Be Tested*. The commit is deployed from Git platform to the QAS system.
5. Once the test is successful, the IT Operator user triggers the deploy of the commit to the production system.

Roles in the SAP Solution Manager System

For the users mentioned above, the delivered template roles are relevant to be used in SAP Solution Manager. The description tab in the individual role lists the affected authorization objects and their added values.

Roles in Managed Systems

The following roles apply for users in the individual managed systems in addition to the delivered template roles for managed systems:

- `SAP_CM_MANAGED_CTS_DEV` - Required for developers.
- `SAP_CM_MANAGED_CTS_OPERATOR` - Required for operators.
- `SAP_CM_MANAGED_CTS_CHANGEM` - Required for change managers.
- `SAP_CM_MANAGED_CTS_TESTER` - Required for testers.
- `SAP_CM_MANAGED_CTS_ADMIN` - Required for administrators.

For more information regarding the roles, refer to SAP Note 3117556.

More Information

For more information, see the Configuration of gCTS help documentation.

6.5.4.3 SAP Cloud Platform (SAP CP) Integration

For a detailed description of the integration and its setup, see the current Online Documentation.

For a general overview on the SAP CP security model, see the specific Security Guideslines for SAP CP integrations.

User Management

1. In the SAP Cloud Platform Cockpit, add a user, such as `CHARM_CONF` as security administrator of the subaccount by assigning to role `User & Role Administrator`.This administrator user requires the role `Administrator` of the subaccount to get the *Service Key* of the *Transport Management Service*.
2. Create a role collection using the role template *Viewer* for the *Transport Management* application identifier. In the Transport Management service application, the administrator user needs at least the role *Viewer* to read the Landscape data.
3. Assign the role collection to your user `CHARM_CONF` in the *SAP ID service*.

For more information on the security measures for the Transport Management service, see the Online Documentation Guide.

RFC Connection in SAP Solution Manager backend system

The Service Key and the Landscape are mandatory information to create a dedicated RFC connections in the backend SAP Solution Manager system. They are used to communicate with the SAP Cloud Platform Transport Management service.

In the Back-end system authorizations are required as described in this guide. In addition, you require to assign dedicated authorizations for the relevant RFC connection, which is used by the SAP Solution Manager system to communicate with the SAP Cloud Platform Transport Management service.

1. Create the RFC Connection in transaction `SM59`.
2. In the *Security Options* of the RFC connection, assign value `SM_C_TMS` to the field *Authorization for Destination*.
3. Assign authorization object `S_ICF` to any user who connects via the RFC to the SAP Cloud Platform service, such as *Administrator, Developer, IT Operator, Tester*.
4. Maintain the authorization object as follows:
   - Field `ICF_FIELD: DEST`
   - Field `ICF_VALUE: SM_C_TMS`

Monitoring and Error Handling

Error logs in the back-end system apply as described in this guide. For detailed information on logs for data privacy measures, see the *Security Optimization Guide for SAP Solution Manager*. For error logs and monitoring in the SAP CP, see the according guide.

6.5.5 Using System Recommendations Application

Use the *System Recommendations* app in SAP Solution Manager to show relevant security notes (Hot News, Legal Change Notes, or Performance Notes) for an SAP system. This app works especially for ABAP, Java and HANA, as well as other SAP system types that you can connect to SAP Solution Manager. You can use this app

for your business systems like ERP, CRM, BW, Portal, as well as for infrastructure systems like XI, or the SAP Solution Manager itself.

Prerequisites

You have to register the systems at the System Landscape Directory (SLD) and define them as technical systems in the SAP Solution Manager. For more information, see the *Secure Configuration Guide*. Then, you can configure the *System Recommentations* app to calculate relevant SAP Notes.

> **Note**
>
> The application cannot judge on manual configurations like profile parameters, settings in *.ini files, allowlists, or other access control entries. Security notes describing such manual activities need to be checked manually. There are additional limitations for the kernel since the kernel contains various individual executables and libraries. These may get individually patched resulting in a mixture of version numbers.

Template End Users

New template users with default ID: `SYR_<user description>_<system ID>` added in the system. These template users are assigned a number of roles relevant for the application.

The users are available in the *Solution Manager User Administration* (SMUA) app in the *Users* view of the *SAP Solution Manager Administration* launchpad group. For more information on SMUA, see the according section in the *Secure Configuration Guide*.

Administrator User SYR_ADM_XXX (Help Text ID: TP_SYR_ADM)

Single role	Help Text ID
SAP_SYSREC_ALL	AUTH_SAP_SYSREC_ALL
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Display User SYR_DIS_XXX (Help Text ID: TP_SYR_DIS)

Single role	Help Text ID
SAP_SYSREC_DIS	AUTH_SAP_SYSREC_DIS
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_CHANGE_MAN	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Main Authorization Objects

S_TABU_DIS: Authorization Group for Tables

All tables relevant for *System Recommendations* are secured by authorization group SMSR.

SM_FUNC: Restricting Tabs

The single tabs for SAP Notes can be restricted by authorization object SM_FUNCS

> ⓘ Note

By default, the tab *SECURITY* is not added to the core roles SAP_SYSREC*, due to the security criticality of the object. You need to explicitely allow this authorization for your end user. We recommend to only allow it for specific security administrators.

6.5.6 Requirements Management

This paragraph gives an overview over users as recommended by SAP and their corresponding user role assignments for *Requirements Management*.

Process Description

1. The business process expert or business manager has 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 implementing the requirement on the specific time, cost, and method.
4. After the commitment from IT department, the business side commits itself to 'purchasing' 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 Web Client UI on SAP Solution Manager to access *Requirements Management*.

Configuration

Transaction SOLMAN_SETUP

You can configure the scenario using SAP Solution Manager (transaction `SOLMAN_SETUP`). When you open the *Requirement Management* procedure view, the system asks you to create a specific configuration user. You can create this`SMC_RM_***` user, or you can add the suggested user roles to another user. See below for specific issues during configuration.

Configuration User SMC_RM_*** (Help TXT: USER_CONFIG_RM)

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_DISP	AUTH_SAP_SETUP_SYSTEM_PREP_DISP

Role	Help Text-ID
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_ADMIN
SAP_SM_TREX_ADMIN	AUTH_SAP_SM_TREX_ADMIN
SAP_SM_ESH_ADMIN	AUTH_SAP_SM_ESH_ADMIN
SAP_SETUP_INFRASTR_DISP	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_DISP	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_APPLOG	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_GEN_TRANSPORT	AUTH_SAP_SM_GEN_TRANSPORT
SAP_RM_CONFIG_ADD	AUTH_SAP_RM_CONFIG
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

> **Note**
>
> To access other scenario configurations than Requirements Management, the configuration user needs authorization objects SM_SETUP for the specific configuration procedure with ACTVT 03 (display). The relevant authorizations are added to the configuration role SAP_RM_CONFIG. If you do not require access to other configuration procedures, you can deactivate the object.

Business Manager: RM_BM_*** (Help TXT: TP_RM_BM)

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
SAP_SM_CRM_UIU_SOLMANREQU_RMBM	AUTH_SAP_SM_CRM_UIU_DELTA

Role	Help Text-ID
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)

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)

Role	Help Text-ID
SAP_RM_BR_ADMIN	AUTH_SAP_RM_BR_ADMIN
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP

Role	Help Text-ID
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
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

IT Requirements Manager: RM_MAN_*** (Help TXT: TP_RM_MAN)

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)

Role	Help Text-ID
SAP_RM_SOL_ARCHITECT	AUTH_SAP_RM_SOL_ARCHITECT

Role	Help Text-ID
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
SAP_BPR_PPM	AUTH_SAP_BPR_PPM

IT Requirements Administrator: RM_ITADM_*** (Help TXT: TP_RM_ITADM)

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

Display User: RM_DISP_*** (Help TXT: TP_RM_DISP)

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

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

BAdI-Implementation

During configuration of Requirement Management, a number of BAdIs are to be implemented. The implementation of BAdIs requires development authorizations, such as authorization object S_DEVELOP. The minimal authorizations that are required are assigned to the role SAP_RM_CONFIG with specific values. If your security guidelines do not permit the configuration user to adapt code, you can set the authorizations for S_DEVELOP containing object types EN* to inactive, remove the according transaction from the menu tab in the role, and assign the authorizations to an according user, such as developer user, who is allowed to implement BAdIs. An additional maintenance might be required of S_DEVELOP with object type SXCI for creating your own custom BAdIs. The authorization is added to the role SAP_RM_CONFIG, but inactive.

Transport Management

During configuration of Requirement Management, you need to be able to transport entries. Transport authorization is assigned to role SAP_SM_GEN_TRANSPORT. If you do not want to allow transport possibilities, you can deassign the role from the configuration user.

Documentation and Translation Transactions

During configuration in transaction SOLMAN_SETUP, you are required to run transactions SE61 and SU63. If you require this, you need to add the according transaction in the menu of the role SAP_RM_CONFIG, and need to adjust referencing authorization objects such as S_TRANSPRT.

Switch Framework Transaction SWF5

During configuration, it is required to run transaction SWF5, the *Business Switch Framework*. To be able to run the Switch Framework, you require authorization object S_SWITCH, which is highly critical.

> → Recommendation
>
> We recommend to assign this transaction and its authorization object S_SWITCH to dedicated users after careful consideration.

TREX and SAP Gateway Administration

During configuration some activities are associated with TREX Administration and SAP Gateway (enabling Gateway Services) configuration. Both, TREX and SAP Gateway, are configured during basic settings configuration of the SAP Solution Manager, which is executed by user SOLMAN_ADMIN. In case you require some additional configuration issues, check the configuration procedures of the basic settings using configuration user SOLMAN_ADMIN.

Scenario Integration

- Change Request Management as follow-up process
- ITPPM for end-user Use Case IDs with transaction type SMIR in authorization object SM_FUNC.
  It allows the IT Requirements Administrator and IT Requirements Manager to assign an ITPPM Project to the IT Requirement.
  - RM_ITADM_***
  - RM_MAN_***

6.5.7 Main Authorization Objects Change Request Management

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_RLT and CRM authorizations are set to inactive in SAP_CM_SMAN* as all BP authorizations are contained in roles SAP_SOCM_*.

In SAP_SOCM_* roles, development environment authorizations are set to 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 the 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 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 an 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 group `SMCP` is required for the integration between ChaRM and PPM tables. This authorization is included in role `SAP_SM_ITPPM_DIS` due to the modularity approach. In any case, you can add the authorization group within the `SAP_SOCM*` roles for any user.

Authorization Object S_TABU_NAM

`S_TABU_NAM` is set to inactive in all roles concerning Change Request Management (ChaRM). If you must restrict access to specific tables, the object can be set to active in the roles. The object is always checked if authorization object `S_TABU_DIS` is not active.

> **Note**
>
> The object is maintained in role `SAP_RM_CONFIG` for the configuration of *Requirement Management* for specific tables.

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` (obsolete, now `SM_CM_DGPN`) 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 SM_CM_RFIT

The authorization object `SM_CM_RFIT` allows you to access the Retrofit function.

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 respective values.

Authorization Object S_DATASET

The authorization object activity field contains `ACTVT 06` (delete). The object allows the deletion of attachments that are added in the *Attachment* assignment block.

Authorization Object SM_PPF

This authorization object restricts, on user interface level, the allowed activities for users in *Requirements Management* and *Change Request Management*. It controls the display of PPF actions on the *Action* button of the WebClient user interface.

Both scenarios are based on CRM transaction usage and base configurations such as user status, PPF actions, date profiles, and so on. They use PPF action implementations to change the user status of the business documents and prerequisite or follow-up business documents via the ChaRM framework. Additionally, PPF actions are used for further functions such as logging on to the development or test system, creating a BPCA analysis, creating a PPM task, and so on. To set a user status, the end user requires the authorization to edit a business document. Additionally, they need the specific authorization value in authorization object `B_USERSTAT` (relevant transaction type, authorization key). On the user interface (UI), the end user can only see those actions which they are allowed to see by authorization object `SM_PPF`. This additional authorization on user interface level, therefore, allows for simplification.

Authorization Object S_SYS_RWBO (S_TRANSPRT)

Authorization object `S_SYS_RWBO (S_TRANSPRT)` is central to scenario *Change Request Management*. Related authorizations are included in the generic role for Transport Management for all Change Management scenarios `SAP_SM_GEN_TRANSPORT`. Make sure, you add the correct values for every user if you do not adopt the SAP standard use case. The object is set to inactive in RM configuration role.

Authorization Object S_CTS_ADMI

Authorization object S_CTS_ADMI in connection with authorization object S_TRANSPRT is highly critical for security. For instance, configuration user SMC_CM* is assigned both objects in relevant transport roles. Make sure that you deassign object S_CTS_ADMI with value TADM from your user when you have finished any configuration activity.

Authorization Object S_SYS_RWBO

This authorization object is critical in combination with objects such as S_TRANSPRT or S_DEVELOP and S_CTS_ADMI (S_CTS_SADM). The object is cointained in a number of managed system roles such as SAP_CM_MANAGED_DEVELOPER (assigned to developer user). In this role, the object contains ACTVT 23 (maintain) for all transport types (TTYPE) for tasks (TASK) and transports (TRAN).

Authorization Object S_DEVELOP

In Combination with BAdI Implementation Transactions AGS*

In the role SAP_CHARM_CONFIG for user SMC_CM*, activities 02 (change) and 03 (display) are required. Activity 02 for change is required if you configure BAdI implementations. Required types include the following:

- SXSD (BAdI Definition) - requires display
- ENHS (Enhancement Spot) - required display
- There is a filter value for each consistency check in the customer namespace (Y*, Z*), for which you can implement the BAdI definition SOCM_CHECK_CONDITION. Apart from calling a consistency check implicitly when a status is saved, you can also use a PPF action to include the action directly in transaction processing as a function of the PPF toolbar with the PPF method HF_CHECK_STATUS.
  BAdI implementation for classic BAdIs (SXCI) and for instance an implementation class (CLAS) - requires change. Authorization object S_DEVELOP with object type SXCI is included in the corresponding configuration roles SAP_***_CONFIG as inactive. You need to activate the authorization object version.
- For a new BAdI with enhancement implementation (ENHO) or composite enhancement implementation (ENHC) and for instance an implementation class (CLAS) - requires change

> → Recommendation
>
> SAP recommends that if you do not require to create BAdI implementations or change them anymore, you can remove the authorization for the above-mentioned types in authorization object S_DEVELOP.

In combination with Retrofit Purposes

The object is optionally required for Retrofit purposes.

In role SAP_SOLMAN_TMW_702 for TMW user SMT<SID>

In Change Request Management, custom code ATC checks can be triggered by the technical TMW user SMT<SID>. This technical user is required to be able to read the custom objects as well. This task is protected by authorization object S_DEVELOP.

> ⓘ Note
>
> For more information about the authorizations needed for the ATC check usage, please refer to SAP Note 3135397.

In role SAP_SOLMAN_TMW_702, the authorization object S_DEVELOP is therefore delivered in an active status with the following field values:

- ACTVT: 03 (display)
- DEVCLASS: /*
  (to allow for custom code)
- OBJNAME: /* (to allow for custom code)
- OBJTYPE: *
- P_GROUP: *

> → Tip
>
> If you are using different name spaces than the ones delivered as standard by SAP, you need to adapt both the DEVCLASS and the OBJNAME fields with your own name space. SAP recommends setting the authorization object to inactive if you are not actively using this function.

In combination with Cloud TMS

Change Request Management (ChaRM) and Quality Gate Management (QGM) provide a dedicated report to remove obsolete Cloud TMS transport request from the import queue of Cloud transport nodes.

Field OBJTYPE Value PROG

Field OBJNAME Value /TMWFLOW/CTMS_ABANDON_TR

Field ACTVT Value 16

Authorization Object S_APPL_LOG

In the *Administration Cockpit*, users can check all transport-related logs in the system with authorization object S_APPL_LOG, which is contained in roles SAP_CM_SMAN_<user>. All subobjects for Change Request Management can be displayed by the relevant user in the SAP Solution Manager system:

- Developer
- IT Operator
- Administrator

The transport related logs are related to technical data such as objects inside transport requests.

> ⚠ Caution
>
> This data can also be obtained directly in the managed system in the transport organizer. In case of security concerns, SAP recommends you to disable S_APPL_LOG in the relevant roles for the users in the SAP Solution Manager system and check logs directly in the relevant managed systems.

Authorization Object SM_SUTMNGT

User role `SAP_SOCM_ADMIN` contains the inactive authorization object `SM_SUTMNGT` with `ACTVT 60` for import. This allows the administrator to create *Change Control Landscapes* with *Logical Component Group* assignment in SAP Solution Administration transaction `SLAN`, see application *Process Management* for details on `SLAN`.

Authorization Object SM_WD_COMP

During configuration, links are displayed only if authorization object `SM_WD_COMP` is assigned for the associated link ID.

> ⓘ Note
>
> In RM configuration, this object is maintained with full authorization.

6.6 Scenario-Specific Guide: Configuration Validation

6.6.1 Prerequisites

To use configuration validation, you need to have *Root Cause Analysis* configured, see *Landscape Setup Guide*.

6.6.2 Users and Authorizations

6.6.2.1 Users and Roles in the SAP Solution Manager

This paragraph gives an overview of users as recommended by SAP and their corresponding user roles.

Template End User

New template users with default ID: `CV_<user description>_<system ID>` added in the system.

The users are available in the *Solution Manager User Administration* (SMUA) app in the *Users* view of the *SAP Solution Manager Administration* launchpad group. For more information on SMUA, see the *Secure Configuration Guide*.

Administrator User CV_ADM_XXX (Help Text ID: TP_CV_ADM)

Single Roles	Help Text ID
SAP_CV_ALL	AUTH_SAP_CV_ALL Full authorization for Configuration Validation, especially Report Directory **Note** Authorization object AI_CCDB_SC is set to 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 this data, set the authorization object to active in this role.
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
BW-Related Single Roles	Help Text ID
SAP_BI_E2E SAP_SM_BI_ADMIN	• AUTH_SAP_BI_E2E • AUTH_SAP_SM_BI_ADMIN **Caution** If the BI scenario is remote, these roles have to be assigned to the BI user in the remote system in addition to authorization object S_RFCACL.

Display User CV_DIS_XXX (Help Text ID: TP_CV_DIS)

Single Roles	Help Text ID
SAP_CV_DIS	AUTH_SAP_CV_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BI_E2E	• AUTH_SAP_SM_BI_E2E • AUTH_SAP_SM_BI_DISP

Single Roles	Help Text ID
SAP_SM_BI_DISP	⚠ Caution If the BI scenario is remote, these roles have to be assigned to the BI user in the remote system in addition to authorization object S_RFCACL.

Main Authorization Objects

AI_CCDB_SC

With the help of this authorization object, you can protect individual configuration stores in customizing. Only users who have authorization for specific stores are able to access them. This is especially useful in regards to data protection, as many configuration stores can contain personal or even sensitive personal data.

→ Recommendation

We recommend that you only assign this authorization to specific administration or configuration users, and only for a specified time period.

6.7 Additional Security Measures

Consider the following actions as additional measures for preventing security breeches and reacting accordingly to events.

Activate Logging of Major Configuration Tables

The activation of table logs for configuration tables allows you to determine the time that a user changes specific values that are important for the configuration settings of your application.

→ Recommendation

SAP highly recommends logging major configuration tables.

For the following tables, the *Log Data Changes* checkbox is selected by SAP:

- AGS_WORK_CUSTOM (AGS: Work Centers Customizing)
- In case of external interfaces: ICT_CUSTOM (SM SD Interface: System Configuration)

SAP recommends that you activate logging for the following table:

- DNOC_USERCFG (Service Desk Customizing)

Steps to Activate Table Logging

1. Select the *Log Data Changes* checkbox for the required tables using transaction `SE13`.
2. Select the parameter value for parameter: `rec/client`.

How-to Information

For detailed information on logging, how to activate logging of tables, and the system requirements for logging, see https://help.sap.com/docs/SAP_NETWEAVER_740/521cd184dd2f491a9a4179edb66951c3/4db6d15036311dcee10000000a42189c.html?version=7.4.23.

See also SAP Note 1916.

Virus Scanning for Attachments

> → Recommendation
>
> SAP recommends you 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 the standard Knowledge Warehouse profile `/SCMS/KPRO_CREATE`, specifically for incidents which are created via an external interface.

7 Custom Code, DVM, and Value Management Dashboard

7.1 Document History

Here, all changes to the specific scenario guide are listed according to the support package.

Support Package Stacks (Version)	Description
SP13	**CCM** • `SAP_CCLM_ALL` and `SAP_CCLM_DIS` • Additional information of RFC connection requirements for *Blocklist Monitoring* **DVM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted roles `SAP_DVM_SERVICE`
SP10	**DVM** Testplan integration has been removed. > ⓘ Note > You do not require business partner integration for data volume management (DVM). **CCM** Added channel related information for the *Blacklist Monitoring* scenario (TRUSTED RFC) and `UPL/SCMON` (TMW RFC) related jobs.

Support Package Stacks (Version)	Description
SP01	**General Adaptations** • Roles SAP_SM_BI_BILO and SAP_SMWORK_BASIC_* are obsolete. • All roles have been adapted to the new *Process Documentation* function and SAP_BASIS 7.40. • Authorization object SM_WC_VIEW from role SAP_SMWORK_BASIC_* has been transferred into core authorization roles. **SAP Fiori Integration** • All users receive SAP Fiori Launchpad authorization role SAP_SM_FIORI_LP_EMBEDDED **Data Migration** • You can run data migration for CCM using the *Custom Code Management Migration* application within SAP Solution Manager Configuration (transaction SOLMAN_SETUP) in the *Related Links* area. **Value Management Dashboard (iCI)** • New configuration user SMC_ICI_*** and the corresponding roles are available.
SP02	**DVM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted roles SAP_DVM_*_COMP. **CCM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted roles SAP_CCLM_*_COMP • Adapted single role SAP_CCLM_ALL • Adapted single role SAP_SM_CCM_CONFIG • Added role SAP_SM_DASHBOARDS_ADMIN to the CCM_ADM* user and the composite role SAP_CCLM_ALL_COMP (to be able to configure dashboards). **iCI Dashboard (Value Management Dashboard)** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Added launchpad navigation role for SAP Engagement and Services to iCI users:SAP_SMWORK_SERVICE_DEV. • Adapted BI role SAP_BI_ICI

Support Package Stacks (Version)	Description
SP03	**CCM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted single role SAP_CCLM_ALL (authorization object S_DEVELOP) • Adapted single role SAP_SMWORK_CCLM **DVM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted role SAP_DVM_CONFIG • Adapted role SAP_DVM_ALL • In case of test plan integration and BPCA, role SAP_SM_KW_ALL must be assigned to the DVM administration user.
SP04	**CCM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted single role SAP_SMWORK_CCLM **DVM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted role SAP_SMWORK_DVM
SP05	**CCM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Added single role SAP_SM_USAGE_LOG to configuration user SMC_CCM_XXX. **DVM** • Substituted links in the DVM launchpad (SAP Fiori) role, see SAP Note 2463798. • Added OData services and authorization values in object SM_DVM_APP in single role SAP_DVM_DISPLAY for SAP Fiori applications, see *SAP Fiori Application Guide* for more information.

Support Package Stacks (Version)	Description
SP06	**CCM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted single role SAP_SM_CCM_CONFIG **DVM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted role SAP_SMWORK_DVM • Adapted role SAP_DVM_ALL (new application ID) **Note** All composite roles for DVM are not maintained anymore as of SP06. Reference role assignment to users is done via transaction SOLMAN_SETUP or application SMUA.
SP07	**CCM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted all single roles, SAP_SM_CCM_CONFIG and SAP_CCLM_* (new authorization objects SM_CC_SET for CCM settings, and SM_CC_LIB (authorization object SM_CC_AUT obsolete) and user roles concept) • **New use case ID for the administrator** in transaction SOLMAN_SETUP due to the adapted authorization concept. • New core role for new use case ID administrator: SAP_CCLM_ADM
SP08	**CCM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted role SAP_SM_CCML_CONFIG **DVM** Adapted authorization objects are described within the *Menu* tab of the respective roles. • Adapted role SAP_SM_BI_DVM_READ
SP08 Plus	**Custom Code Lifecycle Management (CCLM), Data Volume Management (DVM), Value Management Dashboard** • Adapted section on *Communication Channels* • Removed section *Technical Users*

7.2 Scenario-Specific Guide: Custom - Code Life Cycle Management

7.2.1 Getting Started

What is this guide about?

SAP Solution Manager covers a wide range of divers scenarios that you can use. As a customer, you might want to start with one scenario and later on add another scenario to your landscape. Therefore, SAP delivers scenario-specific security guides which cover all relevant information required 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. This information refers to all the security-relevant information required during the basic configuration of SAP Solution Manager. Without this information, SAP does not recommend setting up any specific scenario. This guide also does not replace the daily operations handbook that SAP recommends 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 corresponding roles that represent them. Here, you also find information about the relevant lauchpad groups.

Custom Code Lifecycle Management Use Cases

ATC Monitoring and Exemption Monitoring Integration

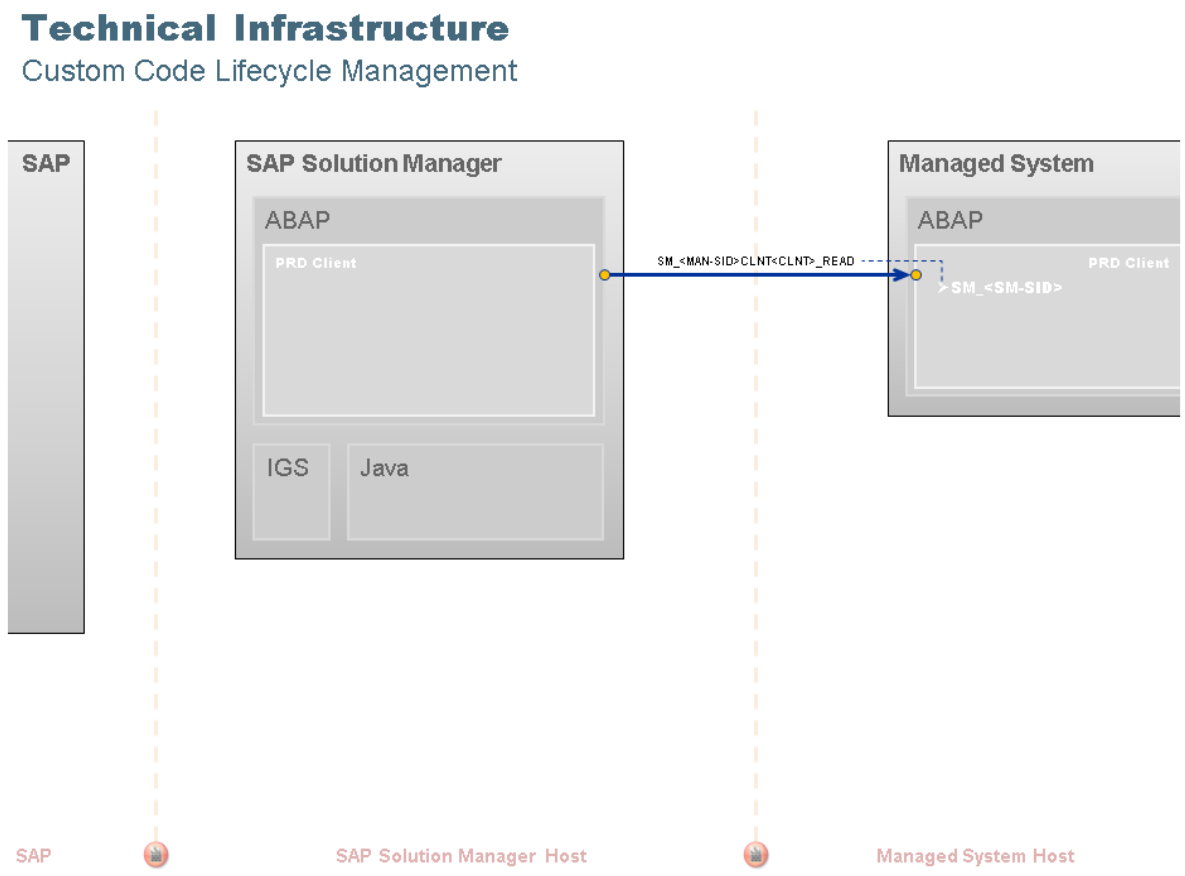
It allows you to extract ATC messages and exemptions for transparency on the quality dimension of custom code objects. The development manager must have central access to all kinds of exemptions within a system landscape.

7.2.2 Prerequisites

7.2.2.1 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 Custom Code Lifecycle Management (CCLM) scenario. SAP Solution Manager is connected via the READ RFC

connection to your managed systems. For more information about the connection, when it is used, and which technical user is required, see the following sections.



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 opening SAP Solution Manager Configuration (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 an upgrade or an installation and prior to configuring or updating your CCM scenario. You can run 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 PFCG. For more information on template users for CCM, see the respective section in this guide.

Data Migration Application Flow

The Migration application runs on the SAP 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 SAP Solution Manager system, locally, to activate extractors and collectors within the Extractor Framework 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 using RFC function modules (technical user: READ user and READ RFC connection). The data is then uploaded into the BW system or client. The ATC monitoring comprises two parts:

- The ATC messages monitoring the display of data read from the BW system or client.
- The ATC exemptions monitoring the display of data read from the BW system or client. This part also allows users with special authorizations to update the exemptions on the remote system via RFC connection.

7.2.2.2 Scenario Configuration User

> **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`.

Creating Configuration User in Basic Configuration Transaction SOLMAN_SETUP

When you call the guided procedure for Custom Code Management (CCM), the system asks you to create a specific configuration user (default technical user name of type `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 the 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 must 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.

Single Role	Help TXT ID
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP_DISP
SAP_SMWORK_CCLM	AUTH_SAP_SMWORK_CCLM
SAP_SM_CCM_CONFIG	AUTH_SAP_SM_CCM_CONFIG

Single Role	Help TXT ID
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
SAP_SM_USAGE_LOG	AUTH_SAP_SM_USAGE_LOG
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL

If you are using a remote BW scenario, role SAP_SM_BI_ADMIN must be assigned to the user with the same user ID in the BW system.

> **Note**
>
> To be able to:
>
> - Create users and assign user roles, you need to assign role SAP_SM_USER_ADMIN as well.
> - Use a trusted RFC connection between SAP Solution Manager and the managed systems, you need to assign role SAP_SM_S_RFCACL in the SAP Solution Manager system as well as the managed system.

Role SAP_SM_USAGE_LOG

For the usage logging, only the configuration user is relevant. This role allows the user to access the cross-scenario guided procedure *Usage Logging* in SOLMAN_SETUP. Due to the extended use of UPL for this scenario, the configuration role is part of the CCM configuration user. In general, the cross scenario can be configured by user SOLMAN_ADMIN. For more information, see section *View: Usage Logging* in the *Secure Configuration Guide*.

Scenario Configuration Transaction SOLMAN_SETUP

You can configure the basic technical settings using transaction SOLMAN_SETUP by 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 respective sections in *Users and User Roles*.

7.2.2.3 Communication Channels and Technical Users

The table below shows the communication channels and technical users used by SAP Solution Manager in this scenario.

> **Note**
>
> All mentioned RFC destinations are automatically created via SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`), see Secure Configuration Guide.

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to SAP backend system	HTTPS	Technical Communication User	Search for SAP Notes
SAP Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			Dashboard functionality
SAP Solution Manager to managed systems (Read) `SMTM<SID>CLNT<Client>`	RFC	`SM_<SID of Solution Manager>`	Reads data such as object lists, usage information, code inspector data, version of program information, and so on from the managed system.
SAP Solution Manager to managed systems (TMW) `SM_<SID>CLNT<Client>`	RFC	`SMTM<SID of Solution Manager>`	Required to run `UPL/SCMON`-related jobs as well as blocklist monitoring in the decommissioning cockpit.
SAP Solution Manager to managed systems (Trusted) `SM_<SID>CLNT<Client>_TRUSTED`	RFC	Named End-user (customer specific)	Required for *ATC* as well as blocklist monitoring in the decommissioning cockpit. For more information, see below. **Note** SAP strongly recommends using SSO in connection with TRUSTED RFC usage.
SAP Solution Manager to managed systems (Login) `SM_<SID>CLNT<Client>_LOGIN`	RFC	Named End-user (customer specific)	Workaround to using TRUSTED RFC

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section File Transfer Protocol (FTP)

Using Blocklist Monitor

When you use the blocklist monitor feature within the decommissioning cockpit, you have the following options as to which RFC connection you configure and use for change related activities.

1. TRUSTED RFC connection: When you use the RFC connection TRUSTED, you can log the user ID that triggers a change activity within the blocklist.
2. TMW RFC connection: If your security policy does not allow a TRUSTED RFC connection, you can use the TWM connection. In this case, you can display the user ID of the person triggering a change activity in the blocklist solely in the SAP Solution Manager system. See also SAP Note2257213.

For all display activities, the READ RFC connection is used.

7.2.3 Users and Authorizations

7.2.3.1 User Roles in SAP Solution Manager

This paragraph gives an overview over users as recommended by SAP and their corresponding user role assignments. 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 below give you a further overview over the single roles that 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 the 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_ADM)

Single Roles	Help Text ID
SAP_CCLM_ADM	AUTH_SAP_CCLM_ADM
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

End User ID: CC_ALL_XXX (Help Text ID: TP_CC_ALL)

Single Roles	Help Text ID
SAP_CCLM_ALL	AUTH_SAP_CCLM_ALL
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
SAP_SM_DASHBOARDS_ADMIN	AUTH_SAP_SM_DASHBOARDS_ADMIN

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

Single Roles	Help Text ID
SAP_BI_E2E_CCM	AUTH_SAP_BI_CCM
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

Managed system role

Single Roles	Remarks
SAP_CCA_ALL	CCA full authorizations

Display User ID: CC_DIS_XXX (Help Text ID: TP_CC_DIS)

Single Roles	Help Text ID
SAP_CCLM_DIS	AUTH_SAP_CCLM_DIS
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

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

Single Roles	Help Text ID
SAP_BI_E2E_CCM	AUTH_SAP_BI_CCM
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

ATC Monitoring

ATC Monitoring can be used within Custom Code Management CCM. The application authorization is included in the CCM roles. If your security requires you to separate the ATC application due to Segregation of Duty, 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. Additionally, assign the following roles:
    - `SAP_SMWORK_CCLM`
    - `SAP_SYSTEM_REPOSITORY_*`

Trusted RFC Destination

`ATC` can also be used with the `LOGIN RFC` destination.

Value Added Reseller (VAR) Compatibility

The application is not compatible with VAR. It also does not offer the possibility to separate system ID restrictions for specific users.

7.2.3.2 Main Authorizations Objects

> **Note**
>
> This function is not compatible with VAR or ISV.

Custom Code Management

Relevant Web Dynpro 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_LIB

The authorization object protects within tile *View Library* access to tabs *Owner* and *Contract*.

> **Note**
>
> Systems are not protected by authorizations, as it is not a list retrieved from LMDB, but separate. It is a list of systems where custom code objects are collected.

Authorization Object SM_CC_SET

This authorization object protects all settings in various tiles.

ATC and Exemption Monitoring Integration

Authorization Object SM_ATC_APP

To separate the display of ATC messages and exemptions and to provide change access to enable working with exemptions, a special authorization is required.

Users with display authorization for authorization object SM_ATC_APP can access both the ATC monitoring screen and the Exemption monitoring screens. However, in the Exemption monitoring screen, the buttons for validating or rejecting 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 (Convert to Database) for creating z-attributes in custom code and writing in the database. The object is delivered in an active state for specific CCM tables:

- AGSCCL_OBJECT
- AGSCCL_SYSTEM
- AGSCCL_CONTRACT
- AGSCCL_OWNER

These tables are initially empty. The central table is AGSCCL_OBJECT.

S_TABU_DIS

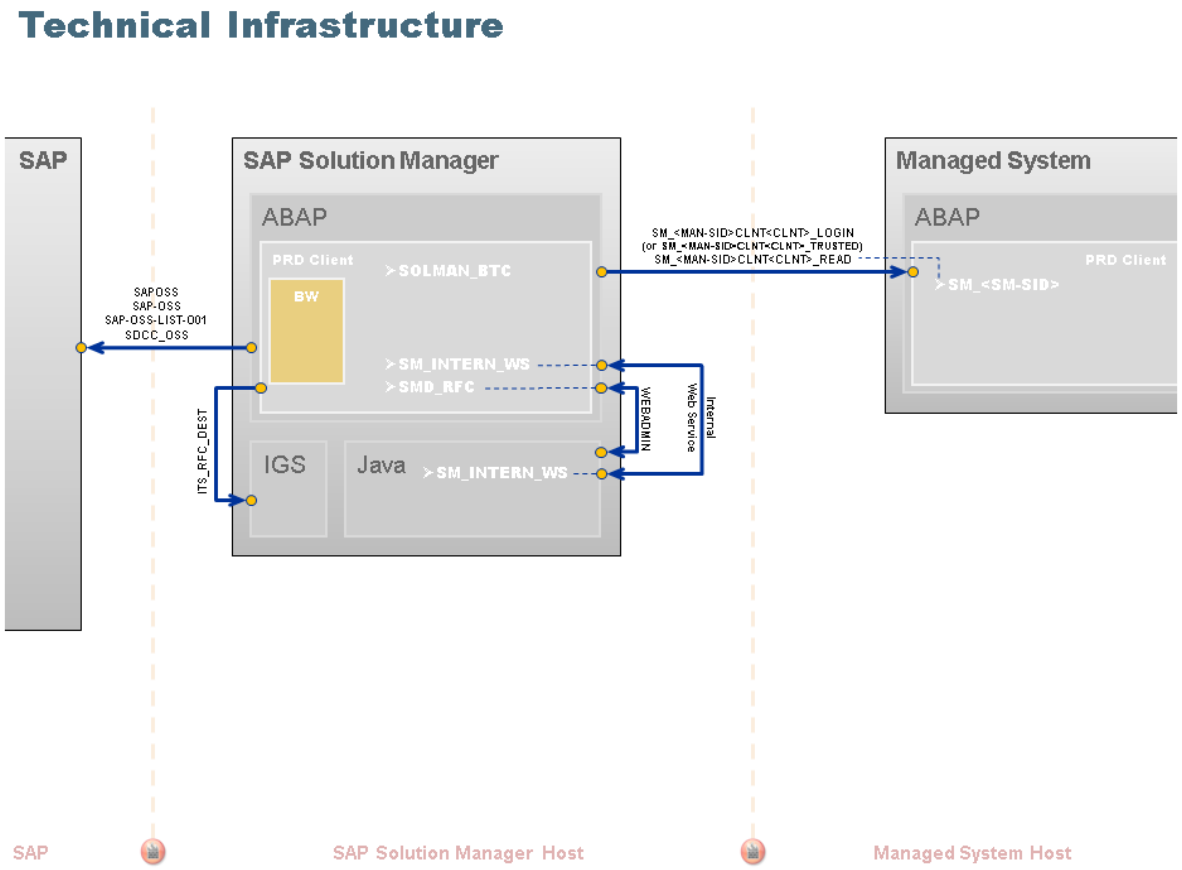
Authorization group SMCC is assigned to CCM tables and to authorization object S_TABU_DIS for all SAP_CCLM_*** roles.

7.3 Scenario-Specific Guide: Data Volume 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 scenario. SAP Solution Manager is connected via READ RFCor TRUSTED RFC (alternatively LOGIN) to your managed systems. You can find more information on all connections, when they are used, and which technical users are required in the following sections.



Infrastructure

7.3.1.2 Scenario Configuration

The *Data Volume Management* scenario is configured in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`).

To configure the scenario proceed as follows:

Configuration Scenario

After you have performed the *Basic Configuration* for SAP Solution Manager, you can perform basic functions.

When you open the *Data Volume Management* scenario, 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.

Single Roles	Help Text ID
SAP_DVM_CONFIG	AUTH_SAP_DVM_CONFIG
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP_DISP
SAP_SMWORK_DVM	AUTH_SAP_SMWORK_DVM
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL

If you use the remote BW scenario, you must assign the following roles to the user with the same user ID in the BW system:

- SAP_BI_E2E_DVM
- SAP_SM_BI_ADMIN

> **Note**
>
> To be able to create users and assign user roles, you must also assign role SAP_SM_USER_ADMIN.

Specific Authorization

During configuration, you are allowed to jump to the *Early Watch Alert Management* scenario to start the DVM report generation. The authorization is added in object SM_SETUP. This is relevant if the DVM section in an EWA report is to be displayed with detailed data.

> **Note**
>
> When you jump from one scenario to another scenario in SAP Solution Manager Configuration, the authorization access pop-up allows you to assign missing authorizations. In the case of DVM, you can ignore the pop-up.

7.3.1.3 Communication Channels and Technical Users

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

> **Note**
>
> All mentioned RFC destinations are automatically created via SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`), see Secure Configuration Guide.

Communication Channel	Protocol	User	Type of Data Transferred/Function
SAP Solution Manager to SAP backend system	HTTPS	Technical Communication User	Search for SAP Notes
SAP Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			Dashboard functionality
SAP Solution Manager to managed systems (Read) `SM_<SID>CLNT<Client>`	RFC	`SM_<SID of Solution Manager>`	To read DVM statistics and analyses
SAP Solution Manager to managed systems (Login) `SM_<SID>CLNT<Client>_LOGIN`	RFC	Named End-user (customer specific)	For self-service and user authentication when starting analysis in the managed system as a workaround to using TRUSTED RFC. For integration with BPCA, see scenario-specific guide for BPCA.
SAP Solution Manager to managed systems within customer network	FTP		Update route permission table, content: `IP` addresses, see section File Transfer Protocol (FTP)
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation Type Registered Server program (program: `IGS.<SID>`)		Graphics inclusion **Restriction** Manually created in transaction `SM59`

7.3.2 Scenario Integration

According to end-to-end business process life cycle, this business scenario needs to integrate with other functions that 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.

> **Note**
>
> For more detail on each individual scenario, see the corresponding 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 SAP Solution Manager system:

- SAP_SM_BPCA_TBOM*
- SAP_SM_BPCA_RES*
- SAP_STWB_2*

As Business Process Change Analyzer (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 authorizations for TRUSTED RFC connections to both users. For more information, see the scenario-specific guide for Business Process Change Analyzer (BPCA).

7.3.3 Users and Authorizations

7.3.3.1 User and Roles

This document provides an overview over users as recommended by SAP and their respective user role assignments for data volume management (DVM). All users are assigned a composite role that contains a number of single roles.

Authorization for Trusted RFCs between SAP Solution Manager and Managed Systems

Trusted authorizations are required between SAP Solution Manager and its managed systems. The user in the managed system and the user in the SAP Solution Manager system receive role SAP_SM_S_RFCACL (help text ID: AUTH_SAP_S_SM_RFCACL) with the authorization object S_RFCACL.

> **Note**
>
> Due to their highly security-relevant character, both roles are not contained in the respective composite roles.

Authorization for Trusted RFC between SAP Solution Manager and BW System

If you use a remote BW connection, the user in the SAP Solution Manager system is additionally assigned the 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 the S_RFCACL authorization (role SAP_SM_BW_S_RFCACL; help text ID AUTH_SAP_S_SM_RFCACL).

Administrator User (Help Text ID: TP_DVM_ADMIN)

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
SAP_SM_DASHBOARDS_ADMIN	AUTH_SAP_SM_DASHBOARDS_ADMIN
SAP_SM_DASHBOARDS_DISP_ICI	AUTH_SAP_SM_DASHBOARDSDISICI

If you use a remote BW scenario, these roles must be assigned to the user with the same user ID and password in the BW system.

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

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)

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
SAP_SM_DASHBOARDS_DISP_ICI	AUTH_SAP_SM_DASHBOARDSDISICI

If you are use a remote BW scenario, these roles must be assigned to the user with the same user ID and password in the BW system.

Single Roles	Help Text ID
SAP_BI_E2E_DVM	AUTH_SAP_BI_E2E
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

Technical Role in Managed System

Single Roles	Help Text ID
SAP_DVM_SERVICE	AUTH_SAP_DVM_SERVICE
SAP_DVM_GSS	AUTH_SAP_DVM_GSS

7.3.3.2 Critical Authorization Objects

The following section gives information on some of the main authorization objects for data volume management (DVM).

Authorization Object S_TABU_DIS

In user roles for DVM, you find the authorization object S_TABU_DIS. Authorization groups SARC and BCTA protect all relevant Customizing views and clusters for this scenario.

Authorization Object SM_DVM_APP

This authorization object gives access to various applications within the DVM frame. This object is also used in combination with the following SAP Fiori DVM applications:

- DVM Unused Data (object value: DVM_UNUSED)
- DVM Aging Data (object value: DVM_AGING)
- BW Housekeeping (object value: DVM_BWADM)
- BW Unused Data (object value: DVM_BWNUSE)

The values are delivered per default as active in role SAP_DVM_DISPLAY. If you do not use SAP Fiori apps, you can remove these values.

7.4 Value Management Dashboard (iCI - Interactive Continuous Improvement)

7.4.1 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 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 applications 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.

7.4.2 Prerequisites

7.4.2.1 Scenario Configuration

You can configure *Value Management Dashboard* in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`).

Creating Configuration User in Transaction SOLMAN_SETUP

When you open 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.

Single Role	Help Test ID
SAP_SETUP_SYSTEM_PREP_DISP	AUTH_SAP_SETUP_SYSTEM_PREP_DISP
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONF
SAP_SM_ICI_CONFIG	AUTH_SAP_SM_ICI_CONFIG
SAP_SM_SMUA_ALL	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_SL_ADMIN	AUTH_SAP_SM_SL_DISPLAY
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_DIS
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Single Role	Help Test ID
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC

7.4.2.2 Communication Channels and Technical Users

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

> **Note**
>
> All mentioned RFC destinations are automatically created in SAP Solution Manager Configuration (transaction SOLMAN_SETUP). For information, see the Secure Configuration Guide.

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to SAP back-end system	HTTPS	Technical communication user	Search for SAP Notes
SAP Solution Manager to/from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			Dashboard function
Solution Manager to managed systems (READ) SM_<SID>CLNT<Client>	RFC	SM_<SID of SAP Solution Manager>	READ data
SAP Solution Manager to managed systems within customer network	FTP		Update route permission table, content: IP addresses, see section File Transfer Protocol (FTP)
Internet Graphics Server (IGS) ITS_RFC_DEST	Activation type Registered server program (program: IGS.<SID>)		Graphics inclusion **Restriction** Manually created in transaction SM59

7.4.3 Interactive Continuous Improvement (iCI) Dashboard

The Interactive Continuous Improvement (iCI) Dashboard and Value Management Dashboard comprise an automated process of KPI collection. They focus on the following features:

- Value Management Dashboard (iCI)
- Integration into DVM and CCM

Technical System Landscape

The iCI Dashboard is opened using a *URL* on a browser. The iCI dashboard and iCI maintenance applications are both BSP applications which are located in SAP Solution Manager. The BSP applications use the iCI ODataService to fetch data from `ST-BCO` component (BWbsystem). The ODataService is located in ST component (Solution Manager). The ODataservice encapsulates the iCI queries based on the `0SM_ESRSK` multiprovider on the basic `0SM_ESRSG` cube and several iCI function modules. These modules are responsible for either fetching data from iCI tables or creating/updating data in iCI tables. All function modules used in the ODataService are `RFC` enabled if the BW system is configured as a 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 SAP Solution Manager and collects data in BW system, you need authorizations in SAP Solution Manager to display the collected data. In addition, these users must be present in the BW system with the correct authorization to collect the relevant data. This is possible per default with the template users for *DVM* and *CCM*.

Users and Roles in SAP 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 the 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 the following 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 SAP Solution Manager

You can create template users in transaction `SOLMAN_SETUP` via the guided procedure for *Value Management Dashboard* (`ICI_ADM_***` and `ICI_DIS_***`). Depending on whether you run your BW in the SAP Solution Manager client or a separate client, the `SOLMAN_SETUP` step assigns the relevant roles.

Administration User `ICI_ADM_XXX`

Roles in the SAP Solution Manager system

Role	Help TXT
SAP_SMWORK_SERVICE_DEV	AUTH_SAP_SMWORK_SERVICE_DEV
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_DASHBOARDS_DISP_ICI	AUTH_SAP_SM_DASHBOARDSDISICI
SAP_SM_DASHBOARDS_ADMIN	AUTH_SAP_SM_DASHBOARDS_ADMIN

Roles in the BW system

Role	Help TXT
SAP_BI_ICI	AUTH_SAP_BI_ICI
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN

Display User `ICI_DIS_XXX`

Roles in the SAP Solution Manager system

Role	Help TXT
SAP_SMWORK_SERVICE_DEV	AUTH_SAP_SMWORK_SERVICE_DEV
SAP_SM_DASHBOARDS_DISP_ICI	AUTH_SAP_SM_DASHBOARDSDISICI
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED

Roles in the BW system

Role	Help TXT
SAP_BI_ICI_DISP	SAP_SM_BI_DISP_ROLE
SAP_SM_BI_DISP	AUTH_SAP_SM_BI_DISP

Authorization object S_RFC

To be able to configure favorites and personal user settings, the display user also receives write and delete authorizations for this configuration part. It is included in the SAP_BI* roles.

8 Services

8.1 Document History

Here, all changes to the specific scenario guide are listed according to the support package.

Support Package Stacks (Version)	Description
SP01	**General Adaptations to Previous Release 7.1 (Due to new Process Documentation function)** • Removed roles SAP_SMWORK_BASIC* (obsolete) • Substituted roles SAP_SOL_PROJ_ADMIN_*, SAP_SOLAR_*, and SAP_SM_SOLUTION_* with SAP_SM_SL_* • Substituted roles SAP_SOL_KW_* with SAP_SM_KW_* **SAP Fiori Launchpad Integration** • All users receive SAP Fiori launchpad authorization role SAP_SM_FIORI_LP_EMBEDDED
SP02	**Service Request Management** • Adapted roles SAP_SERVICE_REQUEST_*.
SP03	**Service Delivery** • Added role SAP_OP_DSWP_EWA to composite role SAP_SERV_DELIVERY_*COMP and SAPSERVICE user.
SP04	**Service Request Management** • Adapted roles SAP_SERVICE_REQUEST* **Early Watch Alert Reporting** • Adapted role SAP_OP_DSWP_EWA

Support Package Stacks (Version)	Description
SP05	**New: Rapid Content Delivery** • New section on *Rapid Content Delivery* (Download Service) **Early Watch Alert Reporting** • Adapted role SAP_OP_DSWP_EWA **New: Guided Procedure in Transaction SOLMAN_SETUP** • New user SMC_SD for configuration of the guided procedure *SAP Engagement and Service Delivery* in transaction SOLMAN_SETUP **Service Level Reporting** • New section on service level reporting • New template user TP_SLR_EDIT in SMUA with corresponding roles (analogue composite role SAP_SLR_COMP). For more information on SMUA, see *Secure Configuration Guide*. **Service Sessions** • New stand-alone authorization object D_SVAS_DB for clean-up purposes. See section *Main Authorization Objects* **Service Request** • In role SAP_SERVICE_REQUEST_DIS the adapted values in authorization object S_DVAS_SES are used to display all relevant and executed services. For restriction advice, see section on *Main Authorization Objects* • Adapted roles SAP_SERVICE_REQUEST_* for TQM workplace (EWA)
SP06	**New: SAP S/4 Hana Readiness Check** • New section on *SAP S/4 Hana Readiness Check* data collection authorization **SMC_SD_*** Configuration User** Adapted role SAP_SD_CONFIG. For more information, see the corresponding section in this guide. **New: License Management** New section on license management
SP08 Plus	**Service Delivery** • Adapted section on *Communication Channels* • removed *Technical Users* section

8.2 Scenario-Specific Guide: SAP Engagement and Service Delivery

8.2.1 Getting Started

What is this guide about? SAP Solution Manager covers a wide range of divers scenarios that you can use. As a customer, you may 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 the 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 Secure Configuration Guide. This refers to all security-relevant information required during basic configuration of SAP Solution Manager. Without this information, SAP does not recommend you to set up any specific scenario. This guide does not replace the daily operations handbook that SAP recommends customers to create for their productive operations.

This guide covers the following topics:

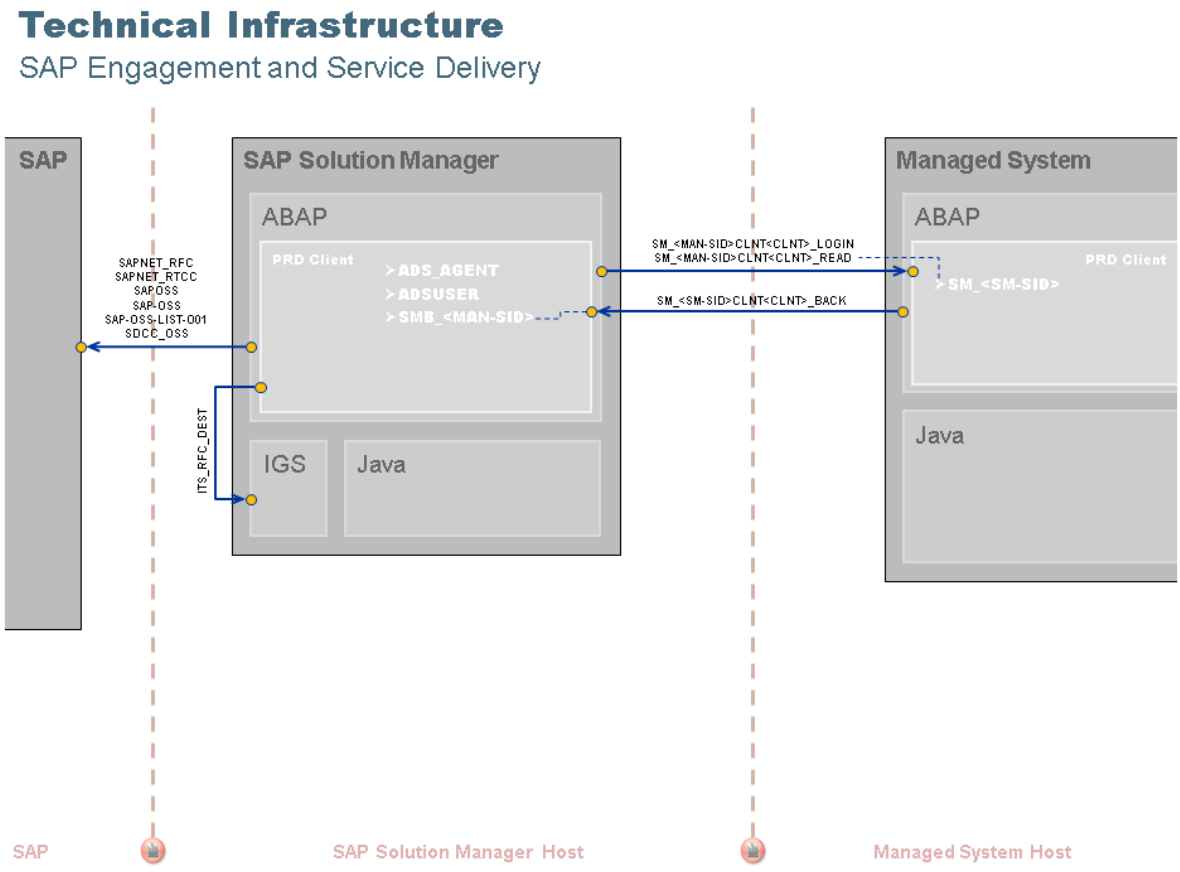
- **Getting Started:** Find out about target groups of this guide. Links for any additional components can be found in the Core Guide.
- **Prerequisites:** Find out about the specific system landscape components such as RFC destinations and technical users and how they connect to each other.
- **Users 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 centers.
- **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.

8.2.2 Prerequisites

8.2.2.1 Technical System Landscape

The graphic below gives you an overview over the basic technical system landscape that is needed to run the complete scenario. SAP Solution Manager is connected via READ-RFC to your managed systems, and your

managed systems are connected to SAP Solution Manager via `BACK-RFC`. You can find more information on all connections, when they are used, and which technical users are required in the following sections:



Infrastructure

8.2.2.2 Scenario Configuration User

Basic Configuration of 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. You can use user `SOLMAN_ADMIN` for the configuration of *Basic Settings*.

Configuration User SMC_SD

When you open the guided procedure, you are prompted to create a specific configuration user with the default technical name: `SMC_SD_<Client>` for Help Text ID: `USER_CONFIG_SD`. The system automatically

adds all relevant user roles. Due to automated configuration, authorizations in the following roles are all fully maintained:

Single Role	Help Text ID
SAP_SD_CONFIG	AUTH_SAP_SD_CONFIG
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_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBEDDED
SAP_SM_ESH_ADMIN	AUTH_SAP_SM_ESH_ADMIN
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC
SAP_SMWORK_SERVICE_DEV	AUTH_SAP_SMWORK_SERVICE_DEV

Notification E-Mail Template

To be able to change *Notification E-Mail Templates*, transaction SE61 (Change Notification E-Mail Template) is required. This transaction references the following critical authorization objects:

- S_DEVELOP
- S_TRANSPRT
- S_DOKU_AUT

These objects are delivered in role SAP_SD_CONFIG but are set to inactive.

> → Recommendation
>
> SAP recommends you to either set these objects active if this function is required, or create a separate role for this function and assign it in addition to the configuration role SAP_SD_CONFIG.

Download of MS Word Content

To be able to configure the activity for *Download of MS Word Content* in the GP in transaction SOLMAN_SETUP, you require transaction SU3. The transaction is added directly in the authorization object S_TCODE but is set to inactive. This transaction references the following critical authorization objects which are delivered in inactive state. They must be activated in the role if the function is required.

- S_DATASET
- S_BTCH_ADM

> **Note**
>
> The possibility to download content from the SAP system poses a potential security risk. If you require this possibility, SAP recommends you to assign it to specific users only.

8.2.2.3 Communication Channels and Technical Users

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

> **Note**
>
> All mentioned RFC destinations are automatically created via transaction SOLMAN_SETUP, see Secure Configuration Guide.

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to SAP backend system	HTTPS	Technical Communication User	• Search for SAP Notes • Exchange problem messages with SAP, synchronize system data with the SAP Support Portal and send data about managed systems, transfer of solution, issue data, transfer feedback to SAP Service Connection, product data download • Retrieve information about the messages that have been changed at SAP • Used by *Service Data Control Center* to communicate with the SAP Support Portal front end system, update Service Definitions (functions: System Monitoring for EWA and Service Plan) See SAP Note 763561 • Send EarlyWatch Alerts (functions: System Monitoring for EWA and Service Plan) • Service Preparation Check (RTCCTOOL)
SAP Solution Manager to/ from SAP BW system/client **Note** Check the *Secure Configuration Guide* section *Communication with SAP BW*			Dashboard functionality for Process Management

Communication Channel	Protocol	User	Type of Data Transferred / Function
SAP Solution Manager to managed systems (Read) `SM_<SID>CLNT<Client>`	`RFC`	`SM_<SID of Solution Manager>`	To retrieve data from the managed systems for service sessions, collect information on product licence and maintenance certificates
Managed systems to SAP Solution Manager (Back) `SM_<SID>CLNT<Client>_BACK`	`RFC`	`SMB_<SID of Solution Manager>`	Send service data from managed systems to SAP Solution Manager
SAP Solution Manager to managed systems within customer network	`FTP`		Update route permission table, content: `IP` addresses, see section File Transfer Protocol (FTP)
Internet Graphics Server (IGS) `ITS_RFC_DEST`	Activation type Registered server program (program: `IGS.<SID>`)		Graphics inclusion **⚠ Restriction** Manually created in transaction `SM59`
`CCMSPING.<server><SystemNr.>`	Registered server program (program `ccmsping.00`)	`CSMREG` (customer specific), User created during configuration of Central Monitoring (`CCMS`)	Service level reporting with `CCMSPING`

8.2.2.4 SAP Support Portal Contact in SAP Solution Manager (Table: AISUSER)

Users who communicate with the SAP Support Portal via the `RFC` destination 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 https://help.sap.com/viewer/p/SAP_Solution_Manager.

8.2.2.5 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

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

8.2.2.6 S-User Authorization for Data Download from SAP

Your S-User needs the following authorizations for SAP Support Portal functions.

S-User Authorization Download Data from SAP

Activity	Authorization
Administration	`ADMIN`
Maintain all logon data	`PWCHGE`
Maintain user data	`USER`
Maintain system data	`INSTPROD`
Request license key	`LICKEY`

8.2.2.7 Business Partners Created During Configuration

Use

When you configure 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:

First Name	Last Name	Remarks
SAP	Technical Quality Manager	Automatically assigned *ID* `TQM` or `SAPTQM`
SAP	Support Advisor	Automatically assigned *ID* `SAPSUPAD`
SAP	Engagement Architect	Automatically assigned *ID* `SAPENAR`
SAP	Back Office	Automatically assigned *ID* `SAPBACKO`
SAP	Consulting	Automatically assigned *ID* `SAPCON`
Customer	Program Management	Automatically assigned *ID* `CUSTPM`
Customer	Business Process Operations	Automatically assigned *ID* `CUSTBPM`
Customer	Custom Development	Automatically assigned *ID* `CUSTCD`
Customer	Technical Operations	Automatically assigned *ID* `CUSTTO`
Customer	Partner	Automatically assigned *ID* `CUSTPAR`

> **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 the section on User SAPSUPPORT).

For SOLMAN_SETUP Template Users and Configuration Users

Users created using transaction `SOLMAN_SETUP` are assigned a corresponding 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

For more information on how to configure the basic settings, see the configuration guide for SAP Solution Manager at https://help.sap.com/viewer/p/SAP_Solution_Manager ▶ *SAP Components* ▶ *SAP Solution Manager <current release>* ▶.

8.2.3 CRM Standard Customizing for Solution Manager

The Service Request and Issue Management use cases are based on `CRM` and use `CRM` Customizing such as transaction types, action profiles, and so on. SAP delivers a standard `CRM` Customizing that is also maintained

in the individual CRM authorization objects. The following table gives you an overview of the used transaction types.

> ⚠ Caution
>
> If you copy SAP standard Customizing, you must add the changed values in the corresponding CRM authorization objects for the scenario. For more information, see the How-to guide on how to maintain authorization objects.

Transaction Type Issue Management

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

Transaction Type	Usage	Remarks
SLFS	Service Request	Supported

8.2.4 Scenario Integration

SAP Engagement and Service Delivery combines a number of tools 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.

8.2.5 Recommended Users and Authorizations

8.2.5.1 Dialog User SAPSERVICE

The SAPSERVICE user is used for service delivery for SAP. It is present in all relevant systems in your system landscape. You can create this user during basic settings configuration for SAP Solution Manager. The user is present in:

- SAP Solution Manager
- Managed Systems
- BW System

In general, this user retains all authorizations of SAPSUPPORT user (read access). In addition, it receives further authorizations in the SAP Solution Manager system and the managed systems.

Trusted RFC Authorizations

The authorization for trusted RFCs should be assigned, in case trusted RFCs are created between SAP Solution Manager and managed systems, and, in case BW is remote, in the BW system and SAP Solution Manager. The corresponding role in SAP Solution Manager and managed systems is SAP_SM_S_RFCACL. In the BW system, the role is called SAP_SM_BW_S_RFCACL.

Specific Role Namespace

Due to the nature of the user being a set user, which should not be changed in its authorizations, all roles in the SAP Solution Manager system and (if it is remote) the BW system are copied automatically into their own namespace ZSD*.

In SAP Solution Manager

For all roles assigned to the SAPSERVICE user in SAP Solution Manager, check the corresponding entry in step *Create Basic Dialog Users* in the view *Basic Configuration*. If you are not sure about the roles assigned by the system, check out the documentation link behind the corresponding role.

In SAP Solution Manager System

Single Role	Help Text ID
SAP_BPR_PPM	AUTH_SAP_BPR_PPM
SAP_CPR_PROJECT_ADMINISTRATOR	AUTH_SAP_CPR_PROJECT_ADMINISTRATOR

Single Role	Help Text ID
SAP_CPR_USER	AUTH_SAP_CPR_USER
SAP_XRPM_ADMINISTRATOR	AUTH_SAP_XRPM_ADMINISTRATOR
SAP_TECH_MONITORING_ONSITE	AUTH_SAP_TECH_MONITORING_ONSITE
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SUPPDESK_PROCESS	AUTH_SAP_SUPPDESK_PROCESS
SAP_STWB_WORK_ALL	AUTH_SAP_STWB_WORK_ALL
SAP_STWB_SET_ALL	AUTH_SAP_STWB_SET_ALL
SAP_STWB_INFO_ALL	AUTH_SAP_STWB_INFO_ALL
SAP_STWB_2_ALL	AUTH_SAP_STWB_2_ALL
SAP_SOL_TRAINING_EDIT	AUTH_SAP_SOL_TRAINING_EDIT
SAP_SM_ST14	AUTH_SAP_SM_ST14
SAP_SM_SPC	AUTH_SAP_SM_SPC
SAP_DBA_DISP	AUTH_SAP_DBA_DISP
SAP_ISSUE_MANAGEMENT_EXE	AUTH_SAP_ISSUE_MANAGEMENT_EXE
SAP_ONSITE_SU01_SE16	AUTH_SAP_ONSITE_SU01_SE16
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SCDT_DIS	AUTH_SAP_SCDT_DIS
SAP_SCIDM_DIS	AUTH_SAP_SCIDM_DIS
SAP_SCOUT_ALL	AUTH_SAP_SCOUT_ALL
SAP_SERVICE_REQUEST_ALL	AUTH_SAP_SERVICE_REQUEST_ALL
SAP_SMWORK_BASIC	AUTH_SAP_SMWORK_BASIC
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SMWORK_SERVICE_DEV	AUTH_SAP_SMWORK_SERVICE_DEV
SAP_SM_BP	AUTH_SAP_SM_BP
SAP_SM_ADMIN_COMPONENT_ALL	AUTH_SAP_SM_ADMIN_COMPONENT_ALL
SAP_SM_EEM_CONF	AUTH_SAP_SM_EEM_CONF

Single Role	Help Text ID
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_ITPPM_ALL	AUTH_SAP_SM_ITPPM_ALL
SAP_SM_KW_ALL	AUTH_SAP_SM_KW_ALL
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_SA38	AUTH_SAP_SM_SA38
SAP_SM_SL_EDIT	AUTH_SAP_SM_SL_EDIT
SAP_SM_ESH_EXE	AUTH_SAP_SM_ESH_EXE
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY

In Managed System

In the managed systems, the user is not created automatically due to required authorizations that depend on the business contexts. See SAP Note 1405975 for appropriate roles.

In BW Client/System: Remote Scenario (Help Text ID: USER_SAPSERVICE)

Assigned Roles	Help Text-ID
SAP_BI_E2E	AUTH_SAP_BI_E2E

ITPPM Project Integration

The following roles are required for the ITPPM Project integration for this user:

- SAP_BPR_PPM
- SAP_CPR_PROJECT_ADMINISTRATOR
- SAP_CPR_USER
- SAP_XRPM_ADMINISTRATOR
- SAP_SM_ITPPM_ALL

8.2.5.2 Introduction

To enable your users to work with the application, you must assign them authorizations in the SAP 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 corresponding 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.

8.2.5.3 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`.

8.2.5.4 Supportability Performance Platform

Use

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 `KPI`s with related industries, transparency and follow up activities based on improving specific `KPI`s can be initiated by the `TQM`s and `ESA`s. 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 `KPI`s are aligned with the IT strategy (for instance innovation driver, service, or solution provider) during an `ACCOE` assessment together with the customer. The `KPI`s are activated and a baseline measurement is performed. The initial action plan to reach the `KPI` target is agreed. The `KPI`s 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)

8.2.5.5 User Descriptions and User Integration Roles for Issue Management

This paragraph gives an overview over users as recommended by SAP and their corresponding user roles assignment for SAP Engagement and Service Delivery. All users are assigned a composite role that includes 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 launchpad relevant roles.

Manager/Administrator

Single Role	Restriction on
SAP_ISSUE_MANAGEMENT_ALL	Authorization to execute Issues
SAP_SM_SL_ADMIN	Full authorization for Process Management

Operations

Single Role	Restriction on
SAP_ISSUE_MANAGEMENT_ALL	Authorization to execute Issues
SAP_SM_SL_EDIT	Maintenance authorization for Process Management

Display User

Single Role	Restriction on
SAP_ISSUE_MANAGEMENT_DIS	Display authorization for Issues
SAP_SM_SL_DISPLAY	Display authorization for Process Management

8.2.6 Security Optimization Service

For Security Optimization service, you need to assign additional authorizations. For more information, see SAP Note 696478.

8.2.7 SAP EarlyWatch Alert Management

The SAP EarlyWatch Alert (EWA) service monitors the most critical areas of an SAP component, focusing on performance and stability. EWA data is based on weekly performance and system statistics, as well as of system configuration and error analysis data. The data is collected by unmodifiable data collectors using transaction SDCCN in the target system and stored in SAP Solution Manager cluster tables BDLDTOC and BDLDATCOL for persistence. The report displays aggregates of this data as analysis results, trend graphs, and so on.

Configuration

You can configure SAP EarlyWatch Alert reporting in SAP Solution Manager Configuration (transaction SOLMAN_SETUP). Since the setup for EWA is mandatory for all systems in your system landscape, the procedure for setting up SAP EarlyWatch Alert Management can be run by user SOLMAN_ADMIN.

Data Protection

The report does not contain any user-specific data. Although the statistical data can contain user names, they are not related to app data, but only to technical data, such as response times or information for technical error analysis. If the user who collects the data in the source system is authorized to run transaction ST03 (Workload Monitor) and display application-related data, the EWA report also displays technical transaction codes with user names. This can be avoided by removing value S_TOOLS_EX_A from the authorization object S_TOOLS_EX for the user in question.

Data Archiving

For more information, see SAP Note 546685.

8.2.8 Service Level Reporting

SLR Recipients Maintenance is an application used to maintain recipients for SLR service reports.

Service level reporting is based on:

- Early Watch Alert and does not use its own data collectors
- Usage of LMDB
- Recipient List for Notification

User and Roles

If you require a user for service level reporting, you need to assign the following roles:

- `SAP_NOTIF_DIS`
- `SAP_OP_DSWP_SLR (<_DIS> in case of display user)`
- `SAP_SMWORK_SERVICE_DEV`
- `SAP_SM_FIORI_EMBEDDED`
- `SAP_SYSTEM_REPOSITORY_DIS`

These roles are also assigned to *Standalone* template users `TP_SLR_EDIT` and `TP_SLR_DIS` in the SAP Solution Manager system. You can create this user from the SAP Solution Manager User Administration (SMUA) tool.

Authorization Objects

Two additional authorization objects are especially relevant for `SLR`.

SM_SLR

This authorization object is required to access the application.

SM_EMAIL

This authorization object restricts on the level of email administration.

8.2.9 Service Download - Rapid Content Delivery

The Rapid Content Delivery application downloads and imports up-to-date SAP Solution Manager content packages.

Configuration

You can configure this application in *Basic Settings* for SAP Solution Manager in transaction `SOLMAN_SETUP` with the user `SOLMAN_ADMIN`.

S-User Assignment

An S-User is necessary to run the background job `SM:RCD_CHECK_UPDATES` for *Download Service*. This S-User can either be assigned to the `SOLMAN_BTC` user or a specific user can be used.

Authorization Object S_SDS_MGR

Authorization object `S_SDS_MGR` controls access to the download function. It is contained in role `SAP_SM_BATCH`. If you use another user than `SOLMAN_BTC` for this function, you need to assign the authorization to it.

8.2.10 SAP Readiness Check

You can start the collection of data for this service from the Scope and Effort Analyser tool or from services. Authorizations for this Service are not shipped within a specific role. To be able to run this collection, you require the following authorizations:

- Transaction `SA38 (S_TCODE)` to run the job
- Aauthorization object `S_PROGRAM` containing `SUBMIT` for value `AGSRC_START_ANALYSIS`
- Authorization objects `SM_CDC_INS` and `SM_CDC_OBJ` with `ACTVT 03` (display)
- Authorization object `AI_DIAGE2E` with `ACTVT 03`
- Authorization object `S_ADMI_FCD` with value `ST0M`
- Authorization object `S_C_FUNC`
- Authorization object `S_SERVICE` for Odata service: `DSWP_CDC_DYNAMIC_TILE*`

> → Recommendation
>
> SAP recommends you to add the Odata service of types `IWSG` and `IWSV` in the menu tab of the role.

8.2.11 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 *Authorization Concept Guide* section `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 object is delivered with full authorization as of SP05. The following list of *Self Service Package ID*s and *Types* are most relevant:

- `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

> ⓘ Note
>
> **How to Maintain Authorization Objects**
>
> 1. In transactions DSADEV, check the *Service Package* name for the service that you want to restrict.
> 2. In the SAP Solution Manager system, check table DSVASSESSPACK.
> 3. Enter the *Service Package* as input in the BUNDLE_ID field. As output, you get the value to enter in the authorization object SES_GR_TYP, which is composed of the SESSGRP and SESSTYPE fields of the table DSVASSESSPACK in this way SESSGRP/SESSTYPE.

Authorization Object D_SVAS_DB

This authorization object is a stand-alone object. It is not included in any delivered role for SAP Solution Manager due to its security-criticality. You only need to use the object once. It is required for the Service Session Reorganization Report RDSMOPREDUCEDATA. With this report, you can clean up your database from inconsistent data. The report and the object are delivered with SP05.

> → Recommendation
>
> SAP recommends that you create a separate role for this authorization object and remove the role after usage again out of the system.

9 Dashboard Framework Integration

9.1 Dashboard Users based on Dashboard Builder

General Dashboard Builder Roles

SAP provides the following roles for Dashboard Builder which you can use to specify the Dashboard Builder objects that you want to be displayed or edited.

Roles in SAP Solution Manager

- `SAP_SM_DSH_CONF`: Assign this role to the users whose tasks include creating, editing, and deleting dashboard categories, dashboards, and tiles.
- `SAP_SM_DSH_DISP`: Assign this role to the users whose tasks include displaying dashboards and tiles.

Roles in SAP BW System

- `SAP_SM_BI_DSH_CONF`: Assign this role to the users whose tasks include creating, editing, and deleting dashboard categories, dashboards, and tiles.
- `SAP_SM_BI_DSH_DISP`: Assign this role to the users whose tasks include displaying dashboards and tiles. This also includes the authorizations for executing and displaying the BW queries that are used in the dashboards.

Scenarios Using Dashboards and Respective Use Case IDs

You can create scenario users with dashboard authorizations in transaction `SOLMAN_SETUP` and application *SAP Solution Manager Administration (SMUA)*.

Change Management

- Use case IDs with the following configuration role:
  - `CH_ADM_<SID>`
- Use case IDs with the following display roles:
  - `CH_CM_<SID>`
  - `CH_OPRT_<SID>`

IT Service Management

- Use case IDs with the following configuration role:
  - `IM_ADM_<SID>`

- Use case IDs with the following display roles:
  - `IM_PROC_<SID>`
  - `IM_DIS_<SID>`

Business Process Operation

- Use case IDs with the following configuration role:
  - `BPO_ADM_<SID>`
- Use case IDs with the following display roles:
  - `BPO_ALRT_<SID>`
  - `BPO_REP_<SID>`
  - `BPO_DIS_<SID>`
  - `BPO_CDC_<SID>`

Creating "PURE" Dashboard Roles

For security reasons, a dedicated user for dashboard access or dashboard configuration may be necessary in addition to SAP Fiori access authorization and core application authorizations.

> → Tip
>
> If your security requires minimal authorizations assigned to any dashboard user, SAP recommends that you trace all the required authorization objects with specified values for your specific application.

Configuration User

A configuration user requires the following roles:

- `SAP_SM_DSH_CONF` in SAP Solution Manager
- `SAP_SM_BI_DSH_CONF` in SAP BW system/client
- `SAP_SM_FIORI_LP_EMBEDDED` for SAP Fiori access
- `SAP_SMWORK_<scenario>` for SAP Fiori access
- `SAP_<core application role>` for application authorizations
- `SAP_BI_E2E_<scenario>` for BW application authorizations

Dashboard End User

A dashboard end user requires the following roles:

- `SAP_SM_DSH_DISP` in SAP Solution Manager
- `SAP_SM_BI_DSH_DISP` in SAP BW system/client
- `SAP_SM_FIORI_LP_EMBEDDED` for SAP Fiori access
- `SAP_SMWORK_<scenario>` for SAP Fiori access
- `SAP_<core application role>` for application authorizations
- `SAP_BI_E2E_<scenario>` for BW application authorizations

9.2 Dashboard User for OLD Framework

Scenarios Using OLD Framework

These scenarios use the old dashboard framework technology for their dashboards:

- Custom Code Management
- Data Volume Management
- Business Process Improvements

Dashboard User Roles

You can create a scenario for end users with dashboard authorizations using use case ID reference in transaction `SOLMAN_SETUP` or in the application *Solution Manager Administration (SMUA)*.

Configuration Users

The configuration of dashboards requires role `SAP_SM_DASHBOARD_ADMIN.`

Dashboard End Users

End users require the dashboard role `SAP_SM_DASHBOARDS_DISP_ <Scenario>`.

Creating "Pure" Dashboard Users

For security reasons, a dedicated user for dashboard access or dashboard configuration may be necessary in addition to SAP Fiori access authorization and core application authorizations.

> → Tip
>
> If your security requires minimal authorizations assigned to any dashboard user, SAP recommends that you trace all the required authorization objects with specified values for your specific application.

Important Disclaimers and Legal Information

Hyperlinks

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

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

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

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

Example Code

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

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2025 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. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company 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 SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP