



SECURITY GUIDE | PUBLIC

Document Version: 2.0 – 2019-09-01

Secure Configuration Guide - SAP Solution Manager 7.2 SPS 6

Content

1	Security Guide - Secure Configuration.	5
2	Changes and News in Secure Configuration: Document History.	6
3	Overview.	17
3.1	Overview: All Users Created in Basic Configuration in Transaction SOLMAN_SETUP.	17
3.2	Overview: Solution Manager Configuration.	21
3.3	Overview: Where Used - Solution Manager Technical RFC - Users per Scenario (READ, TMW, TRUSTED).	21
3.4	Overview: All End-Users and Business Partners per SOLMAN_SETUP Scenario.	23
4	System Landscape.	24
4.1	Technical System Landscape.	24
5	Specific Security Settings.	25
5.1	Solution Manager Administration Work Center: Security Access Point.	25
5.2	Technical System Landscape.	25
5.3	Communication Channels and Destinations.	28
5.4	Required TCP/IP Ports.	43
5.5	Securing Attachments.	46
5.6	Log Entries, Data Storage, and PANKS (NOTE Search).	46
6	User Administration/Authentication and Role Adjustment.	48
6.1	Introduction.	48
6.2	User Management Tools and User Types.	48
6.3	Automatic User Creation Options using Transaction SOLMAN_SETUP.	51
6.4	Solution Manager User Administration (SMUA).	55
6.5	Automatic Managed System Configuration (AMSC) Update using Transaction SOLMAN_SETUP	57
6.6	Passwords for Solution Manager Default Users.	57
6.7	Role Adjustment Tool in Transaction SOLMAN_SETUP.	58
6.8	Using Central User Administration.	59
	Introduction.	59
	Prerequisites.	61
	Configuration Scenarios.	64
	Configuration Integration in Transaction SOLMAN_SETUP.	66
6.9	Secure Storage.	68
6.10	Integration into Single Sign-On Environments (SSO).	69
7	Users and Authorizations Relevant for Configuration.	70

7.1	Getting Started.	70
7.2	Documentation (Help Text IDs) for Users and Roles.	71
7.3	SOLMAN_SETUP Configuration Transaction.	72
7.4	SOLMAN_SETUP Configuration Administration Tool.	74
7.5	Overview on Security - Relevant Activities.	74
7.6	Solution Content Activation (Data Migration).	75
	Content Activation (Migration) Procedures.	75
	Process of Migration and Migration Configuration User SMC_MIG_XXX.	76
7.7	Users Created During Installation.	79
	Database User SAP<SID>DB [MANAGED.DB.USER].	79
	OS Engine User [MANAGED.OS.SIDADM].	80
	OS User Dedicated to the Diagnostics Agent <SID>ADMIN [MANAGED.OS.AGTSIDADMIN]	80
		80
7.8	Configuration Authorization Objects per Procedure.	80
	Configuration Transaction Frame Authorization.	80
	View: System Preparation and Its Authorizations.	82
	View: Infrastructure Preparation and Its Authorizations.	86
	View: Basic Configuration and Its Authorizations.	89
	View: Managed System Configuration and Its Authorizations.	92
	View: Embedded Search.	93
	View: Usage Logging.	94
	View: Additional Security Recommendations.	96
	View: Scenario Configuration and Its Authorizations.	96
7.9	SAP Solution Manager Configuration Users.	97
	Introduction.	97
	Solution Manager Configuration User SOLMAN_ADMIN.	98
	Configuration Users SMC*** for Application-Specific Procedures.	105
7.10	SAP Solution Manager Technical Users.	107
	Introduction.	107
	Technical User SM_INTERN_WS.	107
	Technical User SM_EXTERN_WS.	108
	Technical User SOLMAN_BTC.	108
	Technical User SMD_RFC.	109
	Technical User SM_EFWK.	110
	Technical User SM_AMSC.	112
	Technical User SM_TECH_ADM.	113
	Technical User for RFC - connection BACK	
	<SMB_<SIDofManagedSystem>>[MANAGING.ABAP.RFC].	114
	User Wily Guest.	116
	Technical User SEP_WEBSRV.	116
7.11	Technical Users for SLD and LMDB.	116

	Introduction.	116
	Technical User LMDB_DS_XXX.	117
	Technical User SM_SLD_NOTIF.	117
	Technical User SLD_CS_USER.	118
	Technical User SLDAPUSER.	119
	Technical User SLD_DS_<SID>.	119
7.12	Users and Authorizations for BW Configuration.	120
	Introduction.	120
	BW Administrator User SM_BW_ADMIN.	120
	Technical User SM_BW_ACT.	121
	Technical User SMD_BI_RFC.	121
	Technical User SM_BW_<SID>.	121
	Technical User BI_CALLBACK.	122
	Diagnostics Center.	122
	Technical User SM_BOC.	123
7.13	Users and Authorizations for Managed Systems.	123
	Introduction.	123
	Administrator User in ABAP: SM_ADMIN.	123
	Administrator User in Java: SM_ADMIN_<SolManSID>.	125
	Technical User SMDAGENT_<SolManID> for Wily Host Agent.	126
	Technical Users for RFC - Connections READ and TMW.	126
	Technical User SM_COLL_<SIDofSolMan>.	129
	J2EE Administrator J2EE_ADMIN.	131
	Administrator OS User.	131
7.14	Basic Configuration Dialog Users.	131
	Dialog User SAPSUPPORT.	131
	Dialog User SAPSERVICE.	133
	Solution Manager Administration User.	136
7.15	Standard/Template Users.	139
7.16	S-Users.	139
	Introduction.	139
	Technical Communication User for SAP Backend.	140
	S-User for Communication.	140
7.17	User Role for TREX Administration.	141

1 Security Guide - Secure Configuration

Use

This guide refers to setup topics and specific roles and authorizations for it.

⚠ Caution

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

For general information on the authorization concept of Solution Manager or application specific security, refer to the according complimentary guides on the SAP Service Marketplace at: <http://service.sap.com/instguides>
➤ *SAP Components* ➤ *SAP Solution Manager* ➤ *<current release>* ➤ (updated with every change per Support Package).

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

Integration

Security topics are relevant for the following phases:

- Configuration
- Update

More Information

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

2 Changes and News in Secure Configuration: Document History

⚠ Caution

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

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

Support Package Stacks (Version)	Date	Description
	2019/09/01	Due to the shutdown of SAPOSS connections, this guide has been adapted. Please see section Communication Channels and Destinations for current information.

Support Package Stacks (Version)	Date	Description
SP00/ SP01	2015 / 12 / 11	General Information - As of Release 7.2, the security information is published within four separate guides: SAP Solution Manager Authorization Concept This guide contains all information referring to the general concept of security and authorizations for the complete stack for SAP Solution Manager. 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. New Process Documentation Functionality Obsolete Transactions and Authorizations Transactions SOLAR01, SOLAR02, SOLAR_PROJECT_ADMIN are obsolete. All relevant authorizations and roles are obsolete. New roles are delivered SAP_SM_SL_* (process documentation) and SAP_SM_KW_* (Document Management). For more information on conceptual issues, see SAP Solution Manager Authorization Concept Guide for Infrastructure Authorization. Migration (Solution Content Activation) Information For detailed information on the migration of existing projects and solutions to the new process documentation functionality, see section Migration of Projects/Solutions to Process Documentation in this guide. Restructuring of Procedures and Steps in Transaction SOLMAN_SETUP The steps in transaction SOLMAN_SETUP have been restructured for more simplicity. In the course of this restructuring, users are partially reassigned to new steps within the various views/procedures. - All Configuration Users, including SOLMAN_ADMIN are created initially before the start of the procedures, see section Configuration Users - View System Preparation: All required technical users for Solution Manager, without component BW, are created in Step 4 - View Infrastructure Preparation: All required technical users for BW component are created in Step 3 - View Basic Configuration: All dialog users, required for the basic running of Solution Manager are created in Step 4 - View Managed System Configuration: All required managed system users are created - Authorization object SM_SETUP adapted for ability to restrict on Step level. Accordingly, the structure of this guide is adapted. Overviews

Support Package Stacks (Version)	Date	Description
		- Overview on users created in transaction <code>SOLMAN_SETUP</code> Default Users <code>SOLMAN_ADMIN</code>: added roles <code>SAP_SM_RFC_ADMIN</code> (transaction code <code>SM59</code> authorization), Java role <code>SAP_RCA_AGT_ADM</code>, <code>SAP_SOLMAN_SETUP_ADMIN</code>, and <code>SAP_SDCCN_ALL</code> (SDCCN Administration) - New technical user for managed system configuration <code>SM_TECH_ADM</code> - New technical user for Data Suppliers (SLD) <code>SMDS_XXX</code> <code>SM_ADMIN_XXX</code>: added role <code>SAP_SDCCN_ALL</code> (SDCCN Administration) - New technical user for SLD to LMDB notification background job <code>SMSLDN_XXX</code> Solution Data Migration - New section on Guided Procedures for Solution Data Migration Transaktion PFCG - SAP Note 1723881  ⚠ Caution DO NOT APPLY SAP Note 2166856  (API roles: Maintenance of organizational levels) as SAP Solution Manager roles do not use organizational levels.

Support Package Stacks (Version)	Date	Description
SP02	2016 / 07 / 04	Configuration Authorizations and Users - adapted role SAP_SETUP_SYSTEM_PREP (additional transaction for Support Hub Connectivity) Solution Documentation Content Activation - Transaction start ⚠ Caution Start the Solution Documentation Content Activation in the SOLMAN_SETUP transaction. Make sure that the SAP_SMWORK_CONFIG role is assigned to the user who starts the Content Activation. Without this role, the relevant link is not active (under Related Links > Post-Upgrade Activities > Solution Documentation Content Activation). - added additional roles to SMC_MIG user: SAP_SETUP_SYSTEM_PREP_DISP and SAP_SOLDPRO_OLD - adapted roles SAP_SM_*_MIGRATION_72 User SMD_RFC - Adapted role SAP_SOLMANDIAG_E2E User SAPSUPPORT - Adapted role SAP_RCA_DISP User SOLMAN_ADMIN - Adapted role SAP_SM_BASIC_SETTINGS (removed obsolete transactions LMDB_MIG_INST_PROD and SM_LIC_ACT) ⚠ Caution If these transactions are still included in roles, the error message Invalid authorization proposals for... will appear when the system wants to copy. Remove the mentioned transactions or Web Dynpro Applications from the menu tab of the according role. SAP Notes 2257213 (S_TABU_DIS removed for S_TABU_NAM) 2274503 (7.2 SP01 and SP02 Copy of roles in SOLMAN_SETUP not possible (error message))

Support Package Stacks (Version)	Date	Description
---	------	-------------

SP03 2016 / 08 /
15

⚠ Caution

Before you can work correctly with *User Creation* and *Role Management* in transaction SOLMAN_SETUP, please implement SAP Note [2276832](#) and SAP Note [2183425](#).

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](#).

User SOLMAN_ADMIN

- Adapted role SAP_SM_BASIC_SETTINGS as master role, removed from SOLMAN_ADMIN user, see substitute roles.
- New Guided Procedure roles for each individual guided procedure, see according new sections:
 - SAP_SETUP_INFRASTR (Infrastructure Configuration)
 - SAP_SETUP_SYSTEM_PREP (System Preparation)
 - SAP_SETUP_BASIC (Basic Settings)
 - SAP_SETUP_BASIC_APPLOG (Basic Settings Application Log)
 - SAP_SETUP_BASIC_ARCHIVE (Basic Settings Archive)
 - SAP_SETUP_BASIC_S_DEVELOP (Basic Settings Development Authorization)
 - SAP_SETUP_MANAGED (Managed System Configuration)
 - SAP_BC_SDS_CONF_ADMIN (Service Download Configuration for SAP Support Hub/ Rapid Content Delivery)
 - SAP_SM_ESH_ADMIN (Embedded Search access)
 - SAP_SM_SYM_TRANSPORT (Transport Management authorization)

For each of the SAP_SETUP* roles also a display role is shipped.
- adapted role SAP_SM_USER_ADMIN

User SOLMAN_BTC

- Adapted role SAP_SM_BATCH

User SAPSUPPORT

- Adapted role SAP_RCA_DISP

User SM_BW_ACT

- Adapted role SAP_BI_E2E

User SM_COLL_<XXX>

- Adapted documentation

Support Package Stacks (Version)	Date	Description
		- Added new roles for PI rule activation <code>SAP_XI_ALERTCONF*J2EE</code> User SLDDSUSER - Adapted documentation User SM_MSC_XXX - Added role <code>SAP_SM_USER_ADMIN</code> SAP Notes 2250709  (SAP Solution Manager 7.2: Role Corrections) 2220928  Transport Possibility for Custom Roles in Transaction SOLMAN_SETUP For roles in the SAP Solution Manager, it is possible to document them in transports, see section on transaction SOLMAN_SETUP as well as user <code>SOLMAN_ADMIN</code> and <code>SMC_***</code> users. SMC_*** Users - Added to all <code>SAP_*CONF*</code> roles for <code>SMC_***</code> user authorizations for Guided Procedure document OData - Service and authorization object <code>SM_WD_COMP</code> with value <code>AGS_GPA_DOCU</code>

Support Package Stacks (Version)	Date	Description
SP04	2016 / 12 / 19	Configuration User SOLMAN_ADMIN • adapted role SAP_SETUP_MANAGED (see also SAP Note 2250709 ) • adapted roles SAP_SETUP_SYSTEM_PREP* (Support Hub Functionality, for more details see the according section in this guide and the details in menu tab of the role) • removed work center access roles from the user SAP_SMWORK_CHANGE_MAN, SAP_SMWORK_DIAG, SAP_SMWORK_INCIDENT_MAN, SAP_SMWORK_SERVICE_DEV, SAP_SMWORK_SM_ADMIN, SAP_SMWORK_SYS_ADMIN, SAP_SMWORK_TECH_MON • adapted role SAP_SETUP_BASIC for Fiori Launchpad Configuration, Notification Management integration for Early Watch Alert Management, and RCD (Rapid Content Delivery) • New Dialog User for Solution Administration in New template users in Basic Settings Configuration SOLMAN_SETUP for work center usage SAP Solution Manager Administration. • Template User IDs: SA* • For more information, see section on <i>Dialog Users</i>. User SM_TECH_ADM • Added role SAP_SM_USER_ADMIN (due to task: Create Back User) User SAPSUPPORT • Removed S_RFC authorization object in role SAP_RCA_SAT_DIS User SOLMAN_BTC • Adapted role SAP_SM_BATCH with additional values for S_DEVELOP (SAP Fiori LaunchPad integration), and S_TCODE: SPAM (check of SPAM queue) SAP Notes • 2250709  (SAP Solution Manager 7.2: Role Corrections) • 2341241 

Support Package Stacks (Version)	Date	Description
SP05	2017 / 05 / 08	Template Dialog User for Solution Administration in SOLMAN_SETUP and SMUA - Additional Information for Solution Manager Users Administration (SMUA) Security Relevant Activities Flag and Access Point - Activities and steps in transaction SOLMAN_SETUP which are specifically security relevant are flagged and displayed in work center / tile Solution Manager Administration. For more information, see new section Solution Manager Administration Work Center: Security Access Point. GP: System Preparation - Due to transaction STC02, you may require to add role SAP_BC_STC_USER to your configuration user. Check in the Help Text within transaction SOLMAN_SETUP for further information. GP: Embedded Search - The cross - scenario configuration view: Embedded Search is configured by user SOLMAN_ADMIN. For detailed information, see the new section View: Embedded Search in this guide. Migration Procedure and SAP_ALL Profile - The following obsolete authorization objects have been reentered into class SM (Solution Manager): - SM_CM_CSOL - AI_SA_TAB - D_SOLM_ACT - D_SOL_VSBL - SM_ESD_SOL This allows the profile SAP_ALL to contain all relevant authorizations. New Technical User SM_BOC - To allow the display of ITSM Analytics in the Business Objects Cloud (BOC), technical user SM_BOC with associated role SAP_SM_BI_BOC is required in the BW-system. For detailed information, see the new section Technical User SM_BOC in this guide. Technical User SM_BW_READ - Check SAP Note 2391339  Function Modules /SDF/GET_COPY_ROLES and SUSR_LOGIN_CHECK RFC authorizations are missing in BW READ user - Added new role SAP_SM_BI_DVM_READ to run DVM extractors in the BW-system Technical User SM_EFWK - Corrected role SAP_SM_TWB_EXTRACTOR for authorization object S_RFC. See also SAP Note 1570399 

Support Package Stacks (Version)	Date	Description
		Configuration User SOLMAN_ADMIN - Added role SAP_SM_USAGE_LOG for new guided procedure Usage Log - Adapted role SAP_SETUP_SYSTEM_PREP* due to new activities, for instance Check Virus Scan Profile - Adapted role SAP_SETUP_BASIC* - Adapted role SAP_SETUP_MANAGED - Adapted role SAP_SETUP_BASIC_ARCHIVE User SMC_MIG (Migration User) - Adapted role SAP_SM_SL_MIGRATION_72 Obsolete Technical User SMD_AGT The technical user SMD_AGT is obsolete, as agents are authenticated by certificate CN. The user is removed from transaction SOLMAN_SETUP.

Support Package Stacks (Version)	Date	Description
SP06	2017 / 10 / 16	Authorization Objects per Guided Procedure New section on Guided Procedures for Scenarios Technical User SM_EFWK • SAP_SM_EXTRACTOR_CHARM adapted with authorization object SM_CM_FUNC • adapted role SAP_SM_EXTRACTOR_INC with ACO_SUPER for PPM Technical User BI_CALLBACK • adapted role SAP_BI_CALLBACK Technical User SOLMAN_BTC • adapted role SAP_SM_BATCH • Additional information regarding report RCSU_PREREQ_CHECK (authorization check for SOLMAN_BTC in regards to Rapid Content Delivery Application authorization objects CSU_***) Dialog User SAPSUPPORT • adapted role SAP_DBA_DISP Dialog User SAPSERVICE • added role SAP_SM_ESH_DIS Technical User SMB_*** (Back- User) shipped new inactive role SAP_CM_SMAN_BACK which needs to be assigned in case of cCTS usage in Change Request Management and Quality Gate Management Dialog User SOLMAN_ADMIN • added new role SAP_SETUP_SECURITY_REC* for new GP View Additional Security Recommendation. See also new section in this guide View: Additional Security Recommendations • adapted role SAP_SETUP_MANAGED* • adapted role SAP_SETUP_BASIC* (added new authorization object SM_UPLOAD inactively) Dialog User SOLMAN_ADMIN • adapted role SAP_SETUP_BASIC_ARCHIVE • adapted role SAP_SMWORK_CONFIG to display Job Documentation migration procedure • adapted role SAP_SDCCN_*** Dialog User SMC_MIG_*** • additional authorization object SM_BPCA is required, for more information, see section on user SMC_MIG_*** • additional role assignment SAP_SM_SUTMAN_ADMIN required

Support Package Stacks (Version)	Date	Description
---	------	-------------

- **i Note**

In any case, before executing the acitvation, check SAP Note [2381281](#).

Technical User SMDS_***

Changed user name from SMDS_*** to LMDB_DS_***

Transaction SOLMAN_SETUP

It is possible to lock a Guided Procedure using authorization object SM_SETUP, for more informa-
tion, see section on [Transaction SOLMAN_SETUP](#)..

3 Overview

3.1 Overview: All Users Created in Basic Configuration in Transaction SOLMAN_SETUP

Underneath, you find an overview of all users used and created within transaction `SOLMAN_SETUP` (Configuration of SAP Solution Manager).

- SM=Solution Manager System
- MS=Managed Systems
- BW=Business Warehouse
SAP Solution Manager
- SLD - UsersSAP Solution Manager

Technical Users

Solution Manager System

User	User Type	Stack	In System	Created in Guided Procedure View SOLMAN_SETUP	Additional Remarks
SMD_AGT	System	ABAP	SM	System Preparation	To connect Diagnostics Agent to SAP Solution Manager Java Stack
SOLMAN_BTC	System	ABAP	SM	System Preparation	To run all required batch jobs for the Basic Configuration of SAP Solution Manager
SM_EXTERN_WS	System	ABAP	SM	System Preparation	For external Web Service communication between Diagnostics Agent and SAP Solution Manager
SM_INTERN_WS	System	ABAP	SM	System Preparation	For internal Web Service communication between ABAP and Java Stack of SAP Solution Manager
BI_CALLBACK	System	ABAP	SM	Infrastructure Preparation	For reorganization of BW - data in SAP Solution Manager, and Configuration Validation
SM_AMSC	System	ABAP	SM	System Preparation	For Automated Managed System Configuration to run update job

User	User Type	Stack	In System	Created in Guided Procedure View SOLMAN_SETUP	Additional Remarks
SMD_RFC	System	ABAP	SM	System Preparation	To connect ABAP and Java Stack
SM_EFWK	System	ABAP	SM	System Preparation	To run Extractor Resource Manager Step, and in case of local BW - system used to load data in the BW - system
SM_TECH_ADM	System	ABAP	SM	System Preparation	For setting up Solution Manager as Managed System
SMB_*	System	ABAP	SM	Managed System Configuration	For back - communication from managed system to SAP Solution Manager
Guest (Wily)		Java	SM	Managed System Configuration	Built-in user of the Introscope Enterprise Manager

Managed System

User	User Type	Stack	In System	Created in Guided Procedure View SOLMAN_SETUP	Additional Remarks
SMDAGENT_xxx	System	ABAP	MS	Managed System Configuration	To connect Wily Host to managed systems
READ	System	ABAP	MS	Managed System Configuration	To read table information from the managed systems
TMW	System	ABAP	MS	Managed System Configuration	To read table information from the managed systems and schedule batch jobs in the managed systems
SM_COLL_xxx		ABAP/ Java	MS	Managed System Configuration	For data collection in the managed system

BW System

User	User Type	Stack	In System	Created in Guided Procedure View SOLMAN_SETUP	Additional Remarks
SMD_BI_RFC	System	ABAP	BW	Infrastructure Preparation	In case of a remote BW - system used to load data into the BW - system
SM_BW_ADMIN	System	ABAP	BW	Infrastructure Preparation	To initially configure the BW - system

User	User Type	Stack	In System	Created in Guided Procedure View SOLMAN_SETUP	Additional Remarks
SM_BW_ACT	System	ABAP	BW	Infrastructure Preparation	For scenario-specific content activation on the BW - system
SM_BW_XXX	System	ABAP	BW	Infrastructure Preparation	In case of a stand - alone BW - system used to extract data
SM_BOC	System	ABAP	BW	Infrastructure Preparation	Business Objects Cloud

SLD Users

User	User Type	Stack	In System	Created in Guided Procedure View SOLMAN_SETUP	Additional Remarks
SLD_CS_USER	System	ABAP	SLD	Infrastructure Preparation	For collecting system landscape information
SLDAPIUSER	System	ABAP	Central SLD		
SLDDUSER	System	ABAP	SLD		For SLD Data suppliers to write technical system information into SLD

Dialog Users

User	User Type	Stack	In System	Created in Guided Procedure View SOL-MAN_SETUP	Additional Remarks
DDIC	Dialog	ABAP	SM		This is a user required for any SAP System. For any additional information on this user, read the SAP NetWeaver documentation for the relevant SAP Basis release. ⚠ Caution This user usually receives profiles <code>SAP_ALL</code> and <code>SAP_NEW</code>. Therefore, we highly recommend to deactivate the user after configuration and/or change password.
SOLMAN_ADMIN	Dialog	ABAP	SM	Procedure Call (Pop-Up)	Configuration User relevant for SAP Solution Manager to be used for Guided Procedures: System Preparation, Infrastructure Preparation, Basic Configuration, Managed System Configuration, EWA Management
SAPSUPPORT	Dialog	ABAP	SM, BW, Managed System	Basic Settings Configuration, Managed Systems Configuration	Diagnostics display user for SAP Support
SAPSERVICE	Dialog	ABAP	SM, BW	Basic Settings Configuration	Service Delivery user for SAP Support
SM_ADMIN_xxx	Dialog	ABAP	MS	Managed System Configuration	Configuration User for managed systems in ABAP stack and/or Java Stack
J2EE_ADMIN	Dialog	ABAP/Java	MS	Managed System Configuration	For Java Stack administration

User	User Type	Stack	In System	Created in Guided Procedure View SOLMAN_SETUP	Additional Remarks
SA_ADM_XXX	>Dialog	ABAP	SM	Basic Settings Configuration	SAP Solution Manager Administration

3.2 Overview: Solution Manager Configuration

This section gives you an overview on which functions are configured using transactions `SOLMAN_SETUP`:

- Requirements Management
- Project Management
- Process Management
- Custom Code Management
- Test Suite (CBTA, SAP TAO, PTM, BPCA)
- Change Control Management (QGM, ChaRM)
- IT Service Management
- Application Operation (all sub-scenarios for Technical Monitoring, DRM, EWA Management, SAM, IT Task Management, Job Management)
- Business Process Operation
- Data Volume Management
- Value Management Dashboard

For some of the scenarios, sub-scenarios are defined.

All other scenarios can be configured using transaction `SPRO`.

3.3 Overview: Where Used - Solution Manager Technical RFC - Users per Scenario (READ, TMW, TRUSTED)

This section gives you an overview about which users are necessary pro scenario. An `x` in a column determines whether the user is necessary for this scenario. Detailed information about the RFC - destination used can be found in the according scenario - specific guides.

The table displays which scenario is using `READ`, `TMW`, or `Trusted` RFCs. In case of `READ` RFC, we recommend to create this RFC for any of your scenarios.

For `Trusted` RFC, please see also the comments to any specifics for the according function, which allow to remove `Trusted` RFCs under specific circumstances and contexts.

Scenarios

- Implementation = A

- Test Suite= C
- Business Process Change Analyzer = D
- Incident Management = E
- Change Request Management = F
- Quality Gate Management = G
- Technical Monitoring = H
- Business Process Operation = I
- Job Management = J
- SAP Engagement and Service Delivery = K
- Technical Administration = L
- Data Volume Management = M
- Root Cause Analysis = N
- SAP Fiori (Central Hub) = O
- Custom Code Lyfe - Cycle Management = P
- IT Task Inbox and Guided Procedures = R

User and/or RFC	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R
READ RFC	(X) ⁹	X	X	X	(X) ⁹	(X) ⁹	X	(X) ⁹	X	X	X	X	X		(X) ⁹	
TMW RFC	X ¹				X ²	X		X							X	
BACK RFC			X	X	X					X						
TRUSTED RFC	X ⁴		X ⁸		X ⁵		X ¹¹	X ⁶				X ⁸		X		X ¹⁰
SMD_RFC User							X ⁷						X			

¹ for CDMC

² for creating and releasing of transport request

⁴ for Customizing Distribution; Customizing Synchronization, BC-SetsCDMC

⁵ for Task List Framework

⁶ for CDC, value help for BP Monitoring

⁷ Java - related

⁸ Alternatively [Login RFC - Connection](#) can be used

⁹ if a TMW connection is in place, the TMW connection user has all required authorizations as the READ connection user plus batch and write authorizations. If you have a TMW connection in place, you do not necessarily need a READ connection.

¹⁰ in case of automatic activities (only in customer owned settings)

¹¹ for Message Flow Monitoring

3.4 Overview: All End-Users and Business Partners per SOLMAN_SETUP Scenario

For all scenarios, you need to create users in your systems. For some scenarios, you may as well need to create Business Partners related to your users. The following lists give an overview of scenarios that require users in the Solution Manager system, the managed systems, the BW-system, and functions that require business partner users in the Solution Manager system:

Scenario	User in Solution Manager	User in Managed System	User in BW System	Business Partner Required
Implementation	X	X (Customizing Distribution)		X
Test Management	X	X (Test Execution)		
Incident Management	X			X
Technical Administration	X	X		
Application Monitoring	X		X	X
Business Process Operation	X		X	
Change Request Management	X	X		X
Quality Gate Management	X			X
Root Cause Analysis	X	X	X	
SAP Engagement and Service Delivery	X		X (Issue Management)	
Job Scheduling Management	X		X	
LMDB	X			X

4 System Landscape

4.1 Technical System Landscape

Use

SAP Solution Manager is based on `AS ABAP` and `AS Java`. To use SAP Solution Manager you need either client: `SAP GUI`, Web Browser or SAP NetWeaver Business Client (`NWBC`) (for work center functionality). Communication with other systems is via `RFC` technology and web services.

You find explanations for scenario - specific technical system landscapes within each scenario - specific guide.

More Information

For a detailed view of the overall system architecture of SAP Solution Manager, see master guide for SAP Solution Manager in the Service Marketplace: <http://service.sap.com/instguides>   [SAP Components](#)  [SAP Solution Manager <current release>](#). .

5 Specific Security Settings

5.1 Solution Manager Administration Work Center: Security Access Point

SAP Solution Manager Administration Work Center

The Solution Manager Administration work center contains views which are relevant for the administration of the Solution Manager system. Here, the views [Security](#) and [Users](#) are mentioned in detail as they refer to security of your system.

You can access the tiles for it, using transaction `SM_WORKCENTER` and the Fiori Launchpad.

View: Security Critical Activities

As of SAP Solution Manager Release 7.2 SP05, steps and activities with the basic configuration of `SOLMAN_SETUP` that are relevant for overall security of your system, are flagged as security- relevant. You can display all of them in one view within the SAP Solution Manager Administration work center under the heading of [Security](#). More information on specific topics of these steps can be found in the following sections in this guide.

View: Users

The view Users gives you access to the [Solution Manager User Administration \(SMUA\)](#). This tool is described in detail in one of the following sections in this guide.

5.2 Technical System Landscape

The following sections give you an overview of the technical system landscape of your system landscape setup and Root Cause Analysis, focusing on various aspects:

- connection between SAP Solution Manager and its managed systems after the setup
- BW - related infrastructure according to all possible options after the setup
- LMDB/SLD infrastructure after the setup

SAP Solution Manager and Managed Systems

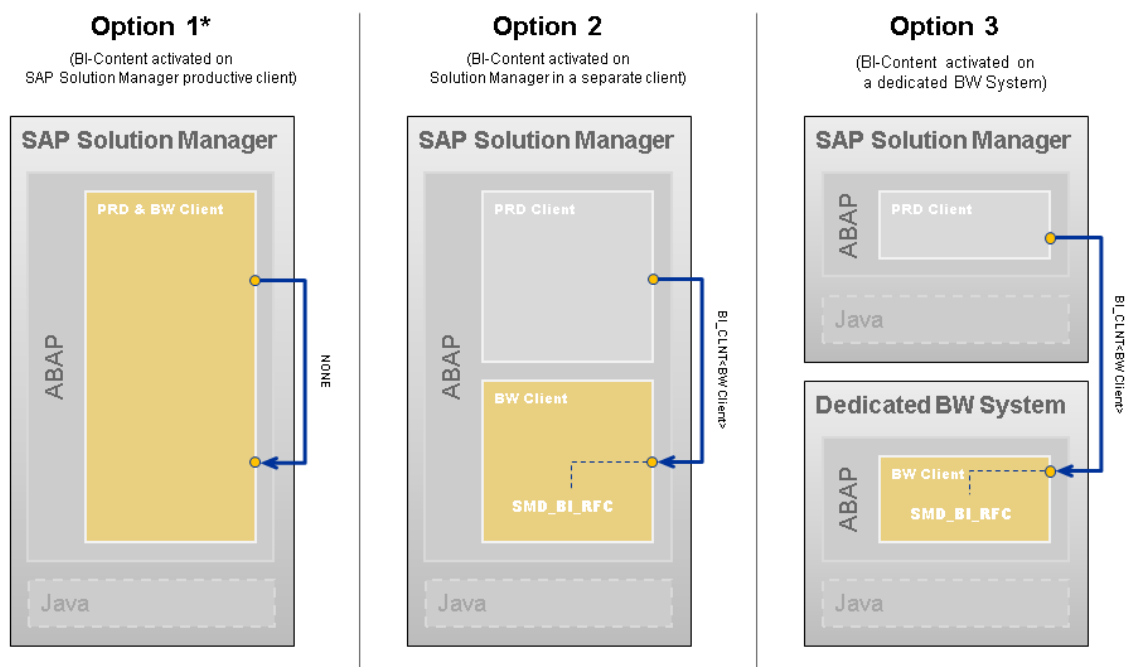
The following graphic displays the technical setup after you have executed the basic configuration of SAP Solution Manager and attached the managed systems to it. The attachment of managed systems includes the RFC generation as well as the integration for Root Cause Analysis.

The overall system landscape includes your SAP Solution Manager double stack system, your managed systems, and SAP. SAP Solution Manager has several connections to SAP, and to your managed systems. When setting up your system landscape, you set up all relevant connections for your scenario. All required connections need technical users, which require specific authorizations.

To run Root Cause Analysis, you need to implement additional components in SAP Solution Manager (for instance *Introscope Enterprise Manager*) as well as the managed systems (for instance Diagnostics Agent)

BW System/Client

The following graphic displays the integration of SAP Solution Manager with BW after the setup of SAP Solution Manager is done. During the setup, you have to choose whether you run the standard scenario for BW, or the remote scenario. Options 2 and 3 display the remote scenario setup.



* SAP standard recommendation is to activate BI-Content on SAP Solution Manager productive client. Please note that RFC destination BI_CLINT<BW Client> and user account SMD_BI_RFC not required in this case.

BI-setup after the automated basic settings configuration (transaction SOLMAN_SETUP)

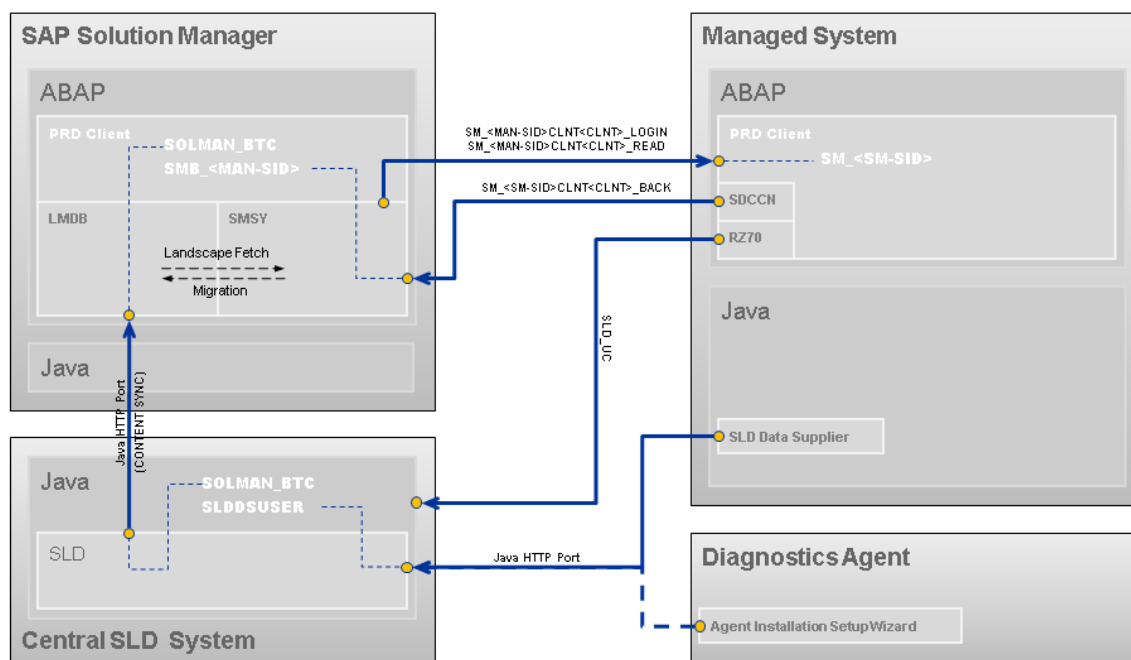
As outlined in the core Security Guide, we differentiate between three possible options to use BW with SAP Solution Manager. According to which option you choose, the BW setup differs in which connections and technical users are required.

- Option 1: Standard Scenario
- Option 2: Remote BW, whereas the system is SAP Solution Manager, but not the productive client
- Option 3: Remote BW, whereas the system is a dedicated BW system

You find more information on which connections are used and which technical users are required for BW - setup in the individual scenario-specific guides.

System Landscape Repository

The following graphic gives you an overview of the technical landscape setup focusing on the new system repository, the **Landscape Management Data Base (LMDB)**. The LMDB is integrated with the **System Landscape Directory (SLD)**. You find more information about this integration in the Online Documentation for LMDB.

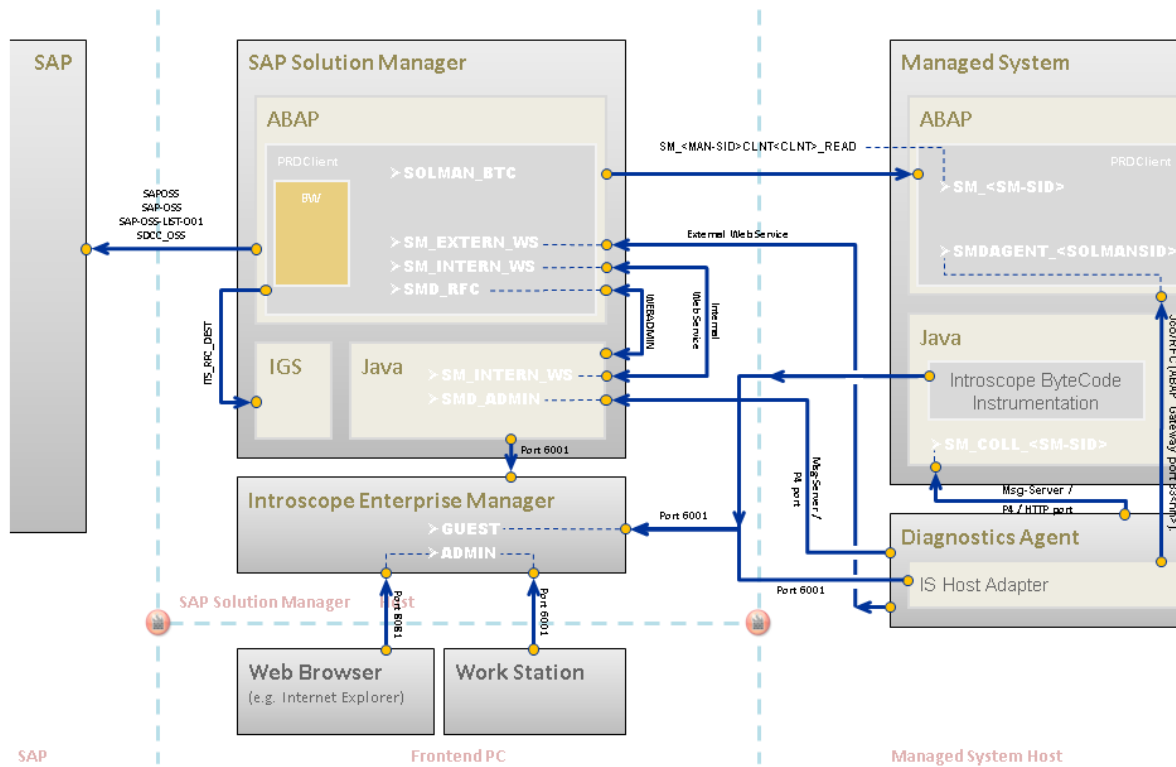


If your central SLD release is lower than 7.1, you do not require User SLDCSUSER.

SLD/LMDB landscape configuration after the automated basic settings configuration (transaction SOLMAN_SETUP)

Root Cause Analysis

The following graphic gives you an overview of the technical landscape setup focusing on the scenario Root Cause Analysis.



RCA system landscape

5.3 Communication Channels and Destinations

The tables below show the communication channels and destinations created during system landscape setup (transaction `SOLMAN_SETUP`)

Communication Channels

⚠ Caution

At the beginning of 2020, new connections to SAP's support backbone are in place. The connections that are required depend on the `SAP_BASIS` release and the kind of procedure you choose for downloading SAP Notes.

General Information

For general references, check the following links:

- [Landing page](#)
- [SAP Solution Manager page](#)

Configuration Procedure: Step by Step Checklist

For a Step-by-Step procedure to configure the new connectivity, please see the Checklist for the current SP <https://support.sap.com/en/alm/solution-manager/sap-support-backbone-update/backbone-update-checklists.html> :

RFC Destination for SAP Notes

Procedure Recommendations for Managed Systems Without an SAP Solution Manager Connection

SAP Basis Release	Behavior and Procedure Recommendations as of January 1, 2020
7.00 – 7.31	SAP <code>SNOTE</code> works with the technical communication user. For more information about this user, see section <i>Technical Communication User</i> in this chapter.
Lower than 7.40 SP19	SAP <code>SNOTE</code> works with the technical communication user. For more information about this user, see section <i>Technical Communication User</i> in this chapter. Note 1. Check TCI for NW task list SAP Note 2738426. 2. Check TCI for SAP Download SAP Note 2576306. 3. In the SAP Download Note all follow up information is described. Check the attached PDF, which describes further manual steps.
7.40 SP20 and above	SAP <code>SNOTE</code> are obsolete. → Remember Enable one of the following procedures: • HTTP protocol HTTP is required by the RFC connections <code>SAP-SUPPORT_PORTAL</code> and <code>SAP-SUPPORT_NOTE_DOWNLOAD</code>. The new RFC <code>SAP-SUPPORT_NOTE_DOWNLOAD</code> is required to download SAP Notes. It is of connection type G. • Download Service

→ Tip

Refer to the PDF document in SAP Note [2508268](#) to learn more about the various procedures available for downloads.

SAP Backbone Connections for Applications Running on SAP Solution Manager

New Channels: Overview

	Asynchronous (Support Backbone) Connection	SAP-SUPPORT_PORTAL	SAP-SUPPORT_PARCELBOX
Type of connection	Asynchronous HTTP connection	Synchronous HTTP connection	Synchronous HTTP connection
Creation	Via logical port for SOAP-based Web service communication <code>LP_SISE_SUPPORTHUB</code>. The logical ports are created inside the consumer proxies as listed at SOAP Runtime Consumer Proxies for Support Backbone Connection [page 31]. The logical ports are created during configuration using <code>SOLMAN_SETUP</code> (if your Support Package is lower than SP08 or if you are a VAR service provider, this must be done manually). Note In the case of VAR service provider conversion, a number of logical ports are created within one consumer proxy.	Transaction <code>SM59</code>: RFC destination of connection type H to SAP Support Portal	HTTP connections to external server of connection type G to SAP Support Documents
VAR service provider conversion	<code>SM_SP_<customer number>_H</code>	<code>SM_SP_<customer number>_H</code>	<code>SM_SP_<customer number>_G</code>

	Asynchronous (Support Backbone) Connection	SAP-SUPPORT_PORTAL	SAP-SUPPORT_PARCELBOX
Specific KBAs	2665368 – No logical port 'LP_SISE_SUPPORTHUB' exists for the proxy class CO_SISEHUB_MI_O_S_SHB_LIST in jobs to SAP's back-end systems 2525987 – Internal Server Error, SoapFaultCode:5 Server Error or Timeout error (ICM_HTTP_TIMEOUT) in jobs using the asynchronous channel	2489770 – Error during Upload to SAP SUPPORT PORTAL 2289984 – Configure the synchronous communication channel	2716729 – SAP backbone connectivity - SAP Parcel Box configuration

SOAP Runtime Consumer Proxies for Support Backbone Connection

Name	Type	Description
CO_SISEHUB_MI_O_AS_PUT_EXTERNA	Asynchronous	Send message to SAP's support backbone
CO_SISEHUB_MI_O_S_SHB_GET_EX	Synchronous	Get postbox entries from SAP's support backbone
CO_SISEHUB_MI_O_S_SHB_LIST	Synchronous	Query Directory of postbox entries from SAP's support backbone
CO_SISEHUB_MI_O_S_SHB_REMOVE	Synchronous	Remove postbox entries from SAP's support backbone

KBAs for Service Provider (VAR) Connection Conversions

- [2698540](#) – REFRESH_ADMIN_DATA_FROM_SUPPORT fails with message "Multi Customer Scenario detected but no specific destination found"
- [2638425](#) – Managing customers assigned to different VARs in one Solution Manager 7.2 system
- [2499200](#) – Setting steps for Multi-customer scenario in Solution Manager 7.2 SP05 or higher
- [2713253](#) – SAP connectivity configuration for VAR and Multi-Customer scenario in Solution Manager 7.2 as of SPS05
- [2651054](#) – Support Hub configuration for VAR and Multi Customer scenario in Solution Manager 7.2 SP07
- [2716879](#) – Information on how to set up the connection in a VAR environment
- [2182476](#) – Ensure the background job REFRESH_ADMIN_DATA_FROM_SUPPORT runs properly

Further Information Sources

- [Questions and Answers](#)
- [Troubleshooting](#)

Background Jobs and Technical User SOLMAN_BTC

Technical user SOLMAN_BTC runs all relevant background jobs for the connection to SAP.

i Note

To run the background jobs successfully, you need to update role `SAP_SM_BATCH` to the latest version, at least `SP09`. The latest version can be found in SAP Note [2250709](#).

SAP Solution Manager-Specific Functions Using SAP Channels

The following numbers represent the individual RFC connections in the tables below:

1. = **Synchronous** `SAP-SUPPORT_PORTAL`
2. = **Asynchronous (Support Backbone) Connection**
3. = **Parcelbox** `SAP-SUPPORT_PARCELBOX`

BW Data Exchange

Some BW reports need data from SAP and some reports in SAP need data from the SAP Solution Manager system. SAP Solution Manager BW Data Exchange can be used to exchange this data. The BW Data Exchange is a generic framework. The data flow depends on the business scenarios that use this framework. Therefore, the data varies between different Support Packages. This framework is used for:

- Customer Usage Provision (CUP)
- SAP Solution Manager Usage

Running Since SP	1	2	3	Additional Information
SP01		x (in both directions)		Additional setup requirements: 1. EFWK Framework and BW system as data provider 2. CUP Data Extraction Setup in transaction <code>SOLMAN_SETUP</code> under Basic Configuration > Configure Basic Functions > Enable System Data Measurement. 3. SAP Solution Manager Usage Data Extraction Setup in transaction <code>SOLMAN_SETUP</code> under Basic Configuration > Configure Basic Functions > Enable Solution Manager Usage Data. Log information in transaction <code>SLG1</code>: • Object: <code>AGSESR</code> • Subobjects: <code>SOLMAN2SAP</code> and <code>SAP2SOLMAN</code>

Rapid Content Delivery (RCD)

Running Since SP	1	2	3	Additional Information
SP03	x for Notifications	x for getting URL and executing download		For additional setup requirements, troubleshooting, and so on, see SAP Note 269246 . You can manually download files from the Support Portal and upload files using report <code>RCSU_MANUAL_UPLOAD</code> .

Remote Service Connection – Transaction `SOLMAN_CONNECT`

- Send and refresh setup data (system information and system number) and connection status to SAP
- Receive connection setup data from SAP
- Upload system data to SAP (system setup data and system constellations)
- Send system relationship to SAP (managed system list)
- Refresh read data (send and receive customer number; send installation number, system number, and last synchronization; and receive system license data) to SAP
- Send installation number

! Restriction

For all managed systems that are directly connected to SAP, the `SAP_OSS` RFC is still used for ST-PI 2008 (with kernel release <742, which allows for remote HTTPS connections via Web calls).

Running Since SP	1	2	3	Additional Information
SP05	x for sending data for a single system	x for background jobs that send or receive data due to high volume of data		Additional setup requirements: - Schedule job in transaction <code>SOLMAN_SETUP</code> under Basic Settings > Schedule Jobs > SM:AGS_SISE_SUPHUB_OUTBOX_PROCES. - Assign S-user in transaction <code>AISUSER</code>. For information on authorizations for this user, see section S-User in transaction AISUSER. For information on personal data security, see the Security Optimization Guide section on Data Privacy Measures. In case the new connectivity cannot be used for this application, you can maintaining the remote connections on SAP Support Portal directly. Important SAP Notes as of SP08: 2734568 2681155 2706775 2582603 2674422 2570080 2671142 2522251 2508210 For troubleshooting, see SAP Note 2598551.

Service Data Control Center Framework

- [Service Definition \(SD\) Refresh](#)
SDs are pulled from SAP's support backbone on demand.
- Sending Service Data
Data that is collected by [SDCCN](#) is sent to SAP's support backbone. The data size ranges from 5 MB to 100 MB or more, with a typical size of 10 MB.

→ Tip

For information about how to set up the connection in a VAR environment, see SAP Note [2716879](#).

Running Since	SP 1	2	3	Additional Information
ST-PI 7.40 SP09 and ST-PI 2008_1_7XX SP19	x for ST-PI 740 (Service Definition Refresh)		x for ST-PI 740 (Service Data)	- Applies to managed systems and SAP Solution Manager - Downport to ST-PI 7.40 SP04 and ST-PI 2008_1_7XX SP09 Additional Setup Information for Software Component version ST-PI 740: - KBA 2289984 (manually creating connection to the support backbone) - KBA 2716729 (creating the SAP's support parcelbox)

⚠ Caution

Common issues are described in SAP Notes [2664268](#) and [2690656](#).

→ Tip

For more information on usage in a high security environment, see SAP Note [727998](#).

If your security policy prevents a connection to SAP, EarlyWatch Alert (EWA) and similar services can be processed in the SAP Solution Manager system. You can forward EarlyWatch Alert downloads to SAP using SAP Solution Manager (if SAP Solution Manager can communicate with SAP's support backbone). Forwarding the EWA to SAP must be configured in SAP Solution Manager transaction SOLMAN_SETUP.

System Recommendations

"System Recommendations" prepares application requests from SAP Solution Manager and sends the request to SAP's support backbone for calculation. The support backbone then sends the calculation results back to the SAP Solution Manager system.

Running Since	SP 1	2	3	Additional Information
SP05	x			A workaround is not available.

i Note

For additional information, see [System Recommendations](#).

Scope and Effort Analyzer

Running Since	SP 1	2	3	Additional Information
SP05	x			A workaround is not available.

License Management

Running Since SP	1	2	3	Additional Information
SP05		x		If you cannot connect to SAP, you can install licenses and maintenance certificates manually using transactions <code>SLICENSE</code> and <code>NWA</code> .

Application Component Hierarchy

The SAP Application Component Hierarchy is updated regularly from SAP's support backbone.

Running Since SP	1	2	3	Additional Information
SP01		x		Application Component Hierarchy data is transferred from SAP's support backbone by a scheduled job in the background.

SAP Engagement and Service Delivery

SAP Engagement and Service Delivery comprises a number of applications, which are listed below. For all applications, you can configure the [Engagement and Service Delivery](#) scenario in transaction `SOLMAN_SETUP`.

! Restriction

Without a connection to SAP, data cannot be exchanged. As a workaround, you can create service sessions locally via the SAP Fiori Launchpad tiles [My Sessions](#) and [Active Sessions](#).

Application Description	Running Since SP	1	2
Send Service Order	SP05		x
Send Session Notification	SP03		x
Send Quality Gate	SP03		x
Send Support Request	SP03		x
Send Top Issue	SP03		x
Send PPMS Data from SAP's Support Backbone to SAP Solution Manager	SP05		x
Send Ruleset Data from SAP's Support Backbone to SAP Solution Manager	SP05		x

Communication RFC Destinations

RFC Connections from SAP Solution Manager to Managed Systems

i Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems). If not specified differently, passwords are customer - specific.

RFC Destination Name	Target Host Name	System		Logon User
		Num-ber	Logon Client	
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	Cus-tomer-specific	Customer-specific
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>
SM_<SID>CLNT<Client>_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific
SM_<SID>CLNT<Client>_TMW (ABAP connection)	Managed System	System-specific	System-specific	Default user: SMTW<SID> of Solution Manager system>

RFC Connection from Managed System to SAP Solution Manager

RFC Destination Name	Target Host Name	System Num-ber	Logon	
			Client	User
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	SMB_<managed system ID>

The role `SAP_SOLMAN_BACK` is assigned to the RFC User. The role authorizations are security-critical in general, as this RFC - connection allows a user from a managed system to connect to the SAP Solution Manager.

→ Recommendation

Check SAP Note [2257213](#) .

Internet Graphics Server (IGS) RFC Connection

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

RFC Connection for BW integration

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
SAP_BILO	remote BW - system (source: SAP Solution Manager)	RFC trusted	Dialog user	Used to read data from remote BW for BI - Reporting created during SOLMAN_SETUP
SAP_DABU	Solution Manager productive client (source: BW - System)	RFC trusted	Dialog user	Used to send data from remote BW for BI - Reporting created during SOLMAN_SETUP
BI_CLNT<BWclient>	remote BW - system (source: SAP Solution Manager)	RFC trusted	Dialog User	
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client		Dialog User	
<SolutionManagerSID>CLNT <SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client		BI_CALLBACK (customer specific)	in transaction SOLMAN_SETUP

SLD - LMDB Destination

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
SLD_UC (Unicode) - analogous to SLD_NUC (Non-Unicode)	System Landscape Directory (SLD)	RFC destination (type T; Registered Server program: SLD_UC) Java Connector (JCo)	Gateway	Used by the SLD data supplier (ABAP) configured in transaction RZ70 of the managed system

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
Connection for SLD data supplier (Java stack)	System Landscape Directory (SLD) (source: managed system Java stack)	Java HTTP(s) port (for instance 5xx00) or web dispatcher	SLDDSUSER	Used by the SLD data supplier (Java) configured in the Visual Administrator or NetWeaver Administrator of the managed system
LMDB_SyncDest<n>	System Landscape Directory (SLD), (source: SAP Solution Manager)	RFC destination (type G; Java HTTP[s] port, e.g. 5xx00, or web dispatcher)	User with read permission (for instance: SLD_CS_USER)	Used for content synchronization created in transaction SOLMAN_SETUP or the SAP Solution Manager Configuration work center

Connections relevant for Root Cause Analysis (also relevant for SLD-LMDB data flow)

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
WEBADMIN	SAP Solution Manager (ABAP Stack), (source: SAP Solution Manager (Java Stack))	Java Connector (JCo)	SMD_(BI)_RFC	WEBADMIN is an internal connection in SAP Solution Manager used for the communication between ABAP and Java.
WEBADMIN	SAP Solution Manager (Java Stack), (source: SAP Solution Manager (ABAP Stack))	RFC destination (type T; Registered Server program: WEBADMIN)	Gateway	
Connection for Diagnostics Agent to SAP Solution Manager	SAP Solution Manager, (source: Diagnostics Agent (on Managed System))	P4 port / Message Server port	SMD_AGT / Password authentication	Used for outside discovery; created in transaction SOLMAN_SETUP or the SAP Solution Manager Configuration work center

Communication RFC Destinations

RFC Connections from SAP Solution Manager to Managed Systems

i Note

All mentioned RFC - destinations are automatically created via transaction `SOLMAN_SETUP` (view: managed systems). If not specified differently, passwords are customer - specific.

RFC Destination Name	Target Host Name	System		Logon User
		Num-ber	Logon Client	
SM_<SID>CLNT<Client>_LOGIN (ABAP connection)	Managed System	System-specific	Cus-tomer-specific	Customer-specific
SM_<SID>CLNT<Client>_READ (ABAP connection)	Managed System	System-specific	System-specific	Default user: SM_<SID> of Solution Manager system>
SM_<SID>CLNT<Client>_TRUSTED (ABAP connection)	Managed System	System-specific	System-specific	Customer-specific
SM_<SID>CLNT<Client>_TMW (ABAP connection)	Managed System	System-specific	System-specific	Default user: SMTW<SID> of Solution Manager system>

RFC Connection from Managed System to SAP Solution Manager

RFC Destination Name	Target Host Name	System Num-ber	Logon	
			Client	User
SM_<SID>CLNT<Client>_BACK (ABAP connection)	Solution Manager System	System-specific	System-specific	SMB_<managed system ID>

The role `SAP_SOLMAN_BACK` is assigned to the RFC User. The role authorizations are security- critical in general, as this RFC - connection allows a user from a managed system to connect to the SAP Solution Manager.

→ Recommendation

Check SAP Note [2257213](#) .

Internet Graphics Server (IGS) RFC Connection

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

RFC Connection for BW integration

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
SAP_BILO	remote BW - system (source: SAP Solution Manager)	RFC trusted	Dialog user	Used to read data from remote BW for BI - Reporting created during SOLMAN_SETUP
SAP_DABU	Solution Manager productive client (source: BW - System)	RFC trusted	Dialog user	Used to send data from remote BW for BI - Reporting created during SOLMAN_SETUP
BI_CLNT<BWclient>	remote BW - system (source: SAP Solution Manager)	RFC trusted	Dialog User	
NONE, if BW - reporting is realized in a BW - standard scenario, for content activation	Solution Manager productive client		Dialog User	
<SolutionManagerSID>CLNT <SolutionManager-ProductiveClient> BI-Callback RFC for reorganization of data and configuration validation	Solution Manager productive client		BI_CALLBACK (customer specific)	in transaction SOLMAN_SETUP

SLD - LMDB Destination

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
SLD_UC (Unicode) - analogous to SLD_NUC (Non-Unicode)	System Landscape Directory (SLD)	RFC destination (type T; Registered Server program: SLD_UC) Java Connector (JCo)	Gateway	Used by the SLD data supplier (ABAP) configured in transaction RZ70 of the managed system

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
Connection for SLD data supplier (Java stack)	System Landscape Directory (SLD) (source: managed system Java stack)	Java HTTP(s) port (for instance 5xx00) or web dispatcher	SLDDSUSER	Used by the SLD data supplier (Java) configured in the Visual Administrator or NetWeaver Administrator of the managed system
LMDB_SyncDest<n>	System Landscape Directory (SLD), (source: SAP Solution Manager)	RFC destination (type G; Java HTTP[s] port, e.g. 5xx00, or web dispatcher)	User with read permission (for instance: SLD_CS_USER)	Used for content synchronization created in transaction SOLMAN_SETUP or the SAP Solution Manager Configuration work center

Connections relevant for Root Cause Analysis (also relevant for SLD-LMDB data flow)

RFC Destination Name	Target Host Name	Connection Type	Authentication	Remark
WEBADMIN	SAP Solution Manager (ABAP Stack), (source: SAP Solution Manager (Java Stack))	Java Connector (JCo)	SMD_ (BI) _RFC	WEBADMIN is an internal connection in SAP Solution Manager used for the communication between ABAP and Java.
WEBADMIN	SAP Solution Manager (Java Stack), (source: SAP Solution Manager (ABAP Stack))	RFC destination (type T; Registered Server program: WEBADMIN)	Gateway	
Connection for Diagnostics Agent to SAP Solution Manager	SAP Solution Manager, (source: Diagnostics Agent (on Managed System))	P4 port / Message Server port	SMD_AGT / Password authentication	Used for outside discovery; created in transaction SOLMAN_SETUP or the SAP Solution Manager Configuration work center

Related Information

<https://support.sap.com/en/alm/solution-manager/sap-support-backbone-update/backbone-update-checklists.html>

5.4 Required TCP/IP Ports

Use

The following ports have to be opened up in your fire wall, prior to installation. The connections listed in the below section Ports for Communication to SAP Solution Manager, allow for example Root Cause Analysis users to connect to the Java managed system to access so called *Expert Tools* (System Information page, and so on). This access is normally performed using the credentials of the `SAPSUPPORT` read-only user. Generally speaking, the tables below allow to understand also that the `Non-RFC` type connections (`HTTP`, `P4` and other `TCP/IP`) are established by the Diagnostics Agent, running on the (productive) managed system host to connect either locally to the managed system itself, or to the Solution Manager System and the Introscope Enterprise Manager Server. Note that this chapter does not address the classical `RFC` connectivity, which is setup between the Solution Manager System and the `ABAP` managed systems.

Note

Only in case you have a business requirement to register the Diagnostics Agents in a central SLD, pay attention to the following. For further details, see SAP Note [1365123](#).

Ports for Communication to SAP Solution Manager

Ports for Communication to SAP Solution Manager

Established Connection		Service on Destination Host	
From Hosts/Source Host	To Host/Destination Host	(Protocol)	Format (example)
SAP Support	All Solution Manager Instances	J2EE engine (HTTP)	5<instance no.>00 (50100)
SAP Support	All Solution Manager Instances	ITS (HTTP)	80<instance no.> (8000)
SAP Support	All Solution Manager Instances	Introscope Manager (HTTP)	Default: 8081
Diagnostics Server	All Solution Manager Instances	IGS (HTTP)	4<instance no.>80 (40180)

Established Connection

From Hosts/Source Host	To Host/Destination Host	Service on Destination Host	
		(Protocol)	Format (example)
Diagnostics Agent (managed system Host)	All Solution Manager Instances	J2EE engine (P4)	5<instance no.>04 (50104)
Diagnostics Agent (managed system Host)	Solution Manager Java Message Server	Message Server (HTTP)	81<instance no.> (8101)
Diagnostics Agent (managed system Host)	Relevant Introscope Enterprise Manager Host	Introscope Enterprise Manager (TCP/IP)	Default: 6001

Consider the following lines when operating a SAP Solution Manager system, setup with a Web Dispatcher, especially when having multiple dual-stack instances.

From Host/Source Host	To Hosts/Destination Hosts	Service on Destination Hosts (Protocol)	Format (example)
All Solution Manager Instances	Web Dispatcher	Web Service (HTTP)	(80)
Diagnostics Agent (managed system host)	Web Dispatcher	Web Service (HTTP)	(80)
Web Dispatcher (forwarded HTTP requests)	All Solution Manager Instances	Web Service via ICM (HTTP)	80<instance no.> (8000)

Consider the following line when operating a Solution Manager system, having one single dual-stack instance and setup without a Web Dispatcher

From Host/Source Host	To Hosts/Destination Hosts	Service on Destination Hosts (Protocol)	Format (example)
Diagnostics Agent (managed system host)	Solution Manager Single Instance	Web Service via ICM (HTTP)	80<instance no.> (8000)

Additional communications performed LOCALLY on Solution Manager host (requiring in general no special security settings)

Consider also following line when operating a SAP Solution Manager system, having one single dual-stack instance and setup without a Web Dispatcher.

From Host/Source Host	To Hosts/Destination Hosts	Service on Destination Hosts (Protocol)	Format (example)
Solution Manager single Instance (ABAP stack)	Solution Manager Single Instance (Java Stack and ABAP stack)	Web Service via ICM (HTTP)	80<instance no.>(8000)

Ports for Communication with Managed Systems

Ports for Communication with Managed Systems

Established Connection

From Host/Source Host	To Hosts/Destination Hosts	Service on Destination Hosts (Protocol)	Format (example)
SAP Support	All managed systems	J2EE engine (HTTP)	5<instance no.>00 (50200)
SAP Support	All managed systems	ITS (HTTP)	80<instance no.> (8000)

Additional communications are performed **LOCALLY** on managed system hosts (requiring in general no special security settings)

From Host/Source Host	To Hosts/Destination Hosts	Service on Destination Hosts (Protocol)	Format (example)
Diagnostics Agent (managed system host)	Associated managed systems	J2EE engine (P4)	5<instance no.>04 (50204)
Diagnostics Agent (managed system host)	Associated managed systems	Java Message Server (internal port)	36<instance no.> (3601) or 39<instance no.> (3901)
Diagnostics Agent (managed system host)	Associated SAP Host Agent (applies when using SAP Solution Manager 7.0 EhP1 SP20 and higher, and Diagnostics Agents 7.11 and higher)	SAP Host Agent Web Service (HTTP)	1128 (standard)

More Information

on the current list of ports used by SAP, in the SAP Service Marketplace: <http://service.sap.com/security>

► [Infrastructure Security](#) ► [TCP/IP Ports Used by SAP Applications](#) ►

5.5 Securing Attachments

→ Recommendation

We recommend to use ABAP Virus Scanning Interface (VSI) for virus scans of attachments. You will find more information about the configuration of the virus scan interface in the SAP library under SAP NetWeaver -> Security -> System Security -> Virus Scan Interface.

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

See SAP Note [1693981](#) (Unauthorized modification of displayed content)

In all applications the following default VSI profiles are used:

- /SCET/GUI_UPLOAD
- /SIHTTP/HTTP_UPLOAD

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

→ Recommendation

We recommend configuring VSI to exclude both executable (.exe) and HTML files from being uploaded. Note, that in case the VSI is active, but you have no Third Party Virus Scan in place, the system will not upload any attachments by default. If you do not set the VSI active, the system will allow you to upload attachments. As this is highly insecure, we strongly recommend to use a Virus Scan Product for uploading attachments.

5.6 Log Entries, Data Storage, and PANKS (NOTE Search)

Use

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

See the [Auditing and Logging](#) on the Service Marketplace at: <http://help.sap.com>  [Search Documentation](#) , search for [Auditing and Logging](#).

In transaction SOLMAN_SETUP, the system displays current log entries. These log entries can be:

- exported
- downloaded to be archived and subsequently removed

Log Entries

Export of Log Entries in User Interface Log

The activity to [Export](#) any logs in the User Interface of transaction `SOLMAN_SETUP` (buttons [Export To HTML](#) and [Send By Email](#)) is protected by authorization object `SM_SETUP` with `ACTVT 61` (Export).

i Note

Due to the criticality of this activity it is not actively shipped in any Solution Manager role. You need to add the activity when you want to export logs.

Archive of Log Entries

You can archive logs using the Solution Manager Administration in transaction `SOLMAN_SETUP_ADMIN`. Then logs are no longer visible in `SOLMAN_SETUP` User Interface. If you assign the delete permissions, you can delete archived logs.

Data Storage

All data is stored in the database.

PANKS (SAP Note Search within the Log)

Within the log for every `SOLMAN_SETUP` step, you have the possibility to search for SAP Notes connected with any errors occurring for the configuration step. The PANKS search connects to the SAP Backbone using RFC `SAPOSS`.

More Information

Data Storage to database in general is described in the SAP NetWeaver Installation Guides.

6 User Administration/Authentication and Role Adjustment

6.1 Introduction

The SAP Solution Manager uses the User Management and authentication mechanisms provided by the SAP NetWeaver platform, in particular the SAP NetWeaver ABAP. It also has its specific User Management tools:

- User Creation Tool in transaction `SOLMAN_SETUP`
- Solution Manager Mass User Creation tool (SMUA)
- Role Adjustment tool in transactions `SOLMAN_SETUP` and `SMUA`

All are explained in the following sections.

If you use Root Cause Analysis, the User Management and authentication mechanisms provided by SAP NetWeaver Java are used, so the security recommendations and guidelines for user administration and authentication, as described in the SAP NetWeaver ABAP Security Guide and the SAP NetWeaver Java Security Guide, also apply to SAP Solution Manager. We also provide a list of the standard users required to operate the Solution Manager for each scenario. As the mechanisms provided by the SAP NetWeaver Java only apply for Diagnostics, see according information in the Service Marketplace: <http://service.sap.com/diagnostics> .

6.2 User Management Tools and User Types

A user in a computing context refers to a human person who uses a computer. Users may need to identify themselves for the purposes of accounting, security, logging and resource management.

In an SAP system, users must be created, and roles containing authorizations and a user menu must be assigned to user master records. A user can only log on to the system if he or she has a user master record. It contains user data such as e-mail address, language and password. It can be changed by an administrator or the user.

Creating and changing user master records is done in the User Management. The User Management for SAP Solution Manager uses the mechanisms provided by the SAP NetWeaver ABAP, and Java tools, user types, and password policies. Since SAP Solution Manager is based on SAP NetWeaver ABAP and Java, the User Management Engine (UME) of the Java stack is to be configured against the ABAP stack. This is done during Infrastructure settings configuration.

The users created in the User Management tool are typically assigned user types which follow specific demands regarding their password policy.

You can also use external applications for the User Management by using technologies like LDAP, Active Directory (Microsoft OS only), or NIS (Linux). For more information regarding any external User Management solutions like the LDAP scenario, see the documentations available on the SAP Service Market Place.

⚠ Caution

Within ABAP transaction SU01 is the User Management tool for users / roles / profiles, which are fetched on the Java UME storage. However, in some cases, some Java users have to be stored and maintained within the Java stack. This is for example the case for the SLD users (SLD is a Java application).

The following sections give you an overview over the User Management tools used by SAP Solution Manager as well as the user types used.

User Management

Tools Overview

Object	Recommended Tool	Remarks
Users	Transaction SU01	User Management in the ABAP system(s) ⚠ Caution For password security information, see SAP Note 862989
PFCG roles	Transaction PFCG	 i Note User Comparison feature was corrected, see SAP Note 1272331
J2EE security roles and UME roles (only applies to Java application, for instance Root Cause Analysis)	UME and the Visual Administrator	Administration console to manage UME roles, and administration tool of the Java Server, to manage J2EE security roles. Both of these tools are part of SAP NetWeaver Java. To integrate the Java-based authorizations supplied by J2EE security roles and UME roles with PFCG roles, you can integrate PFCG roles as groups in SAP NetWeaver Java. More information on UME conversion, see IMG activity: Convert UME (technical name: SOLMAN_CHANGE_UME)
Automatic creation of SAP Solution Manager - specific default users and assignment of relevant roles	Transaction SOLMAN_SETUP	see section on Automatic User Creation in transaction SOLMAN_SETUP
Mass Maintenance for automatic creation of SAP Solution Manager - specific default users and assignment of relevant roles	Work Center SAP Solution Manager Administration	see section on Automatic User Creation in Solution Manager User Administration (SMUA)

Object	Recommended Tool	Remarks
Role Adjustment tool	Transaction SOLMAN_SETUP	see section on Role Adjustment Tool in transaction SOLMAN_SETUP

For more information how to create roles, how to maintain authorizations and authorization profiles, and how to execute the user comparison, see How-to section in this guide.

User Types

When speaking about user types, we mean users in a system, which are created for various purposes. This is necessary to specify different security policies for different types of users. For example, your policy may specify that human users (end users) who perform tasks interactively must change their passwords regularly, whereas users who run jobs in the background need not do so. In this guide we differentiate between human users, who are represented in the system by dialog users, and technical users who perform tasks on behalf of other users in the system. These are represented in the system by the type of system user, service users, or reference users. In transaction `SU01`, tab *Logon Data*, you can determine the user type for your user.

During the SAP Solution Manager configuration, any user can be created automatically and manually, depending whether they are created during basic Solution Manager configuration, technical monitoring setup, or during scenario-specific setup.

Dialog User

A dialog user represents human users, also called end users. It is required for individual, interactive sessions in the SAP system. An end user requires this user type.

With dialog users, it is possible to check for expired/initial passwords, to change passwords, and the system checks for multiple logons. You should assign to a dialog user exactly the authorizations that he or she requires to perform his or her tasks, in accordance with an established roles concept and authorization concept.

SAP Solution Manager ships composite template roles for predefined end users for each scenario, see according scenario-specific guides. This means, that we deliver template roles with authorization objects in roles that are maintained according to a specified authorization concept. This authorization concept is a recommendation by SAP, which you can use. Since your requirements may differ, you need to adapt these delivered templates. In the scenario-specific guides you find a user description relevant for the specific template role.

In case of a dialog user using ABAP stack and Java stack UI, an assigned role (for instance `SAP_J2EE_ADMIN`) can be propagated to user groups of the user management engine (UME), which are then assigned to security roles for Java applications by using the Security Provider service of the Visual Administrator. These roles include no authorization objects.

Dialog users are maintained in the ABAP stack. A session-based single sign-on is supported.

i Note

If you use SAP NWBC as front-end client, you can only logon with a dedicated dialog user.

System User

A system user does not allow interactive system access. This user is used to be able to perform certain system activities, such as background processing, ALE, workflow, and so on. The system excludes a user of this type from the expiry date of passwords. Therefore, the password of these users can only be changed by user administrators. You should also ensure for users of this type that you assign only the rights that are required in the system. If, for example, users of type system users for RFC connections have too many authorizations, RFC administrators from the calling system can easily log on to the called system and abuse the technical user's authorizations. SAP Solution Manager ships according predefined standard roles for such users. This user type is used for user `SOLMAN_BTC` or RFC - users. All technical users created by the automated basic settings configuration via `SOLMAN_SETUP` are of type system.

Reference User

Instead of assigning roles to each user individually, a reference user is created for a selection of roles that are to be assigned to a larger group of users, and the selected roles are assigned to this user. The reference user must now be assigned to the dialog users in the roles tab of the user master record. This minimizes administration costs and improves performance. This method is used when you need to create a high number of users in your system with the same authorizations assigned. For instance in Application Incident Management the report `AI_SDK_SP_GENERATE_BP` is used to create users as well as additional business partners.

With this report, you can use a reference user to create users and according business partners.

6.3 Automatic User Creation Options using Transaction `SOLMAN_SETUP`

Configuration Users and Template/Standard Users

Configuration Users (SMC* Users)

→ Recommendation

We strongly recommend to use specific SMC* users for configuring your scenarios and refrain from using profile `SAP_ALL`. If you nevertheless use this profile, be aware to remove it from the user in question after configuration.

In transaction `SOLMAN_SETUP`, you can create specific configuration users for all scenarios that are configured automatically in a guided procedure in transaction `SOLMAN_SETUP`. These users are created, when you are calling the [Guided Procedure View](#) for your application.

You can either provide an existing user or create a separate configuration user. In case you provide an existing user, the system adds the according missing roles to this user.

The configuration user contains all necessary authorizations for configuring the scenario using the guided procedure. It also contains authorizations to check system prerequisites and run the application.

i Note

You can mass create [Configuration Users](#) using the [Solution Manager User Administration](#) application (SMUA).

Configuration Pop-Up

In case your logged on user has profile `SAP_ALL` or any other not SAP recommended role assigned, proceed as follows:

- Create a new user
- Ignore the information: in this case choose button *Advanced* and then press button *Ignore*.

Template/Standard Users

Within each guided procedure for scenarios it is possible to create so-called Template/Standard Users. These users contain authorizations/roles to allow exactly only those activities in the according application, which are defined in the user description by SAP. **Therefore, these users can be considered as DEMO users.** To create those users is an **optional activity**.

The template users contain only authorizations for the main functions of the scenario.

i Note

They do not include authorizations for additional functions (see sections on *Additional Functions* per scenario- specific guide), or authorizations for integration purposes with other scenarios/functions (see section on *Scenario Integration* per scenario – specific guide). In both cases, you need to manually add the according authorizations.

The roles assigned to a specified user are also available as composite roles, see section on *Users and Authorizations* in the scenario–specific guides.

User Description and Role Descriptions

For all users created in transaction `SOLMAN_SETUP`, and all roles assigned, a documentation is provided through a link in the according user creation step. The user description states which tasks are allowed for this user in the specific application. The role description describes for which functions authorizations are provided.

The roles are listed in the according scenario–specific guides and the system HELP Text ID is mentioned. This HELP Text ID can be checked directly in transaction `SE61`.

For authorization object descriptions, see the SDN Wiki on the topic or check transaction `SUIM` for this authorization object.

User Types

You can create users of the following user types:

- Dialog User
This option should only be used for System Preparation, Basic Settings, and Managed System Configuration. In these configuration procedures users must be created as displayed in the screen. Otherwise, a change of user type can lead to errors during configuration. After configuration, the user type for administration users such as `SOLMAN_ADMIN`, managed system administrator, or BW administrator can be changed to Service User in transaction `SU01` to disable active logon.
- System User
This option is always used for technical users, and should not be changed if it is suggested in the guided procedure for this user.

Automatic User Creation and Update Use Cases

Create Users

When you create a user, the system tells you if an according user already exists. Use field [Action](#) to create a new user. The system provides you with the default name for this user. You can change this user name. The system then automatically creates the user and assigns the roles which are displayed in the column [Copy from SAP Role](#). Navigation roles and [CRM](#) Business Roles are not copied (see section on [Navigation Roles](#)). The system then does not provide any suggestion for a role copy.

Update Users

You need to update your users, when roles/authorizations need to be updated. In addition, you can choose to update/enhance an existing users with additional role assignments using the update functionality. For instance, you can update/enhance user `SOLMAN_ADMIN` with configuration roles for scenario-specific guided procedures in `SOLMAN_SETUP`.

Business Partners

[CRM](#) - based scenarios or Technical Monitoring, require that the user is assigned a Business Partner (BP). When you create a new user using transaction `SOLMAN_SETUP` an additional business partner is created as well. The following scenarios require Business Partners:

- Incident Management
- Change Management
- QGM
- BPCA
- Application Monitoring
- LMDB
- Job Scheduling Management
- Requirement Management
- Process Management
- Service Requests
- Data Volume Management

The system does not create a Business Partner when you update existing users.

Automatic Roles Assignment and Update Use Cases

New Role Assignment

All roles assigned to automatically created users in transaction `SOLMAN_SETUP` are fully maintained. This means, that for authorization fields which cannot be prefilled by SAP with default values, an asterisk (*) is maintained, which allows full authorization for this field. For instance, the [System ID](#) field in authorization object `AI_LMDB_OB` cannot be prefilled by SAP due to its generic nature.

→ Recommendation

If you would like to use these users in productive environment, we recommend to check the roles manually and assign specific values to all fields containing an asterisk.

Update of Role Assignment

When you update a user with new SAP roles, for instance if adapted roles are shipped with a new Support Package, the system indicates which roles need to be updated. Technically, when updating a role, the existing copied role is deleted and a new copy of the SAP role is created by the system. Therefore, if you have manually changed any authorization values for authorization objects in your copied roles, you need to be aware of this. In addition, in case you have manually created a role in the **Z** name space, such as `ZSAP_SUPPDESK_CREATE`, the system will not update the role as it detects that the copied role had been created manually.

Note

- When roles need to be updated, you must at least run transaction `SU25` points 2a) and 2b). Alternatively, follow SAP Note [368496](#).
- For updating individual authorizations and authorization values, choose the *Role Adjustment Tool*.

Role Upload into Managed Systems

You can upload the authorization roles for the `READ` - User and the `TMW` - User from the SAP Solution Manager - system into the managed systems.

Caution

This function is only available for the upload of roles for the above-mentioned users. You should only upload the relevant roles into managed systems, which are not productive. We recommend to upload the roles into your development system and transport them into your productive system. Alternatively, you can download/upload the roles manually. Except if the SAP roles have been manually assigned. In this case we display the real assigned roles in the Target Role column, without the default name space.

Manual Role Assignment

In case you have decided to only manually assign roles to users, the system displays in the column *Target Role* the roles assigned using transaction `PFCG` without the suggested name space.

Expert Mode

The Expert Mode allows you to use the following features in regard to user creation and role creation as well as assignment:

- Define name space for roles
- Define and assign the user to a specified user group

Name Space for Roles

You can set a specified name space for the roles, which the system assigns to one user. The default name space is `*Z*`.

i Note

All roles assigned to the predefined users:

- `SAPSERVICE` receives name space `ZSD`.
- `SMC_MIG_*` receives name space `ZM`.

This name space is set, because the authorizations for these users are predefined.

User Group

You can define a user group for the users you create. The user is assigned to this user group.

→ Recommendation

We recommend to group users. You can then easily search for them and restrict access to them using authorization object `S_USER_GRP`.

BW Scenarios

Depending on your scenario setup for [BW](#), the system detects automatically in which system/client you run [BW](#). It determines in which system the according [BW](#) user needs to be created and displays this in the User Interface. In case of a standard [BW](#) scenario, all [BW](#) roles are added to the user created in the Solution Manager system.

In case of a remote [BW](#), a separate user is created in the [BW](#) system/client. This last setup requires that both users, in the SAP Solution Manager system as well as in the [BW](#) system, receive the additional authorization for trusted `RFC` destinations, authorization object `S RFCACL`. The roles for trusted `RFC` - destination are explicitly explained in the User Interface HELP. Also check section [Users and Authorizations](#) in each scenario - specific guide.

If you run [BW](#) in a remote scenario, user names of the created users in the Solution Manager system and in the [BW](#) - system must be identical.

6.4 Solution Manager User Administration (SMUA)

The Solution Manager User Administration ([SMUA](#)) allows you to maintain all users that are created automatically via transaction `SOLMAN_SETUP` and application `SMUA`.

In general, the functionality reflects the same technical aspects and similar User Interface as the user creation using transaction `SOLMAN_SETUP`. `SMUA` allows you to see all created users in one tab for Solution Manager users, managed system users, BW-system users, configuration users.

For all individual Solution Manager - specific default users, you can:

- display users and their user roles per system landscape relevance (used in Solution Manager - system, used in managed system, used in BW-system)

- create and update users and their user roles
- create users in mass maintenance
- set passwords
- upload user roles for Read-User (Read - Connection) and `TMW - User` (`TMW - Connection`) into the managed system (for more information, see the according section on these `RFC - Connections`).

User Interface Possibilities

The User Interface allows for a range of different activities which you can use according to your individual needs. For instance, you want to:

Update All Configuration Users

Choose tab Configuration Users. Here, you find all Configuration Users available for transaction `SOLMAN_SETUP`. You can do all above mentioned activities here, update all or just one.

Update All Users Relating to One Specific Scenario

In all available steps, check column *Used In*. Here, you find the scenario mentioned you search for. Choose your scenario, and the system displays all relevant users available for this scenario.

Tool Access Authorization

To access the application, your user needs to have:

- authorizations for the work center Solution Manager Administration assigned (see [Scenario-Specific Guide for Solution Manager Administration](#)). In the view navigation in the work center Solution Manager Administration, choose *Users*. This allows you to access and use `SMUA`.
- authorization object `SM_SMUA` assigned. This object is contained in the single role `SAP_SM_SMUA_*`. The role `SAP_SM_SMUA_*` is contained in the composite roles for SAP Solution Manager Administration (see the according scenario-specific guide for reference), or you can assign it separately.

For more information on the features of the application itself, see the Online Help for SAP Solution Manager.

Additional Authorizations for User Creation

You can use the user creation and update in `SMUA` if:

- general User Management and Role Assignment authorization is granted. These authorizations are contained in role `SAP_SM_USER_*`.
- `RFC - connections` related to specific technical users can only be displayed if authorizations for transaction `SM59` are granted. These authorizations are contained in role `SAP_SM_RFC_*`.

Multiple Storage of Users

The system stores all dialog users created within transaction `SOLMAN_SETUP` and in [SMUA](#). For technical users, it stores the last user created, and removes the former.

6.5 Automatic Managed System Configuration (AMSC) Update using Transaction `SOLMAN_SETUP`

In case of an update to your managed systems, the Managed System Setup in transaction `SOLMAN_SETUP` can be run automatically. This requires the automatic update of users in your managed system.

In Case of SLD Changes

Use Case

In case of system updates in the System Landscape Directory (SLD), a configuration update job runs in the Solution Manager with a dedicated technical user `SM_AMSC`.

Technical User `SM_AMSC`

The update job of the managed system configuration is run by the technical user `SM_AMSC` in the Solution Manager system. This user is created during System Preparation in the Solution Manager system. For more details, see section on [Technical User `SM\_AMSC`](#) in this guide.

6.6 Passwords for Solution Manager Default Users

You can create a number of SAP Solution Manager default users using transaction `SOLMAN_SETUP` or the Solution Manager User Administration (`SMUA`) in the work center [SAP Solution Manager Administration](#).

Set Initial Passwords

When creating these users, the system automatically:

- sets an automatically generated password to all users of type [System User](#).
- requires of you to set an initial password for all users of type [Dialog User](#).

Within `SMUA`, you can set a password for a number of dialog users in one User Interface. Users of type system user are not displayed in the User Interface. For more information, see Online Documentation for `SMUA`.

i Note

SAP-wide default users such as DDIC, SAP*, and so on, are not considered. For those users, the general SAP policy for passwords is relevant. After configuration, change the password for these users, or deactivate them. For more information, check the SAP NetWeaver Security Guide.

Update Passwords

If you manage users and their passwords solely using transaction SOLMAN_SETUP, the passwords are automatically adapted in transaction SU01 and the RFC destination. In case of CUA, SOLMAN_SETUP can not adapt passwords accordingly. For more information on CUA, see the according section.

6.7 Role Adjustment Tool in Transaction SOLMAN_SETUP

Use

Within transaction SOLMAN_SETUP, you can create users and update user roles. The *Role Adjustment* tool helps you to compare authorization objects and authorization values of your already customized roles with newly delivered SAP roles. This tool is delivered with Software Component ST, and is only relevant for roles created in transaction SOLMAN_SETUP.

How does the System Role Copy Work

When you update a user with user roles in SOLMAN_SETUP, the following steps are executed by the system:

1. The system deletes the present copied target role.
2. The system copies the SAP source role.

When you have modified any authorization field in your copied role, this modification would be lost. **If you want to keep the modification, you can compare your copied role with the newly delivered SAP role update, and then decide on how your modified role is updated.**

How to Access the Role Adjustment Tool

1. Access transaction SOLMAN_SETUP in *Edit* mode.
2. Select the action *Create User* or *Update User Roles*.
3. Mark the line of the role in which the *Update* flag is set.
4. Choose the button *Manual Role Adjustment* in the upper left corner above the list of roles which are assigned to a user.

How to Use the Adjustment Tool

The *Adjustment Tool* compares the delivered SAP role with the existing copied role. The *Comparison Status* of the *Target Role* (the copied role) shows you for which authorization objects and authorization fields differences exist in the target role to the SAP role. Checking these differences, you can decide whether to replace or adjust authorization objects and authorization fields in the copied role.

Constraints

Adaptation of Authorization Objects

The following authorization objects can only be adapted using transaction PFCG:

- S_TCODE, S_SERVICE and S_START: Any start transaction authorization object can only be maintained by using the Menu tab in a role using transaction PFCG.
- S_RFC: S_RFC is not maintainable by maintaining the Standard values. You need to either adapt the authorization object for the application in transaction SU24, or add a manually created authorization object maintenance in transaction PFCG.
- PLOG: Organization Units (such as PLOG for HR) must be maintained in transaction PFCG.

6.8 Using Central User Administration

6.8.1 Introduction

→ Recommendation

We strongly recommend NOT to use SAP Solution Manager with Central User Administration (CUA) in one central system.

Central User Administration (CUA) enables central administration of the user data for all back-end systems, like a Solution Manager system, a managed PI system, and so on. That means, you administer users for all systems of the CUA and their authorizations in the central system. With an active CUA, you can only create and delete users in the central system and not in the connected child systems. You can lock and unlock users, assign roles to users, and so on, from the central system, in accordance with the settings that you have chosen in transaction SCUM for the distribution of the data.

This documentation regarding the integration of CUA in the automated basic configuration for SAP Solution Manager does not replace CUA configuration guide. It supplements the usage of central user administration (CUA) in combination with SAP Solution Manager configuration. During the automated basic setup (in transaction SOLMAN_SETUP or SAP Solution Manager configuration work center) numerous technical users and dialog users are automatically created. In former releases you had to create these users manually on SAP Solution Manager and its managed systems as soon as the effected system was connected to a CUA.

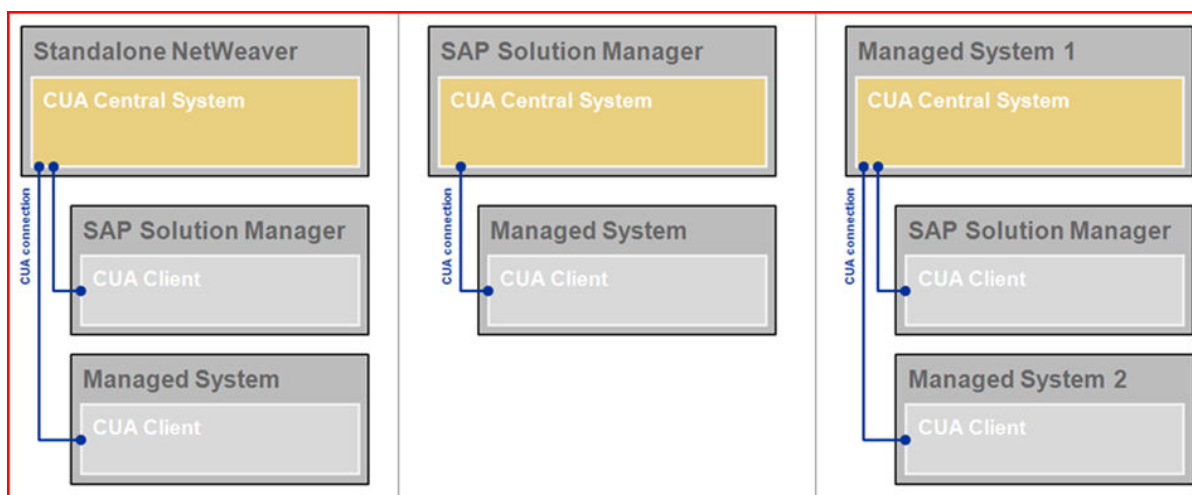
Possible CUA scenarios

→ Recommendation

We recommend to enable CUA in another client/system than the productive Solution Manager client.

Central User Administration can be activated on every SAP NetWeaver system (as a CUA client or central system). Since every SAP NetWeaver system in your landscape can be candidate for CUA central system, the following three scenarios exist in the SAP Solution Manager environment:

1. Standalone CUA central system
2. SAP Solution Manager as CUA central system
3. Managed System as CUA central system



Possible CUA scenarios in your landscape

→ Recommendation

We recommend you configuring the CUA on a high availability solution. In case you want to install the CUA central system on SAP Solution Manager, consider the required maintenance windows of the system.

Steps for configuration of CUA:

If the CUA is already in place within your system landscape you can skip the following step:

1. Decide which system in your landscape should become the CUA central system.
2. Configure your CUA as described in the SAP help documentation.

These configuration steps have to be considered in order to link SAP Solution Manager to CUA:

1. the configuration for user CUA_<SID> (example: CUA_ADM) on the CUA central system, see section *Prerequisites*.

2. Verify which RFC scenario you are using for your CUA configuration, see section *Configuration*.

i Note

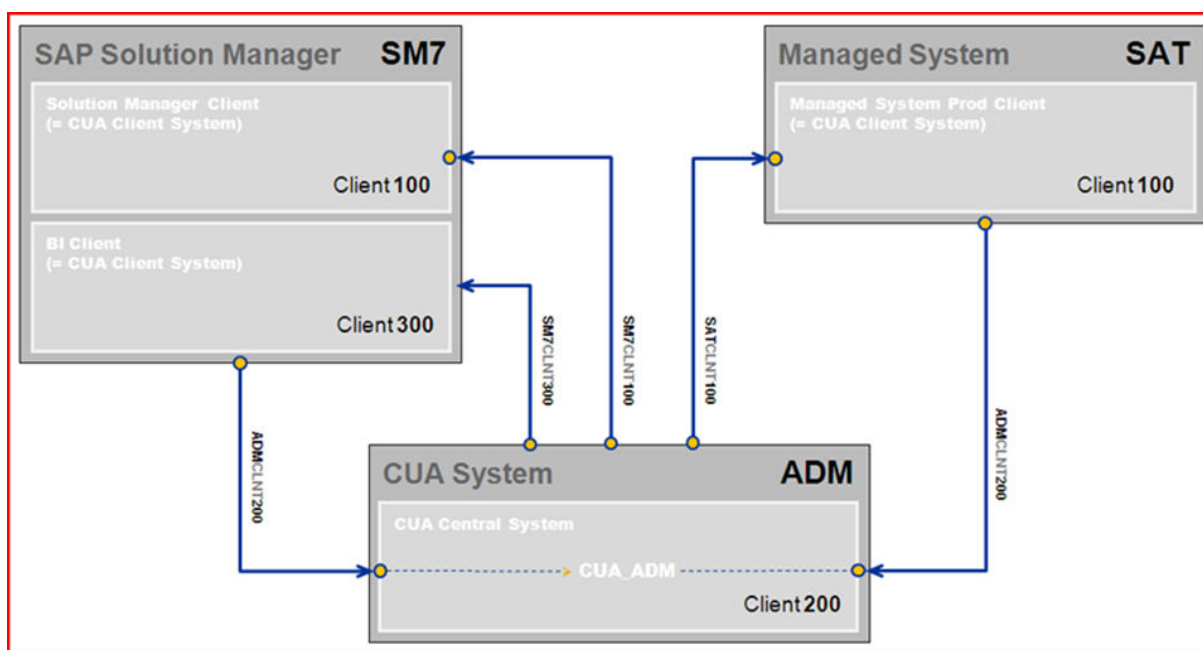
If your preceding check shows that you are using Trusted RFC destinations, you still need to create a system user on the CUA client system.

3. Finally, we recommend you running report `PFCG_TIME_DEPENDENCY`, see section *Prerequisites*.

Example

The subsequent sections explain the configuration based on the following example scenario:

- System **SM7** (SAP Solution Manager with Solution Manager client and local **BI** client)
- System **SAT** (managed system with one productive client, which is connected to SAP Solution Manager)
- CUA system **ADM** (Central User Administration central system)



Example

6.8.2 Prerequisites

CUA should be configured as described in the SAP help documentation, see section [Additional Links](#).

SLD Configuration

Ensure that software component `LMTOOLS 702 SP6` Patch Level 6 is applied on your SAP Solution Manager Java stack. This ensures that the local SLD configuration can be performed when SAP Solution Manager is connected to CUA.

Note

In case the SLD is in a CUA environment, you have to manually add the parameter `&CUA=true` at the end of the URL called by the SLD Local Configuration and Central SLD Configuration in transaction `SOLMAN_SETUP` in System Preparation for SLD.

You need to apply [SAP Note 1572856](#) and [SAP Note 1577918](#) in your SAP Solution Manager system in advance.

RFC Destinations, Users and Authorizations

As a prerequisite, you define the logical systems for all effected systems. The RFC - destinations have the same names (like logical systems), and must exist in each direction:

- from the CUA central system to the CUA client system (for example: `SM7CLNT300`, `SM7CLNT100`, `SATCLNT100`)
- from the CUA client system to the CUA central system (for example: `ADMCLNT200`)

In the CUA central system the user `CUA_<SID>` (for example: `CUA_ADM`) is assigned the following ABAP single roles:

Roles for user `CUA_<SID>`

Technical Role Name	Remarks
<code>SAP_BC_USR_CUA_CENTRAL</code>	Authorization for the CUA central system user to maintain user master data and distribute changes to the CUA client systems.
<code>SAP_BC_USR_CUA_CENTRAL_BDIST</code>	All users in the central system require this role if CUA field attributes are set to redistribution.
<code>SAP_BC_USR_CUA_CLIENT</code>	This role contains authorizations for user administration in the child systems. For calling the CUA central system, and initiate the user creation in transaction <code>SOLMAN_SETUP</code> , the CUA central system user requires this permission. For more information, see notes below.

This user is assigned in all RFC destinations in direction of the CUA central system (for example: `ADMCLNT200`).

Note

Role `SAP_BC_USR_CUA_CLIENT` contains extensive authorizations for user administration in the child systems. If you do not allow this ABAP role on the CUA central system, use the following alternative: Copy

ABAP role SAP_BC_USR_CUA_CENTRAL_EXTERN in your name space according to [SAP Note 492589](#)  section 2, and maintain the following minimum authorizations:

Minimum Authorizations

Authorization Object	Field	Value	Remarks
S_USER_GRP	ACTVT	01, 03	no remarks
	CLASS	full authorization	
S_USER_AGR	ACTVT	02 (22)	If you set the customizing switch ASSIGN_ROLE_AUTH to the value ASSIGN in your CUA central system according to SAP Note 312682  , set in field ACTVT value 22, otherwise value 02.
	ACT_GROUP	full authorization	
S_USER_PRO	ACTVT	22	no remarks
	PROFILE	full authorization	
S_USER_SYS	ACTVT	78	no remarks
	SUBSYSTEM	*	

Note

If you activated the authorization check on object S_USER_SAS according to [SAP Note 536101](#)  (customizing switch CHECK_S_USER_SAS in table SSM_CUST), assign the following authorization to the ABAP role: S_USER_SAS with activity ACTVT 01, 06, 22. In field SUBSYSTEM, enter the logical systems that you would like to connect to your SAP Solution Manager. Consider that you might need to change this authorization later as soon as you need to connect a new system.

The authorization object is shipped in role SAP_SM_USER_ADMIN with ACTVT 22.

User Master Data Reconciliation

If you assign roles to users for a limited period of time only, you must perform a comparison at the beginning and at the end of the validity period. We recommend that you schedule the background job PFCG_TIME_DEPENDENCY in such cases.

⚠ Caution

Do not enter generated profiles directly into the user master record in transaction SU01. During a user comparison, the system removes generated profiles from the user masters if they are not among the roles that are assigned to the user.

Proceed as follows:

1. Start transaction `PFUD`.
For the system to consider all roles, do not specify any roles and leave the fields empty.
2. Choose action *[Schedule or check job for the full comparison](#)*.
Here, you can start the report `PFCG_TIME_DEPENDENCY` by specifying the time when the job is to start.
The overview displays the status of background jobs that have already been scheduled.

If you schedule the report `PFCG_TIME_DEPENDENCY` daily before the start of business as a total comparison and it runs error-free, the authorization profiles in the user master are up-to-date every morning.

6.8.3 Configuration Scenarios

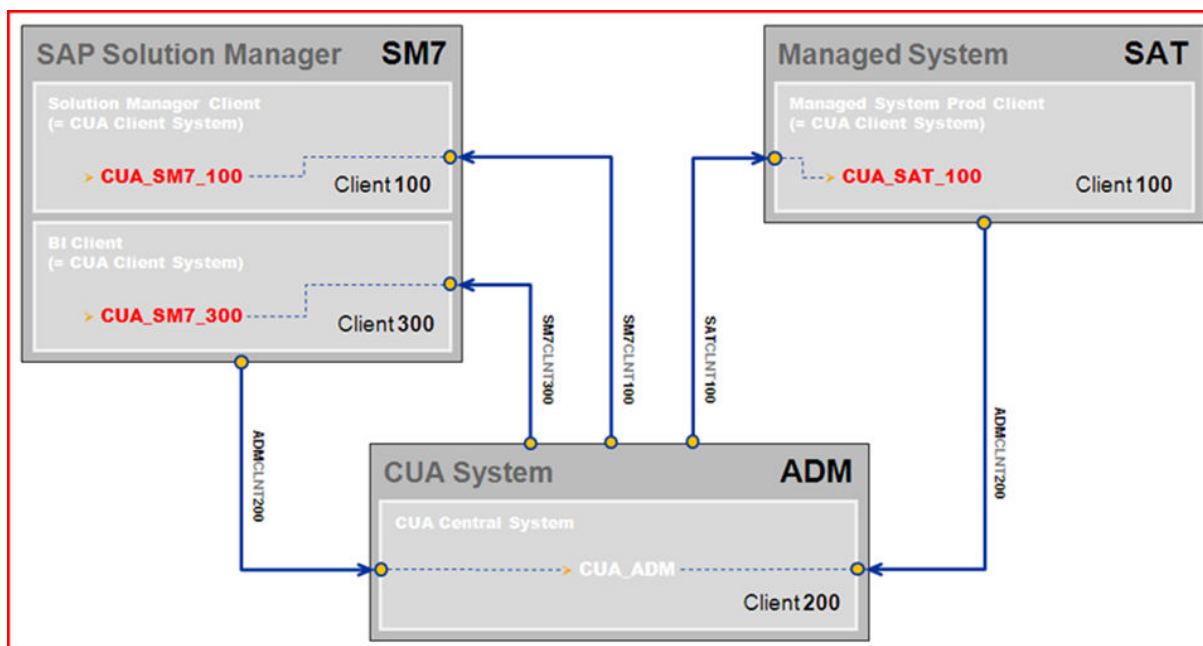
You can configure the CUA with two options:

- RFC - destination with defined system user
- Trusted RFC - destination

RFC - destination with defined system user

This CUA variant requires RFC - destinations to CUA client systems with defined system users named `CUA_<SID>_<Client>`. The user requires the following role: `SAP_BC_USR_CUA_CLIENT`. This role contains extended authorizations for the user administration in the child systems. This division is only useful for background processing.

The following graphic shows the example scenario with the corresponding users and RFC - destinations with the default naming convention:



Example

Trusted RFC - destination

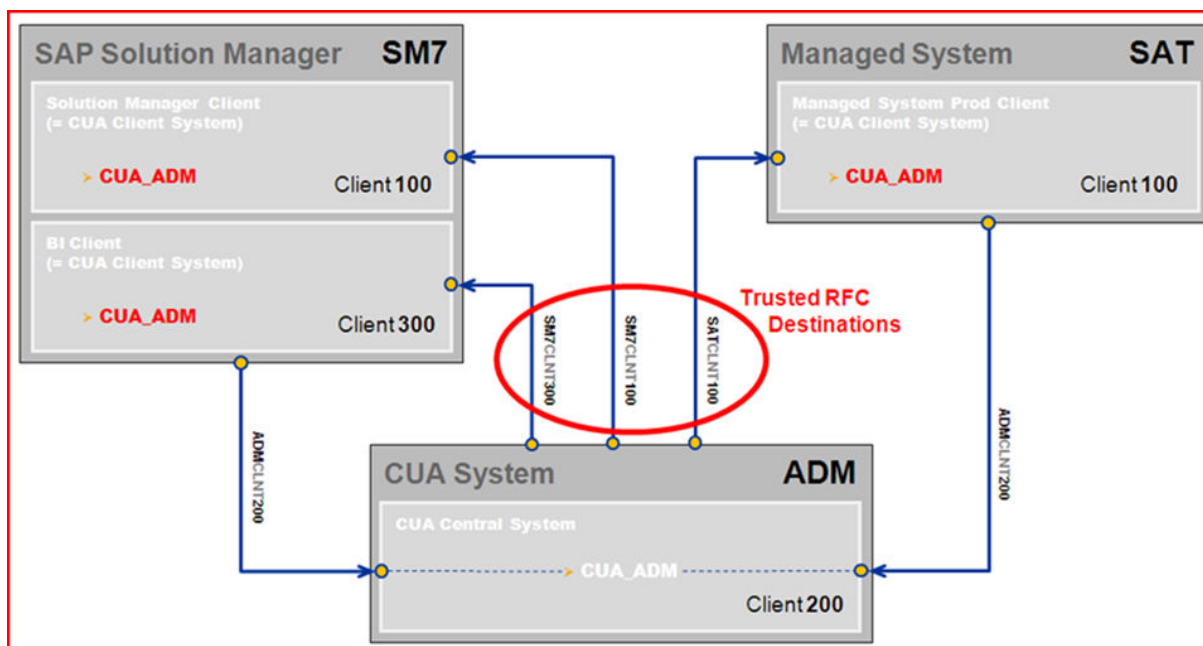
CUA configuration using trusted RFC - destinations to the CUA client systems needs a user in the CUA client with role `SAP_BC_USR_CUA_CLIENT`, and the additional authorization object `S_RFCACL` (for trusting permission). According to the SAP Solution Manager configuration the user administrator is the CUA central system user `CUA_<SID>` (for example: `CUA_ADM`).

To complete the CUA configuration for the SAP Solution Manager integration this user must exist on the CUA client systems with the following role: `SAP_BC_USR_CUA_CLIENT`.

Note

For trusted systems, the authorization object `S_RFCACL` is checked and therefore required in child systems. This ensures that only particular applications (such as transaction `SU01`) can access the child system by RFC. You cannot use trusted systems with the *current user* settings for data distribution from the child to the central system (redistribution with distribution parameters) as the users could change their own user data with transaction `SU3` and distribute it to the central system by redistribution. This means that all users would require change authorization for the user administration in the central system and could also change all other user data.

The following graphic shows an example scenario with the corresponding users and RFC - destinations with the default naming convention:



Example

6.8.4 Configuration Integration in Transaction SOLMAN_SETUP

Whenever a user (in our example: on the Managed System) is created or changed by the automated basic setup from SAP Solution Manager the user master data is changed as follows:

1. On SAP Solution Manager an administrative user (for example: user `SOLMAN_ADMIN`) creates or changes a user. For this the corresponding administrative user on the target system (for example: user `SOLMAN_ADMIN`) is called.

Users

Refresh

User Name	ID	User Type	System	Status	Documenta...	Login
SAPSUPPORT	SAPSUPPORT	A Dialog	SM6~ABAP	⚠ User exists but without all required roles. Update of authorizations is required	Display	
SMDAGENT...	SMDAGENT...	B System	SM6~ABAP	⚠ User exists but without all required roles. Update of authorizations is required	Display	Test

SAPSUPPORT Dialog User (in Managed System SM6 Client 100)

User exists but without all required roles. Update of authorizations is required ⚠

Action:

Update Authorizations of Existing User

User Name:

SAPSUPPORT

Password:

Repeat Password:

Needed Roles

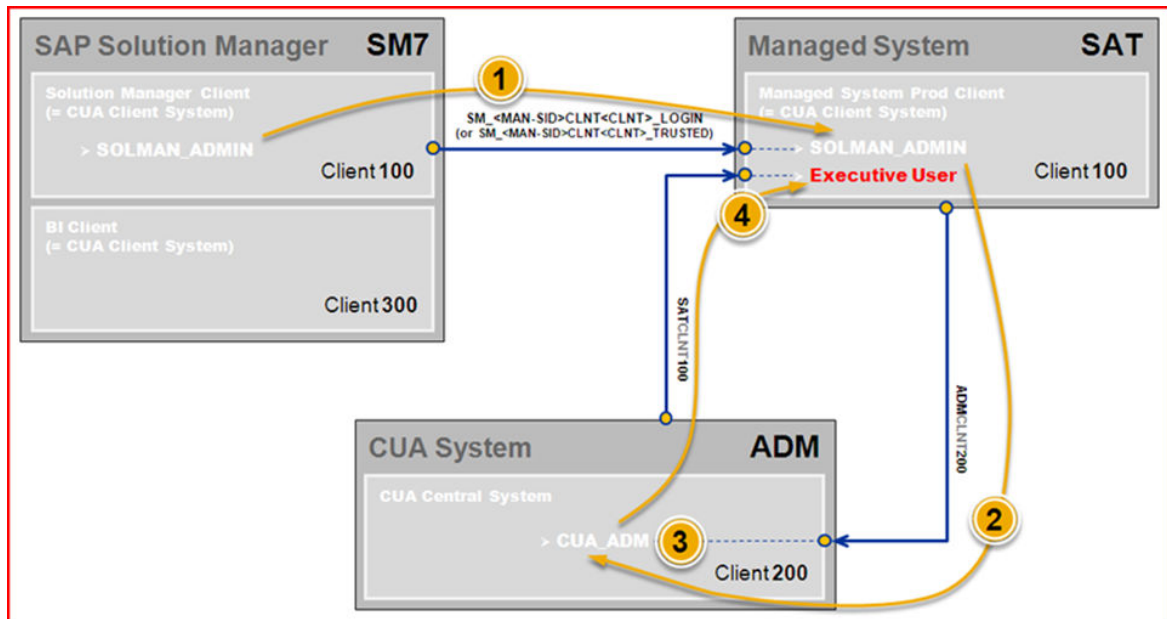
Action Taken	Delivered SAP Role	Copy from SAP Role	Update ne...	Start trans...	Role Descr...
Create and assign cust...	SAP_RCA_SAT_DISP	ZSAP_RCA_SAT_DISP	☐	Display	Display

Execute

Example

- The administrative user on the target system (for example: user `SOLMAN_ADMIN`) automatically calls RFC - destination to the CUA central system (for example: `ADMCLNT200`) with CUA central system user `CUA_<SID>` (for example: `CUA_ADM`).
- CUA central system user `CUA_<SID>` (for example: `CUA_ADM`) now changes the user master records on the central system.
- Finally, the CUA central system user `CUA_<SID>` (for example: `CUA_ADM`) distributes the changes to the CUA client system using RFC - destination `<SID>_CLNT_<Client>`.

The user master data changes on the client system are executed by either the user defined in the RFC destination (for example: `CUA_SAT_100`), or the CUA central system user (for example: `CUA_ADM`).



Example

6.9 Secure Storage

Use

The secure storage stores encoded data, for instance access data of systems, `SLD`, SAP Portal connection, and so on. The system uses the installation number of the system and the system ID when creating the key for the secure storage.

⚠ Caution

If one or more of these values change, the system can no longer read the data in the secure storage.

More Information

[SAP Note 816861](#) and [SAP Note 1027439](#).

6.10 Integration into Single Sign-On Environments (SSO)

Use

The Solution Manager supports the Single Sign-On (SSO) mechanisms provided by the SAP NetWeaver. It uses various front ends (SAP GUI, SAP NWBC, and Web browser, in this case an HTML Control). The system opens several sessions on the server, that require, for example, a second logon. The user uses SAP GUI to log on to a system, the application uses the SAP GUI for HTML Control to call another application, and the system then prompts the user to re-enter the logon data.

Caution

If you are using external SSO with SAP Solution Manager, see [SAP Note 1153116](#) .

The supported mechanisms are:

- [Secure Network Communications \(SNC\)](#) : SNC authenticates users and provides an SSO environment when using the SAP GUI for Windows or Remote Function Calls.
- [SAP logon tickets](#): The Solution Manager supports the use of logon tickets for SSO when using a Web browser to access Solution Manager documents via URLs from outside. Users can be issued a logon ticket after they have authenticated themselves with the Solution Manager system. The ticket can then be submitted to the system as an authentication token, each time the users access documents via URLs from within the same Browser session. The user does not need to enter a user ID or password for authentication, he can access the system directly after the system has checked the logon ticket.

More Information

- on SNC, see Secure Network Communications (SAP Library) in the SAP NetWeaver Application Server ABAP Security Guide.
- on how to use Single Sign-On, see Service Marketplace: <http://service.sap.com/sso-smp> .

7 Users and Authorizations Relevant for Configuration

7.1 Getting Started

What is this guide about? SAP Solution Manager covers a wide range of diverse scenarios you can use. You need to setup the SAP Solution Manager first, and make your system landscape known. This is done during SAP Solution Manager setup. Subsequently, you setup the specific scenarios you want to use. For more information, see scenario-specific security guides per scenario which cover all relevant information.

⚠ Caution

Before you start using this guide, you must read the authorization concept information about security issues in SAP Solution Manager. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

Setting up the system landscape includes to configure the basic SAP Solution Manager scenarios, that is enable Solution Manager to run Root Cause Analysis, Services, and simple Incident Management. This requires, the setup of the Solution Manager itself, the connection to its managed systems, the integration of BW functionality, and basic CRM functionality. It requires the setup of dedicated users for the setup and the assignment of specific authorizations in roles. To be able to run the setup, you must know how the setup of all these components is realized in your landscape. That is, you should know how you setup the SLD, remote or local, how you setup BW, standard or remote, and so on.

Therefore, this guide covers the following topics:

Technical System Landscape

Due to the complexity of the setup of SAP Solution Manager, we give you an overview of specific aspects of the technical system landscape for SAP Solution Manager, which are relevant for security aspects, such as the setup of managed systems and their RFC connections, the integration of BW depending on your system landscape, and the technical overview over the new system landscape repository, its integration with SLD and transaction LMDB. To get to know the different aspects helps you setting up the SAP Solution Manager successfully.

Communication Channels and Destinations

Here, you find an overview of all channels and destinations created during the automated basic setup. Note, that in the process of setting up individual scenarios, you may need to create other RFC connection or communication channels. Each scenario-specific guide contains all relevant RFCs needed for the scenario. For

instance, even if you can setup all RFC connections to the managed system during basic setup, you might not need all of them, when you run just one scenario.

Users and Authorizations

Users and authorizations are divided into a number sections, which are semantically divided into the following categories:

- Users Created During Installation
- Configuration Users
- SAP Solution Manager specific technical users
- BW specific technical users
- Specific dialog users
- Managed system users

In each category, you find one section specifically for one user. The users can be of type *Dialog*, like user `SOLMAN_ADMIN`, or of type *System* (technical user), such as `SOLMAN_BTC`. The role assignment for all of these users is documented in the system in transaction `SOLMAN_SETUP`. Here, you find the according Help ID texts, which you can call separately in the system and also adapt to your own needs.

i Note

A number of users that are relevant in any other system like user `DDIC` or the `J2EE` Administration users, are not explicitly explained in this guide. For more information refer to the NW guides security relevant sections. If necessary the users are mentioned in relation to the setup of SAP Solution Manager.

Any users and authorizations for other than Solution Manager or managed systems, like Wily Introscope, are mentioned, but not explained in detail. For more information refer to the according guides.

7.2 Documentation (Help Text IDs) for Users and Roles

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

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

1. Call transaction `SE61`.
2. Choose *Document Class General text* (TX).
3. Choose your language.
4. Enter the technical ID of the help text as given in the tables in this guide.

5. Choose button *Display*. The system displays the text, which is also linked in the setup screen.

i Note

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

7.3 SOLMAN_SETUP Configuration Transaction

⚠ Caution

Before you can work correctly with *User Creation* and *Role Management* in transaction SOLMAN_SETUP, please implement SAP Note [2276832](#) and SAP Note [2183425](#).

You can execute the automated basic configuration using transaction SOLMAN_SETUP.

The application is also the home application for work center SAP Solution Manager configuration. Therefore, to set up your SAP Solution Manager and update it, you can either use the transaction or the work center. When you initially set up an SAP Solution Manager system, the system automatically guides you to the transaction.

→ Recommendation

At a later stage, you can lock the transaction and work within the SAP Solution Manager configuration work center.

In general, the authorizations for this work center are automatically assigned during the configuration process to the users, which are created during the setup. These users are explained in more detail in the next sections of this guide.

User Creation Steps

Steps for creating template/standard users are optional. They are mandatory for default users for the *Basic Settings* and *Managed System Configuration*.

The **optional flag** works at activity level. An optional activity is an activity for which the end-users are not forced to execute the corresponding configuration. The status of this activity is not taken into account in the status consolidation at step level. If a step contains only optional activities, the step itself is considered as optional. The step is then grayed out.

Transporting Custom User Role

It is possible to document custom (name space) - roles for SAP Solution Manager in transport requests.

Prerequisites for Usage

- configured [Automatic Recording of Changes](#) in transaction SCC4
- configured [Transport Management](#)
- The according user requires authorization object S_TRANSPRT

i Note

It is only possible for SAP Solution Manager.

Log Upload and Download

i Note

The logs of any guided procedure in transaction SOLMAN_SETUP can be attached to an Incident Message and downloaded for the purpose of error reference. Any user data or other data in this respect are visible in these HTML reports. Reports are only available for download if the current user has access to SOLMAN_SETUP or the SAP Solution Manager Configuration work center.

Guided Procedure (GP) Lock

Any GP can be locked. The possibility to lock a GP is available when authorization object SM_SETUP with ACTVT 02 (change) is given. Unlocking a locked GP can be done in transaction SOLMAN_SETUP_ADMIN.

Advanced Option in Managed System Configuration

The following configuration possibilities are bundled as [Advanced Option](#) in guided procedure [Managed System Configuration](#):

- Decommissioning
- Automation Option

Related Links Section

You can see the Related Links Section in transaction SOLMAN_SETUP only when you have assigned navigation role SAP_SMWORK_CONFIG.

→ Recommendation

We recommend to assign the navigation role SAP_SMWORK_CONFIG when you upgrade the Release from 7.1. to 7.2, as all migration related Guided Procedures are contained in the Related Links section.

7.4 SOLMAN_SETUP Configuration Administration Tool

You can use transaction `SOLMAN_SETUP_ADMIN` to administer the configuration done in transaction `SOLMAN_SETUP`.

The transaction `SOLMAN_SETUP_ADMIN` contains the following views:

- Overview
- Generic Storage Admin
This view contains the data which is stored during the execution of transaction `SOLMAN_SETUP`. The view of the steps is controlled by authorization object `SM_SETUP` (similar to the use of the object within transaction `SOLMAN_SETUP`).
- SolMan Setup Migration
This view displays logs of the migrations related to `SOLMAN_SETUP`.
- Log Archiving

Roles and Authorizations

The transaction is not integrated in any work center. You have to assign the following roles to a dedicated user, manually:

Roles allowing access to all views, but Log Archiving are:

- `SAP_SOLMAN_SETUP_ADMIN_ALL`
- `SAP_SOLMAN_SETUP_ADMIN_DIS`

Role allowing access to Log Archiving only: `SAP_SM_ARCHIVE_LOG_ALL`

Log Archiving

Log Archiving can be accessed from the following applications:

- any step in transaction `SOLMAN_SETUP`, see section on user `SOLMAN_ADMIN`
- transaction `SOLMAN_SETUP_ADMIN`
- Solution Manager User Management (SMUA), in work center SAP Solution Manager Administration view [Users](#), see scenario-specific Guide for SAP Solution Manager Administration

7.5 Overview on Security - Relevant Activities

How to Access The Overview

You can access the overview on all security-relevant in the according tile from section [Solution Manager Administration](#) on the SAP Fiori Launchpad.

The tile is not displayed by default. If you require the tile, you need to personalize the SAP Fiori Launchpad accordingly.

Required Authorization

To be able to access the tile, you require at least the following roles:

- SAP_SM_SECRET
- SAP_SOLMAN_SETUP_ADMIN_ALL
- SAP_SMWORK_SM_ADMIN

in addition to the Solution Manager Administration user (template user [SA_DIS_<System ID>](#)), which you can create as a template user in the Basic Configuration procedure in transaction `SOLMAN_SETUP`.

→ Recommendation

We recommend to use a dialog user created from the template user `SOLMAN_ADMIN` to use the application in edit mode.

7.6 Solution Content Activation (Data Migration)

7.6.1 Content Activation (Migration) Procedures

With Release 7.2, entities such as solutions and projects are substituted by the function of [Process Documentation](#). For more information, see Online Documentation.

Before you can work with the new process/solution documentation, you must migrate your existing solutions and/or projects to the new functionality. For this purpose, two guided procedures (GP1 and GP2) are delivered.

After you have migrated your solutions and processes, you can proceed to migrate application specific content in Release 7.2. Underneath, see how to proceed according to your Release level. In the following section, you find a detailed description.

How to Proceed

To successfully migrate solution data to Release 7.2 Process Management, proceed as follows:

1. In Release 7.1: Run Guided Procedure 1 (GP1) **or** In Release 7.2: Run Guided Procedure 1 (GP1)
2. In Release 7.2: Run Guided Procedure 2 (GP2)
3. In Release 7.2: Run Application Specific Migration Procedures

7.6.2 Process of Migration and Migration Configuration User SMC_MIG_XXX

Migration Configuration User

You can run the migration procedure in transaction `SOLMAN_SETUP` using migration configuration user `SMC_MIG_XXX`. If the procedure is accessed by any dialog user, the system suggests to create the specific predefined user `SMC_MIG_XXX` with its specified authorizations/roles. To be able to create the `SMC_MIG_XXX` user, the dialog user needs to have authorizations for transactions `SU01` and `PF00`. These authorizations are contained in role `SAP_SM_USER_ADMIN`.

You can create the `SMC_MIG_XXX` user in transaction `SOLMAN_SETUP`, by calling the Guided Procedure: Solution Content Activation, or you can go directly to the [Solution Manager User Administration](#) (SMUA, see [Work Center Solution Manager Administration](#) topic *Users*).

i Note

In any case, before executing the activation, check SAP Note [2381281](#).

In Release 7.1: Run Guided Procedure 1 (GP1)

The migration procedure can be accessed in [edit mode](#) in transaction `PREPARE_ACTIVATION`. For authorization information, see SAP Note [2381281](#).

In Release 7.2: Run Guided Procedure 1 (GP1)

The migration procedure can be accessed in [edit mode](#) in transaction `PREPARE_ACTIVATION`. For authorization information, see SAP Note [2045230](#).

- Work Center application using authorization object: `SM_WC_VIEW`
- To call transaction `SOLMAN_SETUP`: `S_TCODE` (value `SOLMAN_SETUP`)
- Change/edit authorization for transaction `SOLMAN_SETUP` using authorization object `SM_SETUP`
If a user should only be able to access the migration procedure in [display mode](#), only display authorization (`ACTVT 03`) should be assigned to this user.
The authorization objects are contained in single role `SAP_SM_SL_MIGRATION_72`.

In Release 7.2: Run Guided Procedure 2 (GP2)

You can migrate all solution data for all relevant applications which rely in Release 7.1 on solutions. To do so, you can run the according migration procedure GP2 in transaction `SOLMAN_SETUP`. You can find this procedure in section [Related Links](#).

This procedure is based on the setup configuration framework. Therefore, all relevant authorization restrictions which apply for using transaction `SOLMAN_SETUP`, are also relevant for the migration procedure. The migration procedure contains various steps for migration. For each migration, specific authorizations are required by the user executing the migration. Assign the following roles to the user executing the steps of the migration procedure:

1. Solution authorizations and project authorizations as of Release 7.1, which are relevant for display and edit purposes, assign **mandatory** role `SAP_SOLPRO_OLD`. Note: even though this role contains full authorization for all obsolete authorization objects, transactions such as `SOLAR01` and so on can only be viewed in display mode, as no changes are allowed. In addition, **even though you may have assigned profile `SAP_ALL` to your user, obsolete authorization objects are not contained in this profile.**
2. Transaction `SOLMAN_SETUP`, for display of System Prerequisites assign **mandatory** role `SAP_SETUP_SYSTEM_PREP_DISP`.
3. Solutions/projects for Process Documentation and ITPPM, assign **mandatory** composite role `SAP_SOL_PM_COMP`.
4. Roles assigned in `SOLMAN_SETUP` to the user `SMC_MIG_XXX`:

Role	Help Text ID
<code>SAP_CPR_USER</code>	<code>AUTH_SAP_CPR_USER</code>
<code>SAP_BPR_PPM</code>	<code>AUTH_SAP_BPR_PPM</code>
<code>SAP_RMMAIN_EXE</code>	<code>AUTH_SAP_RMMAIN_EXE</code>
<code>SAP_SMWORK_IMPL</code>	<code>AUTH_SAP_SMWORK_IMPL</code>
<code>SAP_SM_KW_ALL</code>	<code>AUTH_SAP_SM_KW_ALL</code>
<code>SAP_SM_SL_ADMIN</code>	<code>AUTH_SAP_SM_SL_ADMIN</code>
<code>SAP_SOL_TRAINING_ALL</code>	<code>AUTH_SAP_SOL_TRAINING_EDIT</code>
<code>SAP_SUPPDESK_CREATE</code>	<code>AUTH_SAP_SUPPDESK_CREATE</code>
<code>SAP_SYSTEM_REPOSITORY_ALL</code>	<code>AUTH_SAP_SYSTEM_REP_ALL</code>
<code>SAP_SM_SL_MIGRATION_72</code>	<code>AUTH_SAP_SM_SL_MIGRATION_72</code>
<code>SAP_SETUP_BASIC_ARCHIVE</code>	<code>AUTH_SAP_SETUP_BASIC_ARCHIVE</code>
<code>SAP_SETUP_SYSTEM_PREP_DISP</code>	<code>AUTH_SAP_SETUP_SYSTEM_PREP_DISP</code>
<code>SAP_SMWORK_CONFIG</code>	<code>AUTH_SAP_SMWORK_CONFIG</code>
<code>SAP_SM_FIORI_LP_EMBEDDED</code>	<code>AUTH_SAP_SM_FIORI_LP_EMBEDDED</code>
<code>SAP_SM_ROLECMP_ALL</code>	<code>AUTH_SAP_SM_ROLECMP_ALL</code>
<code>SAP_SM_SMUA_ALL</code>	<code>AUTH_SAP_SM_SMUA_ALL</code>
<code>SAP_SM_USER_ADMIN</code>	<code>AUTH_SAP_SM_USER_ADMIN</code>

Role	Help Text ID
SAP_SOLPRO_OLD	AUTH_SAP_SOLPRO_OLD
SAP_SM_SUTMAN_ADMIN	AUTH_SAP_SM_SUTMAN_ADMIN

5. Change Request Management (optional, if it is migrated): composite role SAP_CM_ADMINISTRATOR_COMP. The role must be assigned in addition to SAP_SOL_PM_COMP (see above point 1). Roles assigned in SOLMAN_SETUP to the user SMC_MIG_XXX:

Role	Help Text ID
SAP_CM_SMAN_ADMINISTRATOR	AUTH_SAP_CM_SMAN_ADMIN
SAP_ITCALENDER_DIS	AUTH_SAP_ITCALENDER_DIS
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_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

6. Quality Gate Management (optional, if it is migrated): SAP_QGM_ADMIN_COMP. The role must be assigned in addition to SAP_SOL_PM_COMP (see above point 1). Roles assigned in SOLMAN_SETUP to the user SMC_MIG_XXX:

Role	Help Text ID
SAP_CPR_PROJECT_ADMINISTRATOR	AUTH_SAP_CPR_PROJECT_ADMIN
SAP_SM_BUSINESS_PARTNER	AUTH_SAP_SM_BUSINESS_PARTNER
SAP_SM_QGM_ALL	AUTH_SAP_SM_QGM_ALL
SAP_SM_QGM_CM_ALL	AUTH_SAP_SM_QGM_CM_ALL

7. Test Workbench (optional, if it is migrated): SAP_SM_TWB_MIGRATION_72. Roles assigned in SOLMAN_SETUP to the user SMC_MIG_XXX:

Role	Help Text ID
SAP_SM_TWB_MIGRATION_72	AUTH_SAP_SM_SL_MIGRATION_72

Specific Name Space

If you create user SMC_MIG_XXX in SOLMAN_SETUP, the roles are copied in transaction SOLMAN_SETUP into name space MGR.

In Release 7.2: Run Application Specific Migration Procedures

All application specific migration procedures can be accessed via transaction SOLMAN_SETUP links in the [Related Links](#) section in folder [Data Migration](#).

→ Recommendation

For each procedure, we advise to assign in addition to the scenario-specific roles (**see scenario-specific guide**) the following roles:

- SAP_SM_SL_ADMIN (for solution data migration)
- SAP_SYSTEM_REPOSITORY_ALL (for LMDB migration)

7.7 Users Created During Installation

7.7.1 Database User SAP<SID>DB [MANAGED.DB.USER]

This database administrator user (situated in the database server) is created during the SAP engine installation of the managed system, and it is the owner of the database schema created for the system needs. The user store is the database server, group: database administrators. This user is required during the SAP Engine installation and also for some Diagnostics tools like:

- DBA Cockpit
- In case of JDBC connection problems, you are able to retrieve the full JDBC configuration by using the Diagnostics Config Tool available by running the following script: `/usr/sap/<SID>/Shortcuts/configtool`.

i Note

If you require a dedicated user for Root Cause Analysis with the corresponding credentials, it is possible to create a user with read access to the database schema.

Password change

It is strongly recommended not to update this user. If necessary, this user's password can be updated in the database administration tool. The password change has to be applied accordingly within the Configtool in the SecStore part.

7.7.2 OS Engine User [MANAGED.OS.SIDADM]

This OS user is created with the installation of the SAP Engine on the Windows platform of the managed system. This user is required to restart the managed system to take into account the Java parameter updates performed by Diagnostics.

Note that on UNIX systems the user `<SID>adm` must have an unmask like `027` as well as make sure that the group `sapsys` has at least a read access to the managed system engine files. On Windows, the recommended value for the user is `SAPService<SID>adm` in group administrators.

This user's password can be upgraded according to the local user policy.

7.7.3 OS User Dedicated to the Diagnostics Agent <SID>ADMIN [MANAGED.OS.AGTSIDADMIN]

This OS user is created during the Diagnostics Agent installation on the managed system. The default user name is: `<SID>ADMIN`. Therefore, for the UNIX system, this user has to have the required credentials to read data from the managed system, and to write them to the agent directory. It is mandatory to restart for instance Diagnostics Agent. The following platform families may be considered:

- **Managed system based on a Microsoft Windows Server**
Using Microsoft OS which involves having a user part of the administrators group OS
- **Managed system based on a UNIX OS**
On UNIX system, this user must be a member of the `sapsys` group. The Diagnostics agent temp directory must have the read, write and execute permissions for the group. This allows users belonging to `sapsys` group to have full access to it. The permission must be equal to the result of the command `chmod g+rwX` on the Diagnostics agent temp directory. This user must have the mask equal to `027` (umask).

i Note

- If your system owns a daemon task to check and restore automatically your default permissions access, you may have to adapt this daemon to remain compliant with the requirements described above.
- see [SAP Note 1163751](#)  for solution check

7.8 Configuration Authorization Objects per Procedure

7.8.1 Configuration Transaction Frame Authorization

Any time you call a transaction in the `SOLMAN_SETUP` procedures, authorization objects `S_DATASET` and `S_GUI` with value `ACTVT 61` are called.

Almost every step requires batch job authorizations, as most configuration is done as background jobs. For editing access to the transaction, you require authorization object `SM_SETUP` with `ACTVT 02` (change).

Before Starting the Configuration Transaction the First Time

The first call of the transaction `SOLMAN_SETUP` is usually done by an existing user in the system such as `DDIC` or `SAP*` with `SAP_ALL` profile authorizations.

→ Recommendation

We strongly recommend to disable at least user `SAP*` afterwards and change passwords.

When you can call the transaction `SOLMAN_SETUP` the first time, you will be prompted by a popup to activate all relevant Web Dynpro Applications. This requires the following authorizations:

- `S_TCODE`: `SOLMAN_SETUP` and `SICF` (for Service Activation)
- `S_ADMI_FCD` with value `NADM`
- `S_BTCH*` as the activation is run by a batch job
- `S_USER_GRP` with `ACTVT 03`
- `SM_WC_VIEW` with value `WD_SISE_MAIN` to be able to display the main `SOLMAN_SETUP` frame
- `SM_SETUP` for `SOLMAN_SETUP` access in general
- `SM_APP_ID` for the call authorization

Calling Transaction `SOLMAN_SETUP` the First Time

When you start to run the Solution Manager configuration, you need to call it with a dialog user via transaction `SOLMAN_SETUP`. The system directs you to the [Overview](#) page which displays the overall status for all relevant procedures that constitute the mandatory configuration of your Solution Manager system. This user requires a specific set of authorizations, which we will look at in detail in the following sections.

When you call the transaction for the first time, you are prompted with a dialog window giving you hints on what to do next.

In case, you run an update of the configuration, you may find check marks in the column [Update Needed](#) in this popup. This indicates which procedure you need to run again. The window is displayed by the system by default. No specific authorization is required.

General Authorizations For Each Call of Transaction `SOLMAN_SETUP`

Whenever you call transaction `SOLMAN_SETUP` for any of the Guided Procedures, the following set of authorization objects is always asked for by the system:

- `SM_SETUP` with `ACTVT 02`

i Note

In a trace file, `ACTVT 61` appears as checked by the Frame of the transaction `SOLMAN_SETUP`. This `ACTVT` allows to display the `SOLMAN_SETUP` log files for any of the steps. Due to its **security criticality**, it is not included in any of the configuration roles. You can either assign it separately to your users or assign role `SAP_SETUP_BASIC_ARCHIVE`, which includes as well further transactions for archiving purposes.

- S_TCODE for transaction SNOTE_DISPLAY as the central SAP Note is checked with every new call of transaction SOLMAN_SETUP.
- SM_SDK_ACT with value PROC
- SM_SDK_IBA with value ALL
- CRM_ORD_LP with reference to transaction types SMIN, SMFG, SMDT, SMOR and ACTVT 01 (create)
As CRM_ORD_LP is always set inactive in all relevant CRM related Solution Manager roles, the object is always replaced by CRM_ORD_PR. For more information on the *Authorization Concept for CRM*, see the specific section in the Guide for *Concept of Authorizations in SAP Solution Manager*.
- B_NOTIF_BC with ACTVT 41

Note, that all checked authorization objects relate to message processing in *Incident Management*. The system checks whether the user has permission to process all relevant transaction types in SOLMAN_SETUP.

7.8.2 View: System Preparation and Its Authorizations

In this paragraph, the *Guided Procedure* for the *System Preparation* is explained in more detail in regards to authorization objects and values. These authorizations reflect authorization objects which are included in roles SAP_SETUP_SYSTEM_PREP and SAP_SETUP_SYSTEM_PREP_DISP as well as SAP_SETUP_BASIC_S_DEVELOP (for SAP Note implementation).

i Note

To run only *System Preparation* successfully, you need to assign the following roles to your user:

- SAP_SETUP_SYSTEM_PREP
- SAP_SM_USER_ADMIN
- SAP_SM_ROLECMP_ALL
- SAP_SM_RFC_ADMIN
- SAP_SYSTEM_REPOSITORY_ALL
- SAP_J2EE_ADMIN
- SAP_SM_SMUA_ALL (optional)
- SAP_SMWORK_CONFIG (optional)
- SAP_SMWORK_SM_ADMIN (optional)
- SAP_SM_BP_ADMIN
- SAP_BC_STC_USER (optional for transaction STC02)

System Preparation

All mentioned authorization objects are contained in role SAP_SETUP_SYSTEM_PREP. We will therefore only reference specific fields and values in this document.

Step 1: Define System Role

There are no specific checks for this step, except for authorization object SM_SETUP to either change (ACTVT 02) or display (ACTVT 03) access.

Step 2: Run All Automatic Activities

In this *automatic* step, the following authorization objects are required.

- **S_TOCDE:** STMS for Transport Management, SLICENSE for License Management, RZ10 for System Profile Parameter Checks, SRT_ADMIN for SOAP Management

→ Recommendation

All three transactions are security - critical, we recommend to remove the transactions after you have executed the relevant steps from role SAP_SETUP_SYSTEM_PREP, if you do not disable the user after configuration.

- SM_SETUP with value 61 to display logs
- SM_WD_COMP with value C_SRT_MANAGEMENT_MAIN to access SOAP management application
- S_BTCH* as all automatic activities run in batch jobs

Step 2: Check SLD Configuration on Java

As this step refers to the Java Stack and SLD, you require role assignment SAP_J2EE_ADMIN.

Step 2: Run Post Installation on ABAP

In this *manual* step, the following authorization objects are required.

- **S_TOCDE:** STC01, STC02

i Note

Transaction STC02 requires another set of authorization objects to run required jobs successfully. You need to assign role SAP_BC_STC_USER.

- S_TC with change possibility for SAP_BASIS_SETUP_INITIAL_CONFIG
- S_GUI with ACTVT 61
- S_CTC to run CTC Scripts
- S_RZL_ADM
- S_DATASET with ACTVT 03 and 06 (delete) for program SAPLSPFL for profiles
- S_DOKU_AUT with MAINTAIN
- S_TRANSLAT with change authorization for LONG texts
- S_BTCH* as batch jobs are running

Step 2: Initialize or Update SU24 Authorizations

In this *manual* step, the following authorization objects are required.

- S_DATASET
- S_TCODE: SU25
- S_IMG_GENE with the possibility of change
- S_DOKU_AUT with the possibility to MAINTAIN

i Note

In the role SAP_SETUP_SYSTEM_PREP authorization object S_DEVELOP with ACTVT 02 and object type SUSK is set to inactive. It is per default maintained for transaction SU25, but not required for the Solution Manager setup procedure.

Step 2: Check Transaction SPAU

In this *manual* step, the following authorization objects are required.

- S_DATASET with programs SAPLSTRF and RSUMOD04
- S_TCODE: SPAU

i Note

In the trace file for this transaction, you receive authorization object S_DEVELOP as required, but without any specified values. Therefore, the object is dismissed in the according role SAP_SETUP_SYSTEM_PREP. If you need to make major changes of ABAP objects, please add the object manually to the role.

Step 2: Check Web Service Configuration

In this *manual* step, the following authorization objects are required:

- S_DATASET
- S_TCODE: SRT_ADMIN
- S_SRT_CF_P with the possibility of change

Step 2: Check Secure Web Browser Comm (HTTPS)

In this *manual* step, you are asked to configure a secure HTTP connection. This is specifically security-relevant, as your Solution Manager is accessible via Internet Browser.

→ Recommendation

Due to its **security - criticality**, we strongly recommend to configure this feature. Also check for more information in the [Authorization Concept Guide](#) the section on [Network Security](#).

The following authorization objects are required:

- S_TCODE: SMICM to check all required services
- S_GUI with ACTVT 61
- S_ALV_LAYO
- S_ALV_LAYR with ACTVT 23 for report RSMONICM

Check Virus Scan Profile Paramaters

In this *manual* step, you are asked to check the configuration for scanning attachment with virus scanner. This is especially relevant for all SAP Fiori Applications and attachment uploads.

The following authorization objects are required:

- S_TCODE: SM34
- S_TABU_NAM with table access to VSCAN_PROF
- S_TABU_DIS with general access to tables in authorization group SRZL

Step 3.1: RFC Connectivity

In this *manual* step, the following authorization objects are required:

- S_TABU_DIS with value AISU and ACTVT 02 (change)

i Note

For the connection from the SAP Solution Manager, you need to assign an S-User for the SAP Backbone connection. This S-User is entered by the system in table `AISUSER` which is assigned authorization group `AISU`.

- `S_BTCH*` as batch jobs run
- `S_USER_GRP` with `ACTVT 03`

i Note

This step also requires change and display authorization for the following transactions `S_TCODE`:

- `SM59` the authorization is contained in role `SAP_SM_RFC_ADMIN`.
- `DISPLAY_RFC` the authorization is contained in role `SAP_SM_RFC_ADMIN`.
- `LMDB` the authorization is contained in role `SAP_SYSTEM_REPOSITORY_ALL`.

Step 3.2: Support Hub Connectivity

i Note

To use this new infrastructure feature, you are required to register a new S-User in the SAP Service Marketplace.

In these *automatic* activities, the following authorization objects are required and available in role `SAP_SETUP_SYSTEM_PREP`:

- `S_TCODE` for transaction `SBGRFCCONF` to create the supervisor RFC - destination for the SOAP runtime framework, and attached authorization objects:
 - `S_BGRFC`
 - `S_RFC` with `FUGR SYST`
 - `S_RFC_ADM` with `ACTVT 01` (generate), `02` (change), `03` (display) for destinations `ABAP (03)` as well as `L` (Reference Entry) and `T` (Strat External Program) as `RFCTYPE`

i Note

These authorizations are only required to create this specific RFC - connection and can be removed/set inactive after creation from the role `SAP_SETUP_SYSTEM_PREP`.

- `S_BTCH*` with Release of Jobs authorization as batch jobs run
- `S_DATASET` with program `SAPLSSEFM`
- `S_RZL_ADM` with the possibility to create
- `S_ADMI_FCD` with value `PADM`
- `S_TC` with `ACTVT 03, 16` to execute task list

Step 3.2: Configure SOAP Runtime

For this *manual* step, the following authorization objects are required:

- `SM_APP_ID` with value `AGS_REG_USER_PI`
- `SM_WD_COMP` with value `WD_SISE_SUPHUB_CONF_PROX`

- S_TCODE for SRT_ADMIN and S_START for APPL_SOA_MANAGER which connect to the following authorization objects:
 - S_SRT_CF_P with full authorization
 - S_ADMI_FCD with values NADM and STOR
 - S_BGRFC to allow for inbound destination and outbound destination configuration for SOA.
- S_TCODE for SICF

Step 3.2: Register S-User in SAP's PI System

In this *manual* step, the following authorization object is required:

- SM_APP_ID with value AGS_REG_SUSER_PI

Step 3.2: Specify Configuration Parameters

In this *manual* step, the following authorization object is required:

- SM_WD_COMP with value WD_SISE_SUPHUB_CONF_PROX

Step 4.1 and 4.2: Corrections for SNOTE and Essential ABAP Corrections

In these *manual* steps, the following authorization objects are required:

- S_C_FUNCT with program CL_SM_BASE_SENDER with function name GET_ACCESS_INFO
- S_RFC_ADM with extended maintenance activity for RFC SAP-OSS

Step 5: Maintain Technical Users

This *manual* step requires the following authorization objects:

- S_TCODE for SU01 and PFCG with main authorization objects S_USER_*
Authorization for these two transactions is included in role SAP_SM_USER_ADMIN.

i Note

Authorization object S_USER_TCD is delivered with asterisks (*).

- S_BTCH_* for Batch Jobs
- SM_ROLECMP for Role Adjustment tool
Authorization for the Role Adjust (role comparison) tool is included in role SAP_SM_ROLECMP*.
- B_BUPA_RLT and B_BUPA_GRP in case of automatic *Business Partner* creation
Authorization for Business Partners is included in role SAP_SM_BP*.
- S_C_FUNCT with program CL_SM_BASE_SENDER with function name GET_ACCESS_INFO
- S_ESH_ADM with full authorization
- S_RFC for FUNC AGS_SISE_SET_AUSUSER as well as S_TABU_DIS with change authorization for authorization group AISU relevant for S-User creation for user SOLMAN_BTC.

7.8.3 View: Infrastructure Preparation and Its Authorizations

In this paragraph, the *Guided Procedure* for the *Infrastructure Preparation* is explained in more detail in regards to authorization objects and values. These authorizations reflect authorization objects which are included in roles SAP_SETUP_INFRA and SAP_SETUP_INFRA_DISP.

i Note

To run only *Infrastructure Preparation* successfully, you need to assign the following roles to your user in the Solution Manager system:

- SAP_SETUP_INFRA
- SAP_SM_USER_ADMIN
- SAP_SM_ROLECMP_ALL (optional)
- SAP_SM_RFC_ADMIN
- SAP_SYSTEM_REPOSITORY_ALL
- SAP_SM_GATEWAY_ACTIVATION
- SAP_SM_DASHBOARDS_DISP_LMDB
- SAP_SM_SMUA_ALL (optional)
- SAP_SMWORK_CONFIG (optional)
- SAP_SMWORK_SM_ADMIN (optional)

For BI -related configuration, you require role: SAP_SM_BI_ADMIN in the BI client.

Infrastructure Preparation

Step 1.1: SLD Connection

Within this step, specifically the following authorization objects are called:

- S_TCODE for SM59, and DISPLAY_RFC to create the SLD Connection. The authorizations are contained in role SAP_SM_RFC_ADMIN.
- S_TCODE for LMDB to register the SLD Connection. The authorizations are contained in role SAP_SYSTEM_REPOSITORY_ALL.
- S_RFC_ADM with full authorization to create the SLD Connection. The authorization is contained in role SAP_SM_RFC_ADMIN.

Within this step the dialog user is required to be assigned a role for SLD Connection depending on the SLD type:

- *Runtime SLD* assign SAP_SLD_CONFIGURATOR (no copy required)
- *Source for LMDB* assign SAP_SLD_CONTENT_SYNC (no copy required)
- *PI SLD* assign SAP_SLD_GUEST (no copy required)

Step 1.2: LMDB Synchronization

Within this step, specifically the following authorization objects are called:

- S_RFC_ADM with ACTVT 03 (display). The authorization is contained in role SAP_SM_RFC_ADMIN.
- S_BTCH_* to allow batch job execution with technical user SOLMAN_BTC (S_BTCH_NAM).

Step 1.3: LMDB Content Check

Within this step, specifically the following authorization objects are called:

- S_RFC_ADM with ACTVT 03 (display). The authorization is contained in role SAP_SYSTEM_REPOSITORY_ALL.

- `S_BTCH_*` to allow batch job execution with technical user `SOLMAN_BTC` (`S_BTCH_NAM`).

Step 2: Activities: SSO and WEBADMIN setup

Both these steps are run by a separate technical user `SM_TECH_ADM`.

Step 2: Enable Connectivity, HTTP Connectivity, and Diagnostics Agent Authentication

- `S_TCODE`: `SICF` (with according authorization objects `S_SEC_SESS` and `S_ICF_ADM`) and `S_SRT_CF_P` with `ACTVT 03` (display)
- `S_DEVELOP` for development classes for object type `WEBI`:
 - `AI_SOLMAN_ALRT_PROV_DPC`
 - `AI_SOLMAN_DIAGNOSTICS_E2E_EN`
 - `AI_DIAGNOSTICS_LANDSCAPE_API`

Steps 3.1 and 3.2: Confirm SAP BW and Maintain Users

Within this step, specifically the following authorization objects are called:

- `S_USER_*`: All relevant `S_USER_*` authorizations are included in role `SAP_SM_USER_ADMIN`

Step 3.3: Enable SAP BW

Within this step, specifically the following authorization objects are called:

- `S_RFC_ADM` included in role `SAP_SM_RFC_ADMIN` for maintaining of RFC - connections
- `S_IDOC` and `S_IDOCDEFT` for `WE30` with `ACTVT 03` (display)
- `S_TCODE`: `SCCA` (Client Administration)
- `S_TABU_CLI`, `S_TABU_DIS`, `S_TABU_NAM`, `S_TRANSLAT`, `S_CTS_ADMI` (value `TABL`), `S_ADMI_FCD` (value `PADM`), `S_PROJECT` due to call of transaction `S_TCODE`: `SM30`
- critical authorization object `S_TRANSPRT` related to transaction `SM30`
- `S_TCODE`: `SM50`, `SM51` with related authorization objects `S_BDS_DS`, `S_CTS_ADMI`
- all relevant BW authorizations are contained in role `SAP_SM_BI_ADMIN`

Step 4: Define CA Introscope

Within this step, specifically the following authorization objects are called:

- `AI_LMDB_OB` with `ACTVT 03` (display)
- `SM_APP_ID` for `SMD_EMADMIN_JAVA`
- batch job authorizations `S_BTCH_*` with `S_BTCH_NAM` for `SOLMAN_BTC` user

Step 5: Set-up E-Mail Communication

Within this step, specifically the following authorization objects are called:

- `S_TCODE`: `SCOT` with according objects `S_OC_ROLE` and `S_OC_SEND`
- `S_TABU_NAM` and `S_TABU_DIS` for `RFC_READ_TABLE`
- batch job authorizations `S_BTCH_*` with `S_BTCH_NAM` for `SOLMAN_BTC` user

Step 6: Configure CRM Basics

Within this step, specifically the following authorization objects are called:

- `S_TCODE`: `COMM_HIERARCHY`, `AICRM_PRD_SETUP_MNRO` and `AICRM_PRD_SETUP_MAT` to setup material products with according authorization objects `COM*` as well as `S_TABU_DIS` with authorization groups `SCOM`, `SZ02`; `S_RFC` with function group `SYST`, and `S_CL_FUNC`

- S_TCODE: SA38 with related authorization object S_PROGRAM with ACTVT SUBMIT for all
- S_TCODE: SM30 with related authorization objects S_TABU_NAM (table: COMC_PR_FORMAT) , S_TABU_DIS (authorization group: PRC)
- S_APPL_LOG for object SOLAR and subobject AI_CRM_PRD_IO
- S_TCODE: SE19 for BAdI Implementation possibility

Step 7: Gateway Activation

Within this step, specifically the following authorization objects are called:

- S_TCODE for SICF and /IWFND/MAINT_SERVICE
- S_TABU_DIS with change authorization for authorization group IWAD for Gateway Services
- S_ALV_LAYO
- S_ALV_LAYR for report /IWFND/R_MGW_REGISTRATION
- S_ICF_ADM for services (SICF)
- S_CTS_ADMI with security-critical authorization for TABL

The authorization are separately assigned in role SAP_SM_GATEWAY_ACTIVATION.

Step 8: Completion

Within this step, specifically the following authorization objects are called:

- S_TCODE: SMW3 with related authorization objects CRM_MW_FC
- S_TCODE: SM30 with related authorization objects S_TABU_NAM for table VSMW3, S_TBAU_DIS (authorization group: BMWC)
- critical authorization object S_TRANSPRT with ACTVT 01 (create) for CUST (Customizing) and TASK (Tasks)

7.8.4 View: Basic Configuration and Its Authorizations

In this paragraph, the *Guided Procedure* for the [Basic 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_BASIC, SAP_SETUP_BASIC_APPLOG, SAP_SETUP_BASIC_ARCHIVE, SAP_SETUP_BASIC_S_DEVELOP and SAP_SETUP_BASIC_DISP (default display role for SAP_SETUP_BASIC).

i Note

To run only [Basic Configuration](#) successfully, you need to assign the following roles to your user:

- SAP_SETUP_BASIC
- SAP_SETUP_BASIC_APPLOG
- SAP_SETUP_BASIC_ARCHIVE
- SAP_SETUP_BASIC_S_DEVELOP
- SAP_SM_USER_ADMIN
- SAP_SM_ROLECMP_ALL
- SAP_SDCCN_ALL
- SAP_SYSTEM_REPOSITORY_ALL
- SAP_SM_BP_ADMIN

- SAP_SM_SMUA_ALL (optional)
- SAP_SMWORK_CONFIG (optional)
- SAP_SMWORK_SM_ADMIN (optional)

Basic Configuration

Step 1.: Configure Basic Functions

Within this step, specifically the following authorization objects are called:

Activate SDCCN

- all needed SDCCN authorizations, see role SAP_SDCCN_ALL.

Update RFCs

- S_TCODE: SM59, see according role SAP_SM_RFC_*
- AI_LMDB_OB with ACTVT 03 (display), see according role SAP_SYSTEM_REPOSITORY_*

Activate Piece List

- S_TCODE: SCC1 (client copy) with related authorization objects S_CLNT_IMP, S_SCRP_TXT, S_DATASET for program SAPMSCC1 (required transport authorization must be added manually: Type: CLCP with ACTVT 01)
- S_TCODE: SPAM and related critical authorization object S_TRANSPRT with values PATC and ACTVT 02 (change) and 03 (display)
- critical authorization object S_CTS_ADMI with values EPS2 and TABL with ACTVT 02 (change)

Activate Services

- S_TCODE for SICF and SICF_INST .
- S_ADMI_FCD with value NADM

BW - related activities (extractor frame)

- AI_DIAG_E2E with ACTVT 03

Business Partner - related activities

- S_TCODE: BP with related authorization objects, see role SAP_SM_BP_*

Monitoring setup related activities

- authorization object SM_MOAL_TC for configuration permission monitor CONFIG and ACTVT 02 (change)
- critical authorization object S_DEVELOP with all required entries for object type ENHO with ACTVT 03 (display)
development classes:
 - AGS_BPM_NF
 - AI_SOLMAN_ALRT_AL_REACTION_ENH
 - AI_SOLMAN_ALRT_CONSM
 - AI_SOLMAN_PI_MONITORING
 - DSWP_DTM_OUTAGE_SERVICE

- AI_SOLMAN_ALRT_LOCAL_HELPER
- SM_WD_COMP with component DSWP_SD_SETTINGS

DPC Configuration

- SM_APP_ID

Step 2: Schedule Jobs

Within this step, batch authorization objects are called S_BTCH_*.

Step 3: Configure Manually

Within this step, specifically the following authorization objects are called:

Service Content Update Configuration

- S_DEVELOP with ACTVT 03 (display) for Object Type PROG and Development Class AGS_SERVICE_SESSIONS_ADMIN.
- S_TCODE: AGS_UPDATE

Connections

- AI_LMDB_OB with ACTVT 03 (display), see role SAP_SYSTEM_REPOSITORY_*

Schedule Application Log Cleanup

- S_TCODE: SLG2
- S_APPL_LOG, see role SAP_SETUP_BASIC_APPLOG

Clear Caches for Launchpad (one time activity)

- /UI2/CHIP with ACTVT 06 (Delete) for clearing of cache, see role SAP_SETUP_BASIC
- The following jobs are required:
- /IWBEP/R_MGW_MED_CACHE_CLEANUP
 - /UI2/INVALIDATE_GLOBAL_CACHES
 - /UI2/INVALIDATE_CLIENT_CACHES

NW Download Service Configuration

- S_TCODE: File with according authorization object S_TABU_DIS create, change and display authorization for all tables in authorization group SC
- S_TCODE: SM36 to manually schedule background job for NW Download Service

Step 4: Create Basic Dialog User

Within this step, specifically the following authorization objects are called:

- S_USER_*: All relevant S_USER_* authorizations are included in role SAP_SM_USER_ADMIN

Step 5: Complete

Within this step, specifically the following authorization objects are called:

- S_TCODE: AI_IMG_DISP with S_RFC and FUGR: SHI5 and ACTVT 16 (execute)
- AI_LMDB_OB with ACTVT 03 (display), see role SAP_SYSTEM_REPOSITORY_*

7.8.5 View: Managed System Configuration and Its Authorizations

In this paragraph, the *Guided Procedure* for the [Managed System 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`.

Note

To run [Managed System Configuration](#) successfully on itself, you need to assign the following roles in the Solution Manager system:

- `SAP_SETUP_MANAGED`
- `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)

Managed System Configuration

Step 1: Assign Product

Within this step, specifically the following authorization objects are called:

- `AI_LMDB_OB` with `ACTVT 03` (display) for system display, see role `SAP_SYSTEM_REPOSITORY_*`
- `S_RFC_ADM` with `ACTVT 03` for RFC - destination `LMDB_SYNCDEST1`, see role `SAP_SM_RFC_*`
- Batch authorizations `S_BTCH_*` for technical user `SOLMAN_BTC`
- `AI_DIAG_E2E` with `ACTVT 03` (display) for access to extractor framework

Step 2: Check Prerequisites

Within this step, specifically the following authorization objects are called:

- `AI_LMDB_*`, the authorization objects are contained in role `SAP_SYSTEM_REPOSITORY_*`

Step 3: Maintain RFCs

Within this step the following authorization objects are called (apart from the authorization objects that are called with every transaction call):

- `AI_LMDB_*`. The authorization objects are contained in role `SAP_SYSTEM_REPOSITORY_*`.
- `S_TABU_RFC` with `ACTVT 03` (display)
- Batch authorizations `S_BTCH_*` for technical user `SOLMAN_BTC`

Step 4: Assign Diagnostics Agent

- AI_LMDB_OB with ACTVT 03 (display) for system display, see role SAP_SYSTEM_REPOSITORY_*
- Batch authorizations S_BTCH_* for technical user SOLMAN_BTC
- SM_APP_ID with values DIAG_AGENT_ADMIN and DIAG_AGENT_CANDIDATE

Step 5 and Step 6: Enter System Parameters and Landscape Parameters

- AI_LMDB_OB with ACTVT 03 (display) for system display, see role SAP_SYSTEM_REPOSITORY_*
- Batch authorizations S_BTCH_* for technical user SOLMAN_BTC

Step 7: Maintain Users

No specific authorization required.

Step 8: Finalize Configuration

- AI_LMDB_*. The authorization objects are contained in role SAP_SYSTEM_REPOSITORY_*
- Batch authorizations S_BTCH_* for technical user SOLMAN_BTC
- SM_WD_COMP with access for WD_E2E_WC_EXTRACTOR_FWK
- SM_MOAL_TC with monitor CONFIG (configuration) of monitoring objects

Step 9: Check Configuration

- AI_LMDB_*. The authorization objects are contained in role SAP_SYSTEM_REPOSITORY_*
- SM_WD_COMP with access for WD_DIAG_MAIN
- AI_DIAG_E2E for Extractor Framework permission
- S_RZL_ADM with ACTVT 01 (create)
- S_ADMI_FCD with value STOR

Step 10: Complete

- AI_LMDB_*. The authorization objects are contained in role SAP_SYSTEM_REPOSITORY_*
- Batch authorizations S_BTCH_* for technical user SOLMAN_BTC
- SM_WD_COMP with access for AGS_WORKCENTER_FW

Additional Access Links and Authorizations

System Recommendation

If your user requires to access [System Recommendation](#), you need to assign the relevant roles for it, SAP_SYSTEM_RECOMMEND_*_COMP.

7.8.6 View: Embedded Search

In this paragraph, the *Guided Procedure* for the [Embedded Search](#) is explained in more detail in regards to authorization objects and values.

i Note

This procedure can be configured by using the user `SOLMAN_ADMIN`. To run only *Embedded Search* successfully on its own, you need to assign the following roles to your user:

- `SAP_SETUP_SYSTEM_PREP`
- `SAP_SM_ESH_ADMIN`
- `SAP_SM_TREX_ADMIN`
- `SAP_SM_RFC_ADMIN`
- `SAP_SYSTEM_REPOSITORY_ALL`
- `SAP_SMWORK_CONFIG` (optional)

Step 1: Perform General Configuration

All mentioned roles above are relevant.

Step 2: Check Scenario Configuration

Embedded Search is a cross-scenario configuration which is relevant for the following scenarios:

- Requirements Management
- Process Management
- Quality Gate Management
- Change Request Management
- IT Service Management
- SAP Engagement and Service Delivery

Role `SAP_SM_ESH_ADMIN`:

- contains individual access authorization `SM_SETUP` to all required individual steps of *Embedded Search Configuration* in the guided procedures above
- allows the configuration of all activities for *Embedded Search* in these guided procedures.

i Note

For display, role `SAP_SM_ESH_DIS` is available.

7.8.7 View: Usage Logging

In this paragraph, the *Guided Procedure* for the *Usage Logging* is explained in more detail in regards to authorization objects and values. Several different scenarios rely on usage information (`UPL/SCMON`) for ABAP objects. To be able to leverage the usage history of ABAP objects, usage logging needs to be activated in the managed system and collected by the SAP Solution Manager system.

i Note

This procedure can be configured by using the user `SOLMAN_ADMIN`. To run only *Usage Logging* successfully on its own, you need to assign the following roles to your user:

- `SAP_SETUP_SYSTEM_PREP`
- `SAP_SETUP_BASIC_ARCHIVE`
- `SAP_SM_RFC_ADMIN`
- `SAP_SM_USAGE_LOG`
- `SAP_SYSTEM_REPOSITORY_DIS`
- `SAP_SMWORX_CONFIG` (optional)

Step 1: Check UPL/SCMON background jobs

The jobs checked are: `SM:SCMON_UPLOAD_STATUS_HK` and `SM:SCMON_CONTROL`. All mentioned roles above are relevant.

Step 2: Check Recommended SAP Notes

SAP NOTE display access is given in role `SAP_SM_USAGE_LOG`.

Step 3: BW Content Activation (UPL)

The authorization for Batch Job is contained in role `SAP_SM_USAGE_LOG`.

Affected Scenarios

Usage Logging is a cross-scenario configuration which is relevant for the following scenarios:

- Custom Code Management
- Business Process Change Analysis (BPCA)
- SEA
- System Recommendation

7.8.8 View: Additional Security Recommendations

In this paragraph, the GP for the [Additional Security Recommendation](#) is explained in more detail in regards to authorization objects and values.

Note

This procedure can be configured by using the user `SOLMAN_ADMIN`. To run only [Additional Security Recommendation](#) successfully on its own, you need to assign the following roles to your user:

- `SAP_SETUP_SECURITY_REC` for change access or `SAP_SETUP_SECURITY_REC_DIS` for display access
- `SAP_SETUP_BASIC_APPLOG`
- `SAP_SETUP_BASIC_ARCHIVE`
- `SAP_SYSTEM_REPOSITORY_DIS`
- `SAP_SMWORK_CONFIG`

Check Virus Scan Profile Parameters

Virus Scans should be implemented for any system if attachments are used within any application.

- transaction `SICF`: with authorization object `S_ICF_ADM`
- transaction `SM34`: with authorization object `S_TABU_NAM` with tables `V_VSCAN_PROF_GRP`, `V_VSCAN_PROF_PAR`, `V_VSCAN_PROF_PGL`, `V_VSCAN_PROF_MIM` (`S_TABU_DIS` with value `SRZL`) to set profile parameters for the VSI profile in table `SCAN_PROFILE_VC`.
- authorization object `SM_VCUST` for GPA
- authorization object `SM_WD_COMP`
- authorization object `SM_GPACUST` for GPA
- authorization object `S_BTCH_ADM`
- authorization object `SM_SETUP` with value `AGS_SECUR`

7.8.9 View: Scenario Configuration and Its Authorizations

This paragraph deals with scenario - specific configuration procedures.

Roles and Users

To be able to configure any of the scenario Guided Procedures with a set of minimal authorizations, we recommend to use template user `SMC_<scenario>`. You can create this user either immediately when starting the configuration, or use the `SMUA` application. All configuration users must have assigned one specific

configuration role for the respective scenario `SAP_*<scenario>_CONF*` and a number of additional roles for various purposes required during the configuration process, such as for user generation, SAP Fiori application permission, RFC generation or other topics. The users and their roles are described in the [Application - Specific Security Guide](#) with reference to the specified scenario.

→ Recommendation

We strongly discourage you from using profile `SAP_ALL`, even for a short time frame. For more information on Security Optimization and Restrictions during operation, see [Optimization Security Guide](#).

Mandatory and Optional Activity Configuration

Each scenario Guided Procedure contains a number of mandatory activities and optional activities. In order to run only the minimal scenario, all mandatory activities must be performed. The following entry in the SCN gives a short overview on the advantages and disadvantages of such an approach: <https://blogs.sap.com/2017/08/14/sap-solution-manager-7.2-it-service-management-quick-setup/> 📄

7.9 SAP Solution Manager Configuration Users

7.9.1 Introduction

Configuration Default Users in transaction SOLMAN_SETUP

User Default Names

All configuration users for transaction `SOLMAN_SETUP` procedures are created by the system in name space `<SMC>` (Solution Manager Configuration), with the exception of the configuration user for the [Basic Configuration](#) of Solution Manager itself `SOLMAN_ADMIN`.

Creation and Update

Whenever any dialog user, with permission to enter the transaction `SOLMAN_SETUP`, attempts to access any of the specific procedures, the system:

1. compares authorization objects and authorization fields of the accessing dialog user with the authorizations required for according predefined configuration user.
2. displays a dialog window with the recommendation to create user `SOLMAN_ADMIN`, if any of the required authorization objects and authorization fields is missing due to the comparison.

In case of updates, due to a new Support Package or similar, the same procedure applies.

→ Recommendation

We recommend to use the predefined configuration users for the configuration, as the authorizations assigned to these users are specifically tailored to the individual procedure. In this way, you can ensure,

that the user cannot be misused to any other task. As the user name is only a suggestion, you can also rename the user.

Role Assignments (Authorizations)

All SMC_*[Configuration Users](#) receive the following roles and according authorizations:

- SAP_*_CONF* role: contains all relevant application specific authorizations
- SAP_SM_SMUA_ALL role: contains full authorization for [Mass User](#) creation in the Solution Manager User Administration
- SAP_SM_ROLECMP_ALL role: contains full authorization for the [Role Adjust](#) tool within transaction SOLMAN_SETUP.
- SAP_SM_USER_ADMIN role: contains full authorization for [User Management](#) (transaction SU01) and [Role Management](#) (transaction PFCG).

Depending on the application integration, for instance BW or CRM, additional roles may apply.

Creating Configuration Users using Projects

For any scenario, which is configured using transaction SPRO, you can create configuration users using projects. For more information, see [How to Create Configuration Users with Projects](#).

7.9.2 Solution Manager Configuration User SOLMAN_ADMIN

When you configure your Solution Manager **initially**, you need to create your configuration user (user type: dialog user). Per default this user is called SOLMAN_ADMIN. You can use the default user name, but you can also use any other user name. You can use this user for configuration and update of views:

- [System Preparation](#)
- [Infrastructure Preparation](#)
- [Basic Settings](#)
- [Managed System Settings](#) including [Cloud Services](#)

i Note

To be able to run [Advanced](#) guided procedures, you must maintain the authorization object SM_SETUP within role SAP_SETUP_SET_MANAGED for the specific guided procedure ID, as it is not included in the object per default.

- [Early Watch Alert Management](#)
- [Service Level Management](#)
- [Embedded Search](#)
- [Usage Logging](#)
- [Additional Security Recommendation](#)

i Note

As of **SP03**, SOLMAN_ADMIN user is not allowed to execute [Root Cause Analysis \(RCA\)](#) due to the security critical principle of [Segregation of Duty](#). To run [RCA](#), use dialog user SAPSUPPORT. This user can be created

automatically by `SOLMAN_ADMIN` user in the Guided Procedure [Basic Configuration](#). Alternatively, you can assign the required authorization for [RCA](#) using the Solution Manager User Administration ([SMUA](#)).

How to Create/Update the User

Whenever any dialog user with permission to enter the transaction `SOLMAN_SETUP`, attempting to access one of the above mentioned procedures, the system:

1. compares authorization objects and authorization fields of the accessing dialog user with the authorizations required for dialog user `SOLMAN_ADMIN`.
2. displays a dialog window with the recommendation to create user `SOLMAN_ADMIN`, if any of the required authorization objects and authorization fields is missing due to the comparison.

In case of updates of the Support Package or similar, the same procedures applies. The user can also be updated or created using the link [Create/Update User SolMan Administrator](#) in the [Related Links](#) section of the User Interface.

→ Recommendation

We recommend to create and update user `SOLMAN_ADMIN` for the configuration. As the user name is only a suggestion, you can also rename the user.

Multiple Configuration Users - Segregation of Duty

You can separate the tasks to a number of different users. This is possible by using authorizations:

- **Access mode restriction:** You can allow a user to only be able to access the procedure in [Display](#) mode by restricting to `ACTVT 03` in authorization object `SM_SETUP`.
- **View restriction:** You can allow for the display and access to specific procedures by restricting authorization object `SM_WC_VIEW`.
- **Topic restriction:** You can allow for access to only specific steps within the procedures using authorization object `SM_SETUP`. For instance: You can allow for a specific administrator for users and authorizations, only to be able to edit user - specific steps and display others. Similarly, you can allow an administrator to be only responsible for BW - related setup to access only those steps in [Edit](#) mode, and so on.

Role Assignment

The user `SOLMAN_ADMIN` is created by the system automatically during the automated configuration procedure in transaction `SOLMAN_SETUP`, or Work Center SAP Solution Manager Configuration. It is assigned a number of different roles for various purposes.

SAP delivers all roles in SAP name space (SAP roles). When assigning the roles, the system automatically detects which roles need to be copied in a customer name space `<Z>` (customer roles) or Java related roles. For instance, navigation roles for work center usage (`SAP_SMWORK_<work center>`) do not need to be copied into the customer names space, as they do not contain any relevant authorization objects, but only menu options. The user interface shows you which roles should be copied into a name space. Before copying the roles, you can choose your own name space for the roles that are automatically copied by the system. To do

that, enter your name space instead of the <z> - name space in the column for *Copy from SAP Role* before you create the roles.

The system automatically assigns the selected roles to the SOLMAN_ADMIN user, and generates the according profiles. This allows the user to immediately function as all authorization values in the mentioned roles are delivered with dedicated values. For all fields that are generic, the value asterisk (*) is delivered.

Therefore, if you want to change delivered values, you still need to maintain the authorization objects for the according role manually. For more information, read the *Role Description* for the according role. The role description is provided in the according screen in the user interface of the guided procedure.

The following table gives you an overview over the roles assigned to this user.

Default Roles Assigned to User SOLMAN_ADMIN (Help Text ID: USER_SOLMAN_ADMIN)

Assigned Roles	Help Text — ID
for Basic Configuration	
SAP_J2EE_ADMIN	AUTH_SAP_J2EE_ADMIN
SAP_RCA_AGT_ADM	AUTH_SAP_RCA_AGT_ADM
SAP_BC_SDS_CONF_ADMIN	AUTH_SAP_BC_SDS_CONF_ADMIN
SAP_SETUP_BASIC	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_APPLOG	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_ARCHIVE	AUTH_SAP_SETUP_BASIC
SAP_SETUP_BASIC_S_DEVELOP	AUTH_SAP_SETUP_BASIC
SAP_SETUP_INFRASTR	AUTH_SAP_SETUP_INFRASTR
SAP_SETUP_SYSTEM_PREP	AUTH_SAP_SETUP_SYSTEM_PREP
SAP_SETUP_MANAGED	AUTH_SAP_SETUP_MANAGED
SAP_SETUP_SECURITY_REC	AUTH_SAP_SETUP_SECURITY_REC
SAP_SM_ESH_ADMIN	AUTH_SAP_SM_ESH_ADMIN
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN
SAP_SM_BI_ADMIN	AUTH_SAP_SM_BI_ADMIN
SAP_PI_CCMS_SETUP	AUTH_SAP_PI_CCMS_SETUP
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR
SAP_SMWORK_BASIC	AUTH_SAP_SMWORK_BASIC
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG

Assigned Roles	Help Text — ID
for Basic Configuration	
SAP_SM_DASHBOARDS_DISP_LMDB	AUTH_SAP_SM_DASHBOARDS_DISP_LMDB
SAP_RCA_CONFIG_ADMIN	AUTH_SAP_RCA_CONFIG_ADMIN
SAP_SM_RFC_ADMIN	AUTH_SAP_SM_RFC_ADMIN
SAP_SM_GATEWAY_ACTIVATION	AUTH_SAP_SM_GATEWAY_ACTIVATION
SAP_SM_SYM_TRANSPORT	AUTH_SAP_SM_SYM_TRANSPORT
SAP_BC_SDS_CONF_ADMIN	AUTH_SAP_BC_SDS_CONF_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBEDDED
SAP_SM_TREX_ADMIN	AUTH_SAP_SM_TREX_ADMIN
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP_ADMIN
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REPOSITORY_ALL
SAP_SOLMAN_SETUP_ADMIN_DIS	AUTH_SAP_SOLMAN_SETUP_ADMIN_DIS
Optional: Mass User Management	
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
Optional: Role Comparison Tool	
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
Optional: Role for SDCCN Usage (EWA)	
SAP_SDCCN_ALL	AUTH_SAP_SDCCN_ALL
Optional: Role Usage Logging	
SAP_SM_USAGE_LOG	AUTH_SAP_SM_USAGE_LOG

After creating the `SOLMAN_ADMIN` user, you continue configuring your SAP Solution Manager system using this user. This user creates other users you need in the system, such as user `SMD_RFC`, `SAPSUPPORT`, and so on. These users are described in more detail in the following sections.

i Note

- If you require transaction `ST22` for Dump Analysis, please add this authorization manually.

Role for Rapid Content Delivery (RCD)

You can download the content/Support Packages of Software Component `ST-CONT` from the Service Marketplace and then import and apply the content within the individual Solution Manager applications. This

requires a RFC - connection to the SAP Support Portal. The applications like Technical Monitoring or Guided Procedures pull the content from the RCD application. The RCD application itself is integrated in the SAP Solution Manager Administration work center, see application specific guide.

Roles SAP_SETUP*** for individual Guided Procedures in Cross Scenario Settings

All roles with prefix SAP_SETUP* refer to the configuration procedures executed by SOLMAN_ADMIN user. All authorization objects in these roles are maintained. The following roles are relevant for each individual Guided Procedures:

- SAP_SETUP_INFRASTR (Infrastructure Configuration)
- SAP_SETUP_SYSTEM_PREP (System Preparation)
- SAP_SETUP_BASIC (Basic Settings)
- SAP_SETUP_BASIC_APPLOG (Basic Settings Application Log)
- SAP_SETUP_BASIC_ARCHIVE (Basic Settings Archiving)
- SAP_SETUP_BASIC_S_DEVELOP (Basic Settings Development Authorization)
- SAP_SETUP_MANAGED (Managed System Configuration)

For each of these roles a display role is shipped. For more information on specific authorizations within these roles, see according sections for *Configuration Authorizations* for the individual *Guided Procedures*.

Optional: Role Comparison Tool: Role Adjustment

⚠ Caution

The use of this tool can be critical, as it allows manipulation of any customer roles if authorization is given.

You can use SOLMAN_ADMIN user to use the [Role Comparison Tool](#) for comparing your own customer roles with updated SAP Standard roles in transaction SOLMAN_SETUP per user. You can also create a specific user for this task, manually. You need to assign this user the following authorizations/roles:

- SAP_SM_ROLECMP_ALL
The role contains authorization for role adjustment, authorization object SM_ROLECMP.
- SAP_SM_USER_ADMIN
- In addition, you need to assign authorization objects S_TCODE (for SOLMAN_SETUP) and SM_SETUP with ACTVT 03 (Display) to access transaction SOLMAN_SETUP, as well as ACTVT 02 to be able to maintain the [User Creation](#) step.

i Note

Role SAP_SM_ROLECMP_ALL is assigned to all configuration users, created in [Basic Configuration](#) in transaction SOLMAN_SETUP, technical names: SMC_***.

Optional: Incident Management Integration

To allow the SOLMAN_ADMIN user to create [Incidents](#), you need to assign role SAP_SUPPDESK_CREATE additionally.

Optional: SDCCN Usage

In case you have used user SOLMAN_ADMIN to activate transaction SDCCN and consequently run all required background jobs for SDCCN (/BDL/*) with his user, you need to have role SAP_SDCCN_ALL assigned. This role contains authorization for authorization object S_DEVELOP.

→ Recommendation

Activate `SDCCN` with a separate technical user for background jobs. This allows you to lock the configuration user `SOLMAN_ADMIN` after configuration.

Transporting Custom User Role

It is possible to document custom (name space) - roles for SAP Solution Manager in transport requests.

Prerequisites for Usage

- configured *Automatic Recording of Changes* in transaction `SCC4`
- configured *Transport Management*
- The according user requires authorization object `S_TRANSPRT`

i Note

It is only possible for SAP Solution Manager.

Update Configuration

i Note

When you **update** your Solution Manager, you need to check the user authorizations for this user again, and update its authorizations. This is described in the according screen in transaction `SOLMAN_SETUP`.

Role Restriction During Administration and Operation

After the configuration or update of the configuration of SAP Solution Manager, you can restrict authorizations for the user `SOLMAN_ADMIN`, if needed. For instance, role `SAP_J2EE_ADMIN` allows administration authorization for all areas of `J2EE`. To separate and/or restrict this authorization, you can de-assign this role to user `SOLMAN_ADMIN` and assign the relevant restrictive roles. In addition, the following roles should be **de-assigned after configuration** is done, without status change in `SOLMAN_SETUP`:

- `SAP_SM_USER_ADMIN`
- `SAP_SM_GATEWAY_ACTIVATION`
- `SAP_SM_ROLECMP_ALL`

Restricting Role `SAP_J2EE_ADMIN` for User `SOLMAN_ADMIN`

Assigned Roles	Restricting roles	Help Text - ID
SAP_J2EE_ADMIN	SAP_RCA_AGT_ADM	AUTH_SAP_RCA_AGT_ADM
	SAP_JAVA_NWADMIN_ CENTRAL_READONLY	no Help Text ID, see the according security guide for NW Java
	SAP_RCA_AGT_ADM_VIA_SLD	This role allows to use the Expert User Interface in Java for the Agent Candidate Management. It should only be assigned to specified users.
	sap.com/tc~monitoring~systeminfo*sap_monitoring/SystemInfo_Support_Role	no Help Text ID, see the according security guide for NW Java
	sap.com/SQLTrace*OpenSQLMonitors / Open-SQLMonitorLogonRole	no Help Text ID, see the according security guide for NW Java
	SAP_SLD_GUEST	Read access to SLD
		⚠ Caution If you restrict access to technical systems in the ABAP stack, using authorization object AI_LMDB_OB, a user with access to SLD and role SAP_SLD_GUEST can read all system information in SLD.

Critical Authorizations

Authorization Object SM_SETUP

The authorization object SM_SETUP controls whether a user can access transaction SOLMAN_SETUP. In addition, it controls which functions can be used by user SOLMAN_ADMIN within this transaction. User SOLMAN_ADMIN can therefore:

- maintain all basic configuration steps
- display all views in the navigation panel for scenario-specific procedures

Authorization Object S_USER_GRP

SOLMAN_ADMIN user receives authorization object S_USER_GRP with ACTVT 05 (unlock). This authorization is used to unlock locked users during the configuration of users (create, update).

ACTVT 03 (display) is added for the user to check the status of the BACK RFC-user.

Authorization Object S_RFC_ADM

This object allows the user to have access to transaction SM59 (coupled with authorization object S_TCODE: SM59). This authorization is included in the separate role SAP_SM_RFC_***. If you do not want to allow the

configuration user to maintain RFCs after the configuration of the managed system has been executed, you can remove the role and the authorizations.

i Note

If this authorization object is not assigned to the user who is allowed to display any User Interface with users, roles, and RFC - connection on the same screen such as in transaction `SOLMAN_SETUP` or in transaction `SMUA`, the system does not display the RFC - connection information. This can be the case for instance for the User Interface for creating managed system users `READ` or `TMW`.

7.9.3 Configuration Users SMC* for Application-Specific Procedures**

For every procedure in transaction `SOLMAN_SETUP`, you can create a specified configuration user.

User Naming Convention

The configuration user default name prefix is `<SMC>` for **S**olution **M**anager **C**onfiguration. In addition, the user receives a specific middle name referring to the scenario procedure for which it can be used, such as `<BPCA>` for **B**usiness **P**rocess **C**hange **A**nalysis, and the System ID of the Solution Manager.

❖ Example

The configuration user name for a BPCA procedure in `SOLMAN_SETUP` for a SAP Solution Manager with System ID XYZ would be `SMC_BPCA_XYZ`.

User Creation

→ Recommendation

We recommend to use default user `SOLMAN_ADMIN` to create any of the scenario-specific configuration users `SMC*`.

You can create the configuration users `SMC_***` as follows:

Create User When Calling the Scenario Procedure in Transaction SOLMAN_SETUP

When you call a scenario procedure in transaction `SOLMAN_SETUP` to configure the scenario, the system prompts you with the possibility to create a separate configuration user with specific authorizations necessary for the relevant procedure. You can then decide, if you want to:

- create the `SMC_***` user with the recommended authorizations
- keep your present user and adjust its authorizations

Update of the user is only allowed if the user with whom the user update is run fulfills the following prerequisites. The user

- does not have profile a `SAP_ALL` or is DDIC user (or a user with `SAP_ALL` profile)
- is assigned role `SAP_SM_USER_ADMIN`
- has authorization object `SM_SETUP` permission for the relevant scenario
- use another user and add the recommended authorizations

→ Recommendation

Due to security reasons, we recommend:

- not to use a user with profiles `SAP_ALL` and `SAP_NEW` for configuration
- only allow the configuration user actively in the system for the time of configuration, and lock it afterwards or set limited *Time Validity*.

i Note

You can deactivate this pop-up using the *Personalization* link, whenever roles are updated with authorization objects by SAP. This does not work though for newly shipped roles. Mark the box for **Logged on User**.

Create User in Solution Manager User Administration Tool (SMUA)

At any time, you can create one or many Configuration Users within the SMUA application. The application is accessible in:

- transaction `SOLMAN_SETUP` and the Solution Manager Configuration Work Center in the *Related Links* area
- Solution Manager Administration Work Center in view *Users*

The application can be accessed with the according authorizations (object `SM_SMUA`) for the SMUA tool, role `SAP_SM_SMUA_ADMIN`.

Assigned Authorization Roles

According to the modular approach, the user receives all relevant single roles for the required functionality as well as a core role for configuration. This role contains all specific authorization objects for the procedure, such as specific maintenance of authorization objects for transaction `SOLMAN_SETUP` such as `SM_WC_VIEW`, `SM_SETUP`, and `SM_WD_COMP`, as well as all specific application relevant authorization objects. In case of `BPCA` for instance, that would be authorization object `SM_BPCA` and others.

All relevant roles for the individual configuration users are listed in the *Application-Specific Guide* for SAP Solution Manager in the according section.

Transporting Custom User Role

It is possible to document custom (name space) - roles for SAP Solution Manager in transport requests.

Prerequisites for Usage

- configured [Automatic Recording of Changes](#) in transaction SCC4
- configured [Transport Management](#)
- The according user requires authorization object S_TRANSPRT

i Note

It is only possible for SAP Solution Manager.

Specific Authorization Objects

SLG1 Application Log S_APPL_LOG

You can display the application log for transaction SOLMAN_SETUP, specifically for the HTML report available and who has generated the report. The object for the authorization restriction in S_APPL_LOG is SM_SETUP with sub-object SM_REPORT.

7.10 SAP Solution Manager Technical Users

7.10.1 Introduction

In this section, all technical users are described, which are created in the SAP Solution Manager system in transaction SOLMAN_SETUP view [Infrastructure Preparation](#). Not described are users created in the managed systems, BW - users, SLD users, and S - users.

7.10.2 Technical User SM_INTERN_WS

The technical user SM_INTERN_WS is used for internal web service communication between the ABAP and Java stack of SAP Solution Manager.

Roles Assigned to User SM_INTERN_WS (Help Text ID: USER_SM_INTERN_WS)

Assigned Roles	Help Text-ID
SAP_SM_INTERN_WS	AUTH_SAP_SM_INTERN_WS
SAP_J2EE_ADMIN	AUTH_SAP_J2EE_ADMIN

7.10.3 Technical User SM_EXTERN_WS

To ease support (user tracing) and a potential user locking, the technical user `SM_EXTERN_WS` is used for external web service communication between Diagnostics Agents and SAP Solution Manager.

User Role for SM_EXTERN_WS (Help Text ID: USER_SM_EXTERN_WS)

Assigned Roles	Help Text-ID
SAP_SM_EXTERN_WS	AUTH_SAP_SM_EXTERN_WS
SAP_J2EE_ADMIN	AUTH_SAP_J2EE_ADMIN

Authorization Objects

Batch Job Authorizations S_BTCH*

Batch Job Authorization in role `SAP_SM_EXTERN_WS` are maintained with full authorizations, as the user needs to run a number of jobs to configure system settings for *Monitoring* data, see *Application - Specific Guide* for scenario *Technical Monitoring*.

7.10.4 Technical User SOLMAN_BTC

During System Preparation, you create this technical user (user type: system user) to run all batch jobs (see table `SMCONFIGJOBS`) that are relevant for the basic configuration including the update of the `MAI` - configuration after an upgrade to a new Support Package. The default name for the user is `SOLMAN_BTC`. This user must receive role `SAP_SM_BATCH` which contains all relevant authorizations.

For changes per Support Package, (see also).

If you set up `BW` as standard scenario (local), you also need to assign role `SAP_BI_E2E` for the user to execute all `BW` - related batch jobs.

User Roles for User SOLMAN_BTC (Help Text ID: USER_SOLMAN_BTC)

Assigned Role	Help Text-ID
SAP_SM_BATCH	AUTH_SAP_SM_BATCH

Assigned Role	Help Text-ID
SAP_BI_E2E	AUTH_SAP_BI_E2E
i Note This role is only assigned in case BW resides in the same system and client (Standard Scenario)	

List of Background Jobs

All relevant jobs for basic configuration which run with `SOLMAN_BTC` are listed in transaction `SOLMAN_SETUP` in view *Basic Configuration* in step 2 *Schedule Jobs*. If you would like to run a job which is not in the list, you require a different user or you need to add additional authorizations. Then, you need to trace the authorization for this job and add it to `SOLMAN_BTC` at your own risk. We advice to have a separate role and check for critical authorization combinations. All background jobs that run with this user can also be found in SAP Note [894279](#) .

Authorization Check Report for Rapid Content Delivery Application

To be able to automatically download the content using NetWeaver Download Service and upload again into the system, a background job is started for the program `RCSU_PREREQ_CHECK` using `SOLMAN_BTC` user. To be able to check the log for this application, run transaction `SLG1` with object `RCD` and sub-object `TROUBLESHOOT`.

→ Recommendation

If you do want the `SOLMAN_BTC` user to run the job, due to the criticality of the authorization check report, you can deactivate authorization object `S_PROGRAM` with value `RCSU_PREREQ_CHECK`. We recommend to run the job with a dedicated specific user.

7.10.5 Technical User SMD_RFC

The `SMD_RFC` user is created by user `SOLMAN_ADMIN` during runtime for communication between Root Cause Analysis/Java and SAP Solution Manager /ABAP.

Role Assignment to User SMD_RFC (Help Text ID: USER_SMD_RFC)

Assigned Role	Remarks
SAP_SM_WEBSERVICE_ADMIN	ABAP authorization role, full authorization for Java stack

Assigned Role	Remarks
SAP_SOLMANDIAG_E2E	ABAP authorization role, for diagnostics

Authorization Object S_BTCH_JOB

Authorization object S_BTCH_JOB contains ACTVT DELE (delete). Whenever there is a change in the LMDB, such as due to a result of the SLD->LMDB content synchronization or triggered by Outside Discovery, the job SAP_LMDB_NOTIFY_LDB_* is released to inform LMDB notification consumers. Generally, there is only one notification job running at a time. As a consequence, the user SMD_RFC which is used by Outside Discovery, is allowed to create, release and delete SAP_LMDB_NOTIFY_LDB_* jobs.

7.10.6 Technical User SM_EFWK

The SM_EFWK user is created by user SOLMAN_ADMIN in the Solution Manager system during the BW setup. The user is used to run the step report E2E_EFWK_RESOURCE_MGR in the Job EFWK_RESOURCE_MANAGER (Extractor Resource Manager). The job itself is scheduled by the batch user SOLMAN_BTC. Which roles the user is assigned to depends on two major factors:

- In which system runs BW?
Depending on whether BW runs in the same client as the productive Solution Manager (local), or in a remote BW scenario, the user receives a dedicated set of roles. If BW runs local, then, apart from running the program for the extractors the SM_EFWK also takes over the loading of data into BW.
- For which scenarios is BW - reporting required?
Depending on the scenario-specific dedicated BW - roles need to be assigned to the user for executing the program E2E_EFWK_RESOURCE_MGR and for loading data into BW.

The following sections describe which roles are assigned to the user for which task and scenario:

Case of Remote BW

Automatic Role Assignment to User SM_EFWK for running program E2E_EFWK_RESOURCE_MGR

i Note

If BW runs remote, loading of data is executed by technical user SMD_BI_RFC in the BW system.

Assigned Role	Help Text ID	Scenario-relevance
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR	for all scenarios

Assigned Role	Help Text ID	Scenario-relevance
SAP_SOLMANDIAG_E2E	AUTH_SAP_SOLMANDIAG_E2E	Root Cause Analysis
SAP_SM_TWB_EXTRACTOR	AUTH_SAP_SM_TWB_EXTRACTOR	Test Management
SAP_SM_ICI_EXTRACTOR	AUTH_SAP_SM_ICI_EXTRACTOR	Ici Dashboards
SAP_SM_INC_EXTRACTOR	AUTH_SAP_SM_INC_EXTRACTOR	Incident Management
i Note Role contains authorization object ACO_SUPER for PPM to read projects. You can set this object inactive, if you do not use cProjects.		
SAP_SM_CHARM_EXTRACTOR	AUTH_SAP_SM_CHARM_EXTRACTOR	Change Request Management
SAP_SM_BI_ESR_EXTRACTOR	AUTH_SAP_SM_BI_ESR_EXTRACTOR	Enterprise Reporting
SAP_SM_CCDB_EXTRACTOR	AUTH_SAP_SM_CCDB_EXTRACTOR	CCDB
SAP_SM_DVM_EXTRACTOR	AUTH_SAP_SM_DVM_EXTRACTOR	Data Volume Management
SAP_SM_CV_EXTRACTOR	AUTH_SAP_SM_CV_EXTRACTOR	Configuration Validation
SAP_SM_MAI_EXTRACTOR	AUTH_SAP_SM_MAI_EXTRACTOR	MAI Framework
SAP_SM_BATCH_RELE	AUTH_SAP_SM_BATCH_RELE	Batch job release authorization for BPO Data Collectors to run
SAP_SMPI_AUTH_EXTRACTOR	AUTH_SAP_SMPI_AUTH_EXTRACTOR	The role contains authorizations (/SDF/*) delivered with Software Component ST-PI, which are required in the Solution Manager system for extractor usage.
i Note See also SAP Note 1899598		

Case of Local BW

Automatic Role Assignment to User SM_EFWK for running program E2E_EFWK_RESOURCE_MGR

Assigned Role	Help Text ID	Scenario-relevance
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR	for all scenarios
SAP_SOLMANDIAG_E2E	AUTH_SAP_SOLMANDIAG_E2E	Root Cause Analysis
SAP_SM_TW_B_EXTRACTOR	AUTH_SAP_SM_TW_B_EXTRACTOR	Test Management
SAP_SM_ICI_EXTRACTOR	AUTH_SAP_SM_ICI_EXTRACTOR	Ici Dashboards
SAP_SM_INC_EXTRACTOR	AUTH_SAP_SM_INC_EXTRACTOR	Incident Management
SAP_SM_CHARM_EXTRACTOR	AUTH_SAP_SM_CHARM_EXTRACTOR	Change Request Management
SAP_SM_BI_ESR_EXTRACTOR	AUTH_SAP_SM_BI_ESR_EXTRACTOR	Enterprise Reporting
SAP_SM_CCDB_EXTRACTOR	AUTH_SAP_SM_CCDB_EXTRACTOR	CCDB
SAP_SM_DVM_EXTRACTOR	AUTH_SAP_SM_DVM_EXTRACTOR	Data Volume Management
SAP_SM_CV_EXTRACTOR	AUTH_SAP_SM_CV_EXTRACTOR	Configuration Validation
SAP_SM_MAI_EXTRACTOR	AUTH_SAP_SM_MAI_EXTRACTOR	MAI Framework
SAP_SM_BATCH_RELE	AUTH_SAP_SM_BATCH_RELE	Batch job release authorization for BPO Data Collectors to run
SAP_SMPI_AUTH_EXTRACTOR	AUTH_SAP_SMPI_AUTH_EXTRACTOR	The role contains authorizations (/SDF/*) delivered with Software Component ST-PI, which are required in the Solution Manager system for extractor usage.
i Note See also SAP Note 1899598		
SAP_BI_E2E	AUTH_SAP_BI_E2E	Data Load

7.10.7 Technical User SM_AMSC

This technical user is used during the **Automated Managed System Configuration** to run the update job in the Solution Manager - system. The user is assigned the following role `SAP_SM_MS_SETTINGS`.

The following use cases are handled by this user:

- Read RFC destination update
- Java Server Node removed
- Java Server Node added
- ABAP client removed

- Delete, add, remove Instance
- Instance moved to different physical host
- Product Version/Instance upgraded
- Product Version/Instance added, removed
- Update `SLD` Content

i Note

The `LMDB` notification job runs with user `SOLMAN_BTC`.

Specific Authorization Objects

S_ADMI_FCD

The role contains authorization object `S_ADMI_FCD` with value `DBA`. One use case of `AMSC` is the automatic adoption to rename a host name. For this purpose, the user calls the `DBA Cockpit` setup and provides the new host name. All configuration steps for the remote connection in `DBA Cockpit` require `S_ADMI_FCD` authorization with value `DBA`.

SM_SMUA

One use case of `AMSC` is the possibility to upgrade an `ABAP` stack. In this situation, the system checks if the roles for the `RFC` users (such as `READ` user) need to be updated, too. The update of these users is restricted by authorization object `SM_SMUA`.

7.10.8 Technical User SM_TECH_ADM

The technical user is required to execute a set of activities for managed system setup. The activities run by this user have the specificity that they execute some SAP Solution Manager Java Web Services, that are – for legacy reasons – calling back the SAP Solution Manager `ABAP` stack. This call back requires a technical user with dedicated permissions. The activities depending on the existence of this user are:

- Create `WEBADMIN`
- `SSO` Setup
- Managed System Configuration
- Create Back `RFC`
- Activate `BW` source system once

i Note

For this activity the following authorization objects are requested by the system:

- `S_RFC` with `FUGR`: `RSAP_BW_CONNECT`
- `S_IDOCDEFT` for value `WE30` and `ACTVT` `01`, `02`, `03`

Assigned Single Roles

Single Role	Help Text
SAP_J2EE_ADMIN	AUTH_SAP_J2EE_ADMIN
SAP_SM_TECH_ADM	AUTH_SAP_SM_TECH_ADM
SAP_SM_USER_ADMIN	SAP_SM_USER_ADMIN

⚠ Caution

This role is required for creating the BACK RFC User. You can remove this role if you create the user either manually or via `SOLMAN_SETUP` with user `SOLMAN_ADMIN`.

Transport Authorization

Due to its security criticality, if you require transport authorization, you need to assign the according authorization objects `S_TRANSPRT` and `S_SYS_WBO` manually to your user.

7.10.9 Technical User for RFC - connection BACK <SMB_<SIDofManagedSystem>>[MANAGING.ABAP.RFC]

The technical user is used for the BACK – RFC connection from the managed system to the SAP Solution Manager system. It is created during managed system setup by user `SOLMAN_ADMIN`. The default name of this user is `SMB_<SIDofManagedSystem>`. The password can either be customer-specific or generated by the system.

The RFC is used to send `SDCCN` data or messages from a managed system to the SAP Solution Manager system, lock customizing objects against changes in Customizing Distribution, integrate Change Request Management into Incident Management, and so on.

i Note

If you change the password of this user in user management (transaction `SU01`), you need to change the password for this user in the RFC destination in the Solution Manager system as well.

The user is automatically assigned the generated role: `<namespace>SAP_SOLMAN_BACK`.

Authorization Objects

Authorization Object S_TABU_DIS and S_TABU_NAM

As of SP02, authorization object S_TABU_DIS is removed from the Read - user role. The list of tables is assigned to authorization object S_TABU_NAM in the READ destination and BACK destination. Therefore, the function module RFC_READ_TABLE is supported.

Note

See also SAP Note [2257213](#) .

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 SIG1 is required with the following values:

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

7.10.10 User Wily Guest

This application user [Guest](#) is a built-in user of the Introscope Enterprise Manager (EM). By default it is used to open the proprietary JDBC connection between SAP Solution Manager and the Introscope Enterprise Manager to extract the collected performance data. The user and password is maintained in two places:

- Within Root Cause Analysis
- Within Introscope Enterprise Manager user store (XML files: [users.xml](#), [domains.xml](#))

7.10.11 Technical User SEP_WEBSRV

The technical user `SEP_WEBSRV` is used for the BMC Appsign License Check Service in the Internet Communication Framework (ICF).

Role Assigned to User SEP_WEBSRV (Help Text ID: SEP_WEBSRV)

Assigned Role	Help Text-ID
SAP_APPSIGHT_INTERFACE	AUTH_SAP_APPSIGHT_INTERFACE

7.11 Technical Users for SLD and LMDB

7.11.1 Introduction

The Landscape Management Database (LMDB) serves as a central directory for system landscape data in SAP Solution Manager. It is used by Root Cause Analysis and in the Technical Monitoring work center scenarios. LMDB integrates with the System Landscape Directory (SLD) in productive or non - productive landscape to gather landscape data and provide it to client applications in the SAP Solution Manager. For more information on its configuration, see the [LMDB Setup Guide](#): <http://service.sap.com/instguides>  [SAP Components](#)  [SAP Solution Manager 7.2](#)  [Additional Guides](#) .

Technical System Landscape for SLD and LMDB

In SAP Solution Manager Release 7.2, the System Landscape Directory (SLD) is the primary data provider for LMDB. Technically, LMDB is the ABAP complement of SLD in Java. SLD and LMDB cooperate via a connection to synchronize contents, using the same principle as the synchronization between two SLD systems.

The managed systems send their system information directly via data suppliers to the SLD which is later synchronized with the LMDB. In LMDB, the systems are recognized as technical systems.

Diagnostics Agents are usually installed on each application and database server (of managed systems or SAP Solution Manager) in a system landscape and are additional data providers (of system information) for LMDB. The Diagnostics Agents are connected directly to SAP Solution Manager and constantly send technical system information to LMDB. This process is called *Outside Discovery* and can be configured using transaction SOLMAN_SETUP or the SAP Solution Manager Configuration work center.

7.11.2 Technical User LMDB_DS_XXX

The Data Supplier processing is also available in the LMDB and can optionally be used to take over this role from the SLD.

Data Flow

Technical systems and other relevant parts of the landscape send information about themselves via HTTP(S) in XML format to the SAP Solution Manager System. The information is stored in the LMDB and made available to various consuming applications via different specific APIs.

User LMDB_DS_<XXX>

This user is required for a number of different Data Suppliers to connect to the SAP Solution Manager. This user is only assigned role SAP_SM_LMDB_DATA_SUPPLIER which needs to be copied in the required name space. You need to create the user in SU01 and assign the role in transaction PFCG.

Authorization Object AI_LMDB_DS

The authorization object AI_LMDB_DS is required to allow the Data Supplier functionality, see also SAP Note [2183995](#).

⚠ Caution

The object is solely required for this purpose and should not be assigned to any other user or included in any other Solution Manager role.

7.11.3 Technical User SM_SLD_NOTIF

The Data Supplier processing is adapted in the LMDB for the purpose of an optional SLD usage.

Data Flow

In SAP Solution Manager, data from an SLD (System Landscape Directory) is synchronized to the LMDB (Landscape Management Database). Managed systems and other relevant parts of the landscape send information about themselves to the SLD. Typically, a periodic background job runs every 10 minutes in the SAP Solution Manager system to ensure that all changes in the SLD during the past time interval are synchronized to the LMDB. SLDs can send a notification to the LMDB when a change has occurred, and they can trigger an instant synchronization. The notification from the SLD to the LMDB is sent via HTTP(S) and proper authorization in the SAP Solution Manager system is required.

User SM_SLD_NOTIF

This user is required to connect the SLD to the SAP Solution Manager, send a change notification and trigger an instant synchronization. This user is only assigned role `SAP_SM_SLD_LMDB_NOTIFICATION` which needs to be copied in the required name space. You need to create the user in SU01 and assign the role in transaction PFCG.

7.11.4 Technical User SLD_CS_USER

For collecting system landscape information from the SLD, a user with read permission (for instance `SLD_CS_USER`) is required on the Java stack of the remote or local SLD. In case the SLD system is a dual stack system, it is defined as a system user in transaction SU01 of the ABAP stack.

When connecting the SLD to SAP Solution Manager the user credentials are required in transaction `SOLMAN_SETUP`.

User Creation

The user must exist on the SLD system.

In case of local SLD

If the local SLD on SAP Solution Manager is activated, the user is created automatically.

In case of remote SLD

If you connect a remote SLD (central or productive) to SAP Solution Manager, you need to create the user manually on the SLD system.

User Authorizations

The user requires the following authorizations:

- UME role: SAP_SLD_CONTENT_SYNC (SAP NetWeaver 7.1 or higher)
- UME role: SAP_SLD_GUEST (SAP NetWeaver 7.0, update the support package stack to at least SPS 12)

7.11.5 Technical User SLDAPIUSER

The SLDAPIUSER user is created during installation of the Solution Manager system. In case a central SLD exists in the central SLD. The credentials of the user are needed by the system to configure the SLD Data Supplier and CIM Client.

When connecting the SLD to SAP Solution Manager the user credentials are required in transaction SOLMAN_SETUP.

User Creation

The user must exist on the SLD system.

In case of local SLD

If the local SLD on SAP Solution Manager is activated, the user is created automatically.

In case of remote SLD

If you connect a remote SLD (central or productive) to SAP Solution Manager the user, you need to create the user manually on the SLD system.

User Authorizations

The user requires following authorizations:

- UME role: SAP_SLD_CONTENT_SYNC (SAP NetWeaver 7.1 or higher)
- UME role: SAP_SLD_GUEST (SAP NetWeaver 7.0, update the support package stack to at least SPS 12)

7.11.6 Technical User SLD_DS_<SID>

The user SLD_DS_<SID> in the SAP Solution Manager is required by the SLD data suppliers to write technical system information into SLD. The user exists in the Java stack of the SLD system and is automatically created during the SLD activation. In case the SLD system is a dual stack system it is defined as a system user in transaction SU01.

→ Recommendation

If your managed systems do not authenticate at [SLD](#) via Gateway (User and Password), we recommend to create one specific `SLD_DS_<SID>` user per managed system.

User Authorizations

The user requires UME role: `SAP_SLD_DATA_SUPPLIER` to create, modify, and delete CIM instances of the landscape description subset as a data supplier without access to the SLD User Interface.

i Note

You need to create the role `SAP_SLD_DATA_SUPPLIER` manually before you can assign it to the user. For more information, see the [SLD Configuration Guide](#).

7.12 Users and Authorizations for BW Configuration

7.12.1 Introduction

The following section gives you an overview of all users and authorizations for BW based on the configuration of the scenario, standard or remote.

For information about the **BW / Extractor Framework - concept**, see in the *Authorization Concept Guide* section on [BW - Integration](#).

7.12.2 BW Administrator User SM_BW_ADMIN

You create a BW - administration user when you use a remote BW system/client during Infrastructure Preparation. The default name for this user is `SM_BW_ADMIN`.

i Note

If the BW runs in the standard scenario, these roles are assigned to user `SOLMAN_ADMIN`.

Roles Assigned to User SM_BW_ADMIN

Assigned Roles	Help Text — ID
<code>SAP_SM_BI_ADMIN</code>	<code>AUTH_SAP_SM_BI_ADMIN</code>

Assigned Roles	Help Text — ID
SAP_PI_CCMS_SETUP	AUTH_SAP_PI_CCMS_SETUP
SAP_SM_BI_EXTRACTOR	AUTH_SAP_SM_BI_EXTRACTOR
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN

7.12.3 Technical User SM_BW_ACT

Due to the „divided“ activation of BW content (job CCMS_BI_SETUP) in Infrastructure Preparation and in various scenario-related configurations, it becomes necessary to introduce another new user: SM_BW_ACT (type: system user). The user is assigned single role SAP_BI_E2E.

Role	Help TXT ID
SAP_BI_E2E	AUTH_SAP_BI_E2E

7.12.4 Technical User SMD_BI_RFC

The SMD_BI_RFC user is only created by user SM_BW_ADMIN if you use a remote BW system/client.

Role Assignment to User SMD_BI_RFC

Assigned Role	Help Text ID
SAP_BI_E2E	AUTH_SAP_BI_E2E

7.12.5 Technical User SM_BW_<SID>

The SM_BW_<SID> user is created by user SM_BW_ADMIN if you use a remote BW system/client. The user is assigned to RFC-destination: SM_BW_<SID>CLNT<Client>_READ.

Role Assignment to User SM_BW_<SID>

Assigned Role	Help Text ID
SAP_SM_BI_ESR_EXTR ACTOR	AUTH_SAP_SM_BI_ESR_EXTRACTOR

Assigned Role	Help Text ID
SAP_SM_BI_MAI_EXTR ACTOR	AUTH_SAP_SM_BI_MAI_EXTRACTOR
SAP_SM_BI_DVM_READ	AUTH_SAP_SM_BI_DVM_READ

Usage

Allow Extractor Data to be Read

The user authorization contains extractor authorization for scenarios [Value Realization](#) and [Application Monitoring](#) (MAI). For more information, see scenario-specific guides for ESR and Technical Monitoring.

Check User Status in BW - System

The user authorization allows to check the status for all users created in the BW-system by transaction SOLMAN_SETUP. If this authorization is not given, the system is not able to display the status of BW-users in transaction SOLMAN_SETUP. Status check is triggered by using the [Refresh](#) link.

Note

For first installation and configuration of SAP Solution Manager, the user status check can only be displayed by the system when the complete configuration is finished. This is due to the creation of users before creation of RFC-destinations. As soon as you have created the RFC-destination and the users, the system can check the user status automatically.

7.12.6 Technical User BI_CALLBACK

The BI_CALLBACK user is created as a technical user in transaction SOLMAN_SETUP. This user is relevant for reorganization of BW - data in the SAP Solution Manager and configuration validation.

Role Assignment to User BI_CALLBACK

Assigned Role	Help Text ID	Remarks
SAP_BI_CALLBACK	AUTH_SAP_BI_CALLBACK	ABAP authorization role

7.12.7 Diagnostics Center

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

1. A dialog user starts the diagnostic center from the Solution Manager Administration work center


2. The checks in the managed system are running with system user `SM_<Client>_READ`.
3. The checks in the Solution Manager system are running via the logged on dialog user.
4. The checks for the BI are running via RFC destination `NONE` (dialog user). In the case of a remote scenario, RFC destination `BI_CLNT<client>` (user `SMD_BI_RFC`).

7.12.8 Technical User SM_BOC

The user `SM_BOC` (Help Text ID: `TP_SM_BOC`) is relevant for ITSM Analytics. The user acquires data from BW Queries for Incident Analysis, for the end-user later to view related stories in the Business Object Cloud (BOC).

Role Assignment to User `SM_BOC`

Assigned Role	Help Text ID	Remarks
<code>SAP_SM_BI_BOC</code>	<code>AUTH_SAP_SM_BI_BOC</code>	ABAP authorization role

7.13 Users and Authorizations for Managed Systems

7.13.1 Introduction

You need to create users during the configuration of the managed systems.

Described Users

All users created in the managed system are described.

In addition, the system creates users in the `UME` of a managed system if this system is a Java system or a double stack. Also, `CTC` runtime users are automatically created. These users are mentioned in the protocol of the configuration setup, but not explicitly on the `UI`.

7.13.2 Administrator User in ABAP: SM_ADMIN

When you set up the managed systems with SAP Solution Manager, the system creates a configuration user `SM_ADMIN_<Solution Manager SID>` of type **System User** with specific authorizations in the managed system. This user is allowed to create other users in the managed system, assign roles, and run some Diagnostics self - check activities.

This user creates the following users in the managed systems with type *Double Stack*:

- SAPSUPPORT (dialog user in ABAP)
- SM_COLL_<SolManID> (technical user - relevant for Diagnostics Agent in Java)
- SMDAGENT<SolManID> (technical user for JCo/RFC - relevant for Diagnostics Agent in ABAP)
- Read - User (technical user relevant for READ Connection)
- TMW- User (technical user relevant for TMW Connection)

This user creates the following users in an ABAP Single Stack of the managed systems:

- SAPSUPPORT (dialog user in ABAP)
- SMDAGENT<SolManID> (technical user for JCo/RFC - relevant for Diagnostics Agent in ABAP)
- Read - User (technical user relevant for READ Connection)
- TMW- User (technical user relevant for TMW Connection)

Roles Assigned to Configuration User SM_ADMIN_<SolutionManager SID>

Assigned Roles	Help Text — ID	Additional Remarks
SAP_RCA_CONF_ADMIN	AUTH_SAP_RCA_CONF_ADMIN	Main configuration authorization for managed system, including SDCCN
SAP_SM_USER_ADMIN	AUTH_SAP_SM_USER_ADMIN	ABAP authorization role, authorizations for transaction SU01 and PFCG to allow the creation of, change, and deletion of users and roles. If your security policy does not allow this, you need to create all users manually.
SAP_J2EE_ADMIN	AUTH_SAP_J2EE_ADMIN	in case of double stack or single Java, must be manually added
<i>Optional: SDCCN Administration</i>		

Assigned Roles	Help Text — ID	Additional Remarks
SAP_SDCCN_ALL	AUTH_SAP_SDCCN_ALL	In case you have used user SM_ADMIN_XXX to activate transaction SDCCN and consequently run all required background jobs for SDCCN (/BDL/*) with his user, you need to have role SAP_SDCCN_ALL assigned. This role contains authorization for authorization object S_DEVELOP. → Recommendation Activate SDCCN with a separate technical user for background jobs. This allows you to lock the configuration user SM_ADMIN_<SolutionManagerSID> after configuration.

Transport Connection

For documentation purposes it is possible to activate automatic transport request. In order to activate this function, you need to maintain table PRGN_CUST adding value CLIENT_SET_FOR_ROLES.

Required Transport Authorizations

- S_SYS_RWBO with ACTVT 01, 02, 03 and Request Types CUST, TASK
- S_TRANSPRT with ACTVT 01, 02, 03 and Request Types CUST, TASK

Operations/Upgrade Mode

→ Recommendation

The user should be locked after finished configuration tasks. In case of upgrade configuration, you need to unlock it again.

7.13.3 Administrator User in Java: SM_ADMIN_<SolManSID>

When you set up the managed systems with SAP Solution Manager, you need to create an administration user for Java manually. This user must be allowed to create other users in the managed system, assign roles, and run some Diagnostics self - check activities.

This user creates the following users in the managed systems with type *Double Stack*:

- SAPSUPPORT
- SM_COLL_<SolManID> (technical user - relevant for Diagnostics Agent in Java)

This user creates the following users in a Java Single Stack of the managed systems:

- SAPSUPPORT
- SM_COLL_<SolManID> (technical user - relevant for Diagnostics Agent)

7.13.4 Technical User SMDAGENT_<SolManID> for Wily Host Agent

Use

The user SMDAGENT_<SolutionManagerSID> connects Wily Host agent to the managed system. This is an ABAP user that is used by the Wily Host agent. It is automatically created during runtime during the managed system setup.

The user is used to run dedicated extractors on the managed systems, which are delivered with the ABAP Add-On ST/A-PI. The Wily Host Applications running within the Diagnostics Agent use this user for managed ABAP systems to open a JCo connection, and collect application - specific performance data.

For self monitoring purposes, this user should also exist on the SAP Solution Manager, and the actual ST/A-PI should be installed there as well. The name of the user SMDAGENT_<SolutionManagerSID> is fixed and must not be changed.

Role Assigned to User SMDAGENT_<SolManID>

Role	Text ID	Remarks
SAP_IS_MONITOR	AUTH_SAP_IS_MONITOR	ABAP

More Information

For further details regarding Wily Introscope user administration, read the *Introscope Installation for SAP Introscope Version 8.0 Installation Guide for SAP*.

7.13.5 Technical Users for RFC - Connections READ and TMW

In the managed system, you create two technical users (user type: system user) for RFC - connections, the READ user, or the TMW user.

User Naming Conventions

Per default, the system suggests a name for all technical users required. For Read user, TMW user, and Back user, you can adapt user names as required by your company and for the purpose of uniqueness. For instance, you can add system ID and client of the target system in question to your users, such as `SM<SourceSystemID><TargetSystemID><Client>`. In case of any password changes or locks on your users, this can help to identify the root cause.

Role Upload from SAP Solution Manager to the Managed System

⚠ Caution

We recommend *not to upload roles to a productive system, but instead use the upload to a development system*, and then use the transport mechanism to upload the roles into your productive client. For more information see: on the Service Marketplace: <http://scn.sap.com/docs/DOC-17149>.

You can upload the roles for the `READ` user and `TMW` user using the function *Upload* in step *Maintain RFCs*.

i Note

Even if you decide to not upload the SAP role from the SAP Solution Manager System, the system copies the SAP role that is already present on the managed system. This behavior is triggered every time you use the upload button itself. Background: here is currently no way for the system to distinguish between SAP role upload to the managed system using the *Upload* function or a transport.

This function allows you to upload the roles for the individual users from SAP Solution Manager into your respective client of the managed system. To be able to upload the roles, the system requires you to enter an administration user of your managed system into a pop-up beforehand, which has the authorizations to upload roles in your managed system. The system opens a temporary trusted `RFC` connection in order to be able to upload the role.

i Note

The function can only be used if:

- the client in the managed system is not a productive client. We recommend to upload the role into your development client and transport it into your productive client.
- your user in the SAP Solution Manager system has authorization object `SM_SMUA` assigned. This authorization object is included in role `SAP_SM_SMUA*` for user `SOLMAN_ADMIN`.

Read RFC - Connection (technical name: `SM_<SIDofSolManSystem>CLNT<Clientof SolManSystem>_READ`)

The `READ` – `RFC` connection is used to read data from the managed system, to run a set of extractors and enable the `E2E` tracing in the managed systems (for instance initial `E2E` checks on the managed systems run

E2E extractors). It is mandatory for each managed system, as it enables basic SAP Solution Manager functions.

i Note

If the SAP Solution Manager system is set up as a managed system, the default RFC destination is `NONE`. You have to replace the RFC destination `NONE` and create a standard RFC `READ` destination.

User and Password

The default name of the user is `SM_<SIDofSolutionManagerSystem>`.

The password for this user can either be customer-specific or generated by the system. If you change the password of this user in user management (transaction `SU01`), you need to change the password for this user in the RFC destination in the Solution Manager system as well.

→ Recommendation

When the user password is locked, we recommend the following procedure to be able to determine the root cause for it:

1. Activate the Audit Trace in transaction `SM19` in the managed system (see also SAP Note [495911](#)).
2. Activate the Security Trace in transaction `SM50` (`SM66`).
3. Check for error log entries in transactions `SM20*` (`SM20`, `SM20N`, `SM20_OLD`).

Authorization Roles

i Note

We recommend to check SAP Note [1830640](#).

For these RFC users, the system assigns authorization roles. Which roles are assigned to the individual user is determined by the `SAP_BASIS` level of the managed systems required. The technical role names are visible in the configuration screen of the system.

The system assigns the following roles to the RFC user:

- role `<namespace>SAP_SOLMAN_READ` for all authorizations as of `SAP_BASIS < 7.01`

⚠ Caution

We strongly recommend to have the latest `ST-PI` Support Package applied to SAP Solution Manager and managed systems. To be able to generate this RFC connection during automatic configuration, you need to have at least `ST-PI 2008_1_700 SP08`. If you have not this specified `ST-PI` applied, please see the same section in security guide for `SP08`.

- role `<namespace>SAP_SOLMAN_READ_702` for all authorizations as of `SAP_BASIS => 7.02`

i Note

As per SAP Note [1830640](#) an additional role `Z_SOLMAN_READ_702_ADD` for complementary authorization objects in `SAP_BASIS` release 7.31 is relevant. This role is only available as per this SAP Note.

- role `<namespace>SAP_SOLMAN_BI_READ`; PFCG template: `SAP_SOLMAN_BI_READ` (template for BW - authorizations, only available, if the managed system contain software component `BI_CONT` as of `SP04`)

i Note

If you configure your managed system in transaction `SOLMAN_SETUP` for Service Delivery Enablement, a `READ RFC` - connection to the 000 client of your managed system is required. In addition, role `SAP_SM_BATCH_SD` is assigned to the `READ` user to schedule the collection job: `SAP_COLLECTOR_FOR_PERFMONITOR`. As this job is a collective job, authorizations are not definitely determined. Therefore, the job is run by user `DDIC` in the managed system client 000. This user has full SAP system permission with profiles `SAP_ALL` and `SAP_NEW`.

Authorization Object S_RFC

The authorization object `S_RFC` restricts which function groups or function modules can be accessed. As of `SAP_BASIS 7.02` and higher the object is delivered with all relevant function modules in place. For lower releases, only function groups can be assigned to the object.

i Note

Function Module `RFC_READ_TABLE` is not assigned to any of the assigned roles, as it would allow the user to read almost all tables.

Authorization Object S_TABU_DIS and S_TABU_NAM

As of `SP02`, authorization object `S_TABU_DIS` is removed from the Read - user role. The list of tables is assigned to authorization object `S_TABU_NAM` in the `READ` destination and `BACK` destination. Therefore, the function module `RFC_READ_TABLE` is supported.

i Note

See also SAP Note [2257213](#) .

TMW RFC - Connection (technical name: SM_<SID>CLNT<Client>_TMW)

The `TMW RFC` - connection consists of all authorizations of `READ RFC` - connection and additional authorizations for Change Request Management (remote creation of transport requests with tasks for designed developers in the development systems), and batch job authorizations. The default name for this user is `SMTM_<SID>ofSolution Manager`, The password can either be customer-specific or generated by the system.

For this `RFC`, the system uses all three roles for the `READ RFC` - connection, and an additional role for `TMW RFC` - connection. The roles are then assigned to the `RFC` user. The additional role:

- role `<namespace>SAP_SOLMAN_TMW` for all authorizations as of `SAP_BASIS < 7.01`
- role `<namespace>SAP_SOLMAN_TMW` for all authorizations as of `SAP_BASIS => 7.02`

7.13.6 Technical User SM_COLL_<SID>ofSolMan>

This user is created for data collection in the managed system.

Role	Role Type	Double Stack	Single Java Stack	Mandatory
Administrator	UME	X	X	X
SAP_J2EE_ADMIN	ABAP	X		X

Note

Administration privileges are only required for the initial set-up of the Introscope BCI Adapter. If you are solely interested in Introscope Metrics, you can remove the Java administration privileges. Be aware that some extractors, especially those which are relevant in the context of RCA, may fail. As a consequence the Configuration Validation functions may not work properly. Additionally, the trace enabling of E2E is not possible.

Caution

The CCDB CTC Extractor and CCDB DB Extractor need SAP_J2EE_ADMIN rights to run. The role SAP_J2EE_ADMIN allows administration rights for the complete Java Stack, including UME (user administration).

SAP_REMOTE_USER_ADMIN_READONLY	UME	X	X	
SAP_SLD_CONFIGURATOR	ABAP	X		
SAP_XI_RWB_SERV_USER	ABAP	X		
administrators	Java	X		
NWA_SUPERADMIN	UME		X	
SAP_JAVA_NWADMIN_CENTRAL	UME		X	
SAP_JAJA_NWADMIN_LOCAL	UME		X	
SAP_JAVA_WSNAVIGATOR	UME		X	
SAP_XI_ALERTCONFIGURATOR_J2EE	UME	X		only as of SAP_BASIS 7.30 and higher

Role	Role Type	Double Stack	Single Java Stack	Mandatory
SAP_XI_ALERTCONF_DISPLAY_J2EE	UME	X		only as of SAP_BASIS 7.30 and higher

7.13.7 J2EE Administrator J2EE_ADMIN

This user exists on any SAP dual stack systems. However, SAP recommends to provide the SMD_AGT_ADM user credential during RCA setup. This user account can be useful for administration like manual user creation or UME role / J2EE security role assignment. It could be also used for SLD configuration and validation procedures. The role assigned is SAP_J2EE_ADMIN.

7.13.8 Administrator OS User

The user is an OS user with administrator permissions. It is mandatory to perform the Root Cause Analysis Agent installation. This administrator user is mandatory to perform some tasks like:

- Creating OS user dedicated to the Diagnostics
- Restarting Java processes

On UNIX the user belongs to group [root](#), and on Windows the user belongs to group [administrator](#).

7.14 Basic Configuration Dialog Users

7.14.1 Dialog User SAPSUPPORT

The SAPSUPPORT user is a **Read User for Root Cause Analysis** of type [Dialog](#). The user SOLMAN_ADMIN automatically creates this user in the SAP Solution Manager system, the managed systems, and as well the BW - client/system. This user is the main user to log on to Diagnostics.

In the SAP Solution Manager System: Standard BW Scenario (Help Text ID: USER_SAPSUPPORT)

Assigned Roles	Help Text-ID
SAP_BI_E2E	AUTH_SAP_BI_E2E
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
i Note This role allows only for read access to all tools. If you want to allow your SAPSUPPORT user to be able to change settings, you need to adapt the role. How to adapt the role, see <i>How-to Section</i> .	
SAP_DBA_DISP	AUTH_SAP_DBA_DISP
SAP_CV_DISP	AUTH_SAP_CV_DISP
SAP_EM_DISPLAY	AUTH_SAP_EM_DISPLAY
SAP_SMWORK_BASIC	AUTH_SAP_SMWORK_BASIC
SAP_SMWORK_CONFIG	AUTH_SAP_SMWORK_CONFIG
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_DIAG
SAP_SMWORK_SM_ADMIN	AUTH_SAP_SMWORK_ADMIN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
i Note In the display role for RCA, the authorization object D_SM_S_DIA is delivered with activities 02 (change) and 03 (display). This is due to the nature of the function of self diagnosis and its configuration possibilities. It has no impact on data changes, but on data display.	

In the BW Client / System: Remote Scenario (Help Text ID: USER_SAPSUPPORT_MS)

Assigned Roles	Help Text-ID
SAP_BI_E2E	AUTH_SAP_BI_E2E

7.14.2 Dialog User SAPSERVICE

The 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 the SAP Solution Manager. The according role in Solution Manager and managed systems would be `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 as being a set user which should not be changed in its authorizations, all roles in the SAP Solution Manager system and BW system (in case it is remote), are copied automatically into their own namespace `ZSD*`.

In the SAP Solution Manager

For all roles assigned to the `SAPSERVICE` user in the SAP Solution Manager system, check the according entry in step [2.4 Create Users](#) in the view Basic Settings. If you are not sure about the roles assigned by the system, check out the documentation link behind the according role. The single roles are also shipped with composite role `SAP_SERVICE_EXE_ALL_COMP`.

In the Solution Manager system

Single Role	Help Text ID
<code>SAP_BPR_PPM</code>	<code>AUTH_SAP_BPR_PPM</code>
<code>SAP_CPR_PROJECT_ADMINISTRATOR</code>	<code>AUTH_SAP_CPR_PROJECT_ADMINISTRATOR</code>
<code>SAP_CPR_USER</code>	<code>AUTH_SAP_CPR_USER</code>
<code>SAP_XRPM_ADMINISTRATOR</code>	<code>AUTH_SAP_XRPM_ADMINISTRATOR</code>

Single Role	Help Text ID
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
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_ITPPM_ALL	AUTH_SAP_SM_ITPPM_ALL

Single Role	Help Text ID
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_DIS	AUTH_SAP_SM_ESH_DIS

In the Managed System

In the managed systems the user is not created automatically due to required authorizations which depend on the business contexts. Check SAP Note [1405975](#)  for appropriate roles.

In the 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_SM_DASHBOARDS_DISP_VBD
- SAP_BPR_PPM
- SAP_CPR_PROJECT_ADMINISTRATOR
- SAP_CPR_USER
- SAP_XRPM_ADMINISTRATOR
- SAP_SM_ITPPM_ALL

7.14.3 Solution Manager Administration User

→ Recommendation

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

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

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

Work Center

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

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

i Note

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

Administrator User `SA_ADM_***` (Help Text: `TP_SA_ADM`)

According composite role `SAP_SOLMAN_ADMIN_COMP`

Single role	Help Text
<code>SAP_SM_SL_ADMIN</code>	<code>AUTH_SAP_SM_SL_ADMIN</code>
<code>SAP_RCA_AGT</code>	<code>AUTH_SAP_RCA_AGT</code>
<code>SAP_RCA_DISP</code>	<code>AUTH_SAP_RCA_DISP</code>
<code>SAP_SERVICE_CONNECT</code>	<code>AUTH_SAP_SERVICE_CONNECT</code>
<code>SAP_SMWORK_SM_ADMIN</code>	<code>AUTH_SAP_SMWORK_SM_ADMIN</code>
<code>SAP_SM_SYM_CONF</code>	<code>AUTH_SAP_SM_SYM_CONF</code>

Single role	Help Text
SAP_SYSTEM_REPOSITORY_ALL	AUTH_SAP_SYSTEM_REP_ALL
SAP_SM_CMDB_EXE	AUTH_SAP_SM_CMDB_EXE
SAP_SM_SMUA_ALL	AUTH_SAP_SM_SMUA_ALL
SAP_SM_DASHBOARDS_DISP_LMDB	AUTH_SAP_SM_DASHBOARDS_DISP_LMDB
SAP_SM_BP_ADMIN	AUTH_SAP_SM_BP_ADMIN
SAP_SM_ROLECMP_ALL	AUTH_SAP_SM_ROLECMP_ALL
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

Display User SA_DIS_*** (Help Text ID: SAP_SOLMAN_ADMIN_DISP_COMP)

According composite role SAP_SOLMAN_ADMIN_DISP_COMP

Single role	Help Text ID
SAP_SM_SL_DISPLAY	AUTH_SAP_SM_SL_DISPLAY
SAP_RCA_DISP	AUTH_SAP_RCA_DISP
SAP_SERVICE_CONNECT	AUTH_SAP_SERVICE_CONNECT
SAP_SMWORK_SM_ADMIN	AUTH_SAP_SMWORK_SM_ADMIN
SAP_SM_SYM_LEVEL01	AUTH_SAP_SM_SYM_LEVEL01
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SM_DASHBOARDS_DISP_LMDB	AUTH_SAP_SM_DASHBOARDS_DISP_LMDB
SAP_SM_ROLECMP_DISPLAY	AUTH_SAP_SM_ROLECMP_DISPLAY
SAP_SM_SMUA_DIS	AUTH_SAP_SM_SMUA_DIS
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_SM_BP_DISPLAY	AUTH_SAP_SM_BP_DISPLAY
SAP_SM_RFC_DISP	AUTH_SAP_SM_RFC_DISP

Authorizations for Specific Tools

Solution Manager User Administration (SMUA)

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

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

i Note

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

Segregation of Duty

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

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

Archive Log

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

→ Recommendation

We recommend to limit scenario visibility for which the [Archive Log](#) should be accessible in authorization object `SM_SETUP`.

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

- `SAP_SMWORK_SM_ADMIN`
- `SAP_SYSTEM_REPOSITORY_ALL`
- `SAP_SM_SMUA_DIS`

Role Comparison Tool: Role Adjust

The role `SAP_SM_ROLECMP_*` allows the user to adjust already customized roles with newly shipped values, or value changes, from SAP Standard roles. Access to the application is restricted by authorization object `SM_ROLECMP`.

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

- `SAP_SMWORK_SM_ADMIN`
- `SAP_SM_USER_ADMIN`
- `SAP_SM_SMUA_DIS`

- Authorization object SM_SETUP with ACTVT 02 (Change) for [User Creation](#) steps.

i Note

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

7.15 Standard/Template Users

Standard/template users are templates of users with a set of specified roles. They represent end-users for the specific scenario. For each procedure within transaction SOLMAN_SETUP, template users for end-users are defined.

User Authorizations

The authorizations for these specified users are defined according to a specified use case for the according scenario as described in the *Online Documentation* for the scenario. In the [User Documentation](#), you can find a description of the individual user. In the [Role Documentation](#), you can find a description of the role.

Optional Activities and Status Level

Steps for creating template/standard users are optional

The optional flag works at activity level. An optional activity is an activity for which the end-users are not forced to execute the corresponding configuration. The status of this activity is not taken into account in the status consolidation at step level. If a step contains only optional activities, the step itself is considered as optional. The step is then grayed out.

7.16 S-Users

7.16.1 Introduction

The S-user is a customer user stored within SAP office. It is used by the SAP customer in the following scenarios:

- Exchange problem messages with SAP
- Synchronize system data with Support Portal and send data about satellite systems
- Service connection

- Retrieve information about which messages have been changed at SAP
- To send an up-to-date version of the component `ST-SER` for delivery of services by SAP Active Global Support
- Get some user documentation from SAP Market Place used by the Help Center within Diagnostics

7.16.2 Technical Communication User for SAP Backend

The Technical Communication User is needed to access SAP-internal systems via RFC destinations. You need to provide the user for RFC usage in transaction `STC01`. To learn more about the Technical Communication User, see SAP Note [2174416](#).

⚠ Caution

Only your Super Administrator is allowed to create and activate *Technical Communication Users*. You can have a number of these users according to the number of RFCs you are using. The user is created with a basic authentication password, and is available within 4 hours of request.

The Technical Communication User is required for communication in various scenarios, see section *Communication Channels and Destinations* in this guide.

Relevant KBAs:

- [2668288](#) - Differences between personalized S-user and technical user
- [2435166](#) - S-User used by SAP Solution Manager RFCs keep getting locked

7.16.3 S-User for Communication

! Restriction

This guide does not contain additional information on relevant S-user configurations.

i Note

If a user has sufficient authorization and is assigned correctly to the appropriate S-user in transaction `AIUSER`, this user can display the same personal contact data (name, phone number) for a system as in SAP Support Portal, as this data is replicated from there to the Solution Manager system. For more information on protective measures for personal data, see the *Security Optimization Guide*.

Authorizations

Service Connection

You require the following authorizations for this user:

- Maintain System Data
- Open Service Connection

Incident Management and Expert on Demand

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

Data Download

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

Troubleshooting

Note

For creation and activation issue of users for the SAP's support backbone communication, use application component XX-SER-SAPSMP-USR.

7.17 User Role for TREX Administration

TREX can be administered using the TREX Admin Tool.

TREX

Name	Type	Remarks
SAP_BC_TREX_ADMIN	ABAP	For TREX configuration using the TREX Admin tool

Important Disclaimers and Legal Information

Hyperlinks

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

About the icons:

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

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

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

Gender-Related Language

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

© 2019 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.