

Security Guide | PUBLIC
Document Version: 7.2 SPS 18 – 2023-12-18

Security Optimization Guide

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Document History. 5

2 List of Roles Updated per SP. 9

3 Introduction 13

4 Managing Authentication. 15

4.1 Vulnerability 15

4.2 Overview: All Standard Users Created in Basic Configuration in SAP Solution Manager Configuration. 15

4.3 Overview: All End-Users and Business Partners per Configuration Scenario. 18

4.4 Using Solution Manager User Administration. 19

4.5 How to Handle Default Standard Users - SOLMAN_ADMIN, SMC* Users, and Template Use Case IDs. 21

4.6 How to Handle Technical Users. 26

4.7 Removing Obsolete Users. 28

4.8 Check and Secure Dialog Users 28

4.9 Using Secure Policy for Passwords and Login. 29

5 Managing Authorizations. 32

5.1 Vulnerabilities. 32

5.2 Configuration Transaction SOLMAN_SETUP - Segregation of Duties. 32

5.3 Roles and Authorization Management. 34

5.4 Restricting Roles to Allow Minimal Authorization. 36

5.5 Transporting Roles from Development to Production. 37

5.6 Function Calls. 38

5.7 Start Authorizations. 39

5.8 User Security. 40

5.9 SAP Basis Critical Authorizations and Combinations. 42

5.10 Configuration Authorization. 46

5.11 Updating Authorizations and Roles. 46

5.12 Modifying Values in Authorizations (CRM). 47

6 Securing Your Systems. 48

6.1 Vulnerability. 48

6.2 Checking SAP Basis Infrastructure Security - Settings. 49

6.3 Security Checks of SOLMAN_SETUP. 50

6.4 Using Authorizations to Restrict System (LMDB) Data 50

6.5 Updating Managed Systems in SOLMAN_SETUP. 53

6.6 Checking Security Flags for Relevant Activities in SOLMAN_SETUP. 53
6.7 Using System Recommendations Application. 53

7 Securing Channels and Destinations. 56
7.1 Vulnerability. 56
7.2 Overview: Where Used - Solution Manager Technical RFC - Users per Scenario (READ, TMW, TRUSTED). 56
7.3 Secure RFCs with Authorizations. 56
7.4 SAP's Support Backbone Destinations. 61
7.5 SNC Check. 62

8 Securing Access to Applications. 64
8.1 Vulnerability. 64
8.2 Restrict Access to Transaction SOLMAN_SETUP. 64
8.3 Secure Single Applications in Intranet/Internet. 67
8.4 Guided Procedure Framework. 70
8.5 Protecting ABAP Development Environment. 71
8.6 Protecting Functions and Tables. 72

9 Securing Data, Data Flow, and Processes. 73
9.1 Vulnerability. 73
9.2 Background Jobs. 73
9.3 Securing Attachments, Uploads, and Download. 75
9.4 Processes and Document Management. 77
9.5 Change Control Related Issues 79
9.6 Manage Import Authorization in Change Request Management. 82
9.7 SAP EarlyWatch Alert Data. 84
9.8 Restricting BI Master Role SAP_BI_E2E. 84
Business Partner Data. 84

10 Data Protection and Privacy Measures. 86
10.1 Vulnerabilities. 86
10.2 Glossary. 86
10.3 Overview of Relevant Applications in SAP Solution Manager. 88
10.4 Reporting on Existing Data to Identified Data Subject. 105
10.5 Simplifying Deletion of Personal Data. 114
10.6 Tighten Table Read and Write Access/Table Protection. 151
10.7 Change Log Information per Function. 155
10.8 Archiving of Objects. 167
10.9 SAP ILM Tool Support. 171

11 Useful Tools to Help Your Running Operation Stay Secure. 173
11.1 Run a Security Optimization Service. 173

11.2 SAP EarlyWatch Alert Management. 173
11.3 Using Configuration Validation for Regular Checks of Compliance. 174
Introduction. 174
Prerequisites. 175
Users and Roles in the SAP Solution Manager. 176
Defining Configuration Stores. 177
STANDARD_USERS: Which Standard Users Retain Their Default Password?. 179
AUTH_PROFILE_USER: Which Users Have Profile SAP_ALL / SAP_NEW Assigned?. 179
AUTH_ROLE_USER: Which User Is Assigned Critical Roles. 180
AUTH_PATTERN_ROLE: Which Roles Exist for a Specific Pattern in the Role Name?. 180
AUTH_DISPLAY_ROLE: Which Display Roles Have Change/Edit Authorizations?. 181
AUTH_COMB_CHECK_ROLE: Which Roles Have Specific Authorizations or Authorization Combinations?. 182
AUTH_COMB_CHECK_USER: Which Users Have Specific Authorizations or Combinations Assigned?. 184
AUTH_TRANSACTION_USER: Which Users Are Allowed to Run Critical Transactions?. 185
AUTH_USER_TYPES: Are There Any Users in the System with Wrong User Type?. 185

1 Document History

> ⚠ Caution
>
> Before you start using this guide, make sure you have the latest version of this document. You can find the latest version at https://help.sap.com/viewer/p/SAP_Solution_Manager. *Select your version* > *Implement* > *Security*.

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

Support Package Stacks (Version)	Date	Description
SP13	2021-08-02	**Data Protection and Privacy Measures** In section *Simplification of Deletion*, added information on authorization protection mechanism for application *ASU Toolbox*. **SAP Notes** • 2250709 Solution Manager 7.2: End-User Roles and Authorizations Corrections as of SP01 and higher • 2257213 Berechtigungen für RFC-Benutzer für SAP Solution Manager 7.2 SP02 und höher • 3058852 User Management Recommendation SAP Solution Manager 7.2: SMD_AGT In section *Simplification of Deletion*, added information for *UX Monitoring* on how to delete any personal data within a recorded script before uploading it. In all sections, added information for *SUT Management* application.

Support Package Stacks (Version)	Date	Description
SP12	2021-02-01	**S-User Expiration Date** Updated section on the deletion of personal data within chapter *Data Protection and Privacy Measures*. SAP's backbone is the leading system in regards to S-user assignments and usage. S-users, which are created, edited, and deleted or expired in the backbone are replicated into the SAP Solution Manager system accordingly. → Remember Update your S-User regularly in the SAP backbone system. **Data Protection and Privacy Measures** • added new ILM archiving object for Test Management `SM_TPLN` **New Sections** • Protecting Functions and Tables **Managing Authentication** Added information on removal of obsolete technical users such as `SMD_AGT`, due to security criticality.
SP11	2020-05-11	**Securing Data, Data Flow, and Processes** Updated section *Securing Attachments, Uploads, and Download* with paragraph on parameter setting for size limitations when uploading files. **Updated sections** • Updating Authorizations and Roles • Using Authorizations to Restrict System (LDMB) Data • How to Handle Default Standard Users **New section Modifying Values in Authorizations**
SP09	2019-06-17	**Data Protection and Privacy Measures** • new section on *Interface Documentation* • additional information for *GSS* in section *Simplification of Deletion of Personal Data* • new section on *SAP's Support Backbone Channels*, see in chapter *Securing Channels and Destinations* • additional information on upload functionalities, see section *Securing Attachments, Uploads, and Downloads*
SP08	2019-03-11	Minor changes

Support Package Stacks (Version)	Date	Description
SP08	2018-12-03	**Data Protection and Privacy Measures** Added new information to all sections: • Reporting: Improvement of report options • Deletion: Added deletion relevant authorization objects to specific administration roles • Table Access: Added new authorization groups to administration roles • Change Log: Added change log information to relevant administration roles
SP07	2018-05-25	**New section on Data Protection and Privacy Measures** New chapter on specifics for personal data protection measures. Check the **main collective SAP Note** 2610137 **Personal Data related information within SAP Solution Manager**. **i Note** In the majority of cases, compliance with data privacy laws is not a product feature. SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data. SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source. **Composite Roles** As of SP07, composite roles in SAP Solution Manager are no longer supported. All business user definitions with accordingly assigned roles are available with their documentation in application Solution Manager User Administration (SMUA) and in transaction `SOLMAN_SETUP`. For more information on business users (Use Case IDs), see the according section in the *Authorization Concept Guide*. For more information on the application SMUA, see the *Secure Configuration Guide*. **New section on Managing Authorizations** New section on critical SAP BASIS authorization objects and Solution Manager authorization objects

Support Package Stacks (Version)	Date	Description

SP06	2017-10-16	**General Information**
		First publication
		• As of Release 7.2, the security information on topics related to SAP Solution Manager is published within five 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.
		  i Note
		  All relevant changes for the individual applications/scenarios are documented in the document history of the individual sections.
		  • *SAP Fiori Application Guide*
		  This guide contains all information referring to security aspects for all delivered SAP Fiori Apps (ST-UI).
		  • *Secure Optimization Guide*
		  This guide contains information referring to security aspects for SAP Solution Manager users and roles in regards to Optimization and Operation.

2 List of Roles Updated per SP

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

Updated Roles per SP

SP	Roles
SP18	SAP_STWB_2_ALL
	SAP_TST_AGENT_RFC
SP17	SAP_SERVICE_CONNECT
	SAP_SERVICE_CONNECT_DISP
	SAP_SM_QGM_CM_ALL
	SAP_SM_QGM_CM_TRANSPORT
	SAP_SM_SL_ADMIN
	SAP_SM_SL_DISPLAY
	SAP_SM_SL_EDIT
	SAP_SOLMAN_READ_702
	SAP_STWB_WORK_ALL
	SAP_SDCCN_ALL
	SAP_CM_SMAN_ADMINISTRATOR
	SAP_CM_SMAN_OPERATOR

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

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

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

3 Introduction

Motivation and Use of This Guide

This guide covers **Security Optimization and Operation** topics for SAP Solution Manager to provide a standard security concept.

> ℹ Note
>
> If you require a higher level of security, we recommend specific security consulting.

For general information on the authorization concept of SAP Solution Manager, application-specific authorizations, SAP Fiori apps, or setup security, see the complementary guides on the SAP Support Portal at: https://help.sap.com/viewer/p/SAP_Solution_Manager ▶ *SAP Components* ▶ *SAP Solution Manager* ▶ *<current release>* ▶ (updated with every change per Support Package).

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

This security guide does not provide any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements. In addition, this guide does not recommend additional features that would be required in a particular environment. Decisions related to data protection must be made on a case-by-case basis and under consideration of the specific system landscape and the applicable legal requirements.

OWASP Top 10

> → Remember
>
> **It is highly recommended that you treat an SAP Solution Manager system as an integration platform and a single point of access to all of your connected managed systems, with the same care and attention to security as all of your other business systems.**

Securing your system environment and all the apps that run on them is critical to your business, especially your business data. According to the *Open Web Application Security Project* (OWASP Top 10 in 2017), the main points of attack against your systems are the following:

1. SQL Injections
2. Authentication and Session Management
3. Cross Site Scripting
4. Function Level Access Control
5. Security Misconfiguration

   > → Tip
   >
   > To avoid misconfiguration, check the *Secure Configuration Guide* for SAP Solution Manager.
6. Sensitive Data Exposure

7. Attack Protection
8. Cross - Site Request Forgery
9. Components with Known Vulnerabilities
10. Underprotected APIs

This guide specifically focuses on authentication, data protection, and access control. It is intended to help you secure your SAP Solution Manager applications, and optimize security controls.

Integration

Security topics are relevant for the following phases:

- Upgrade
- Operations
- Optimization

> → Recommendation
>
> Use this guide during the above-mentioned phases. For a detailed overview of which documentation is relevant for each phase, see the guide references on the SAP Support Portal at: https://help.sap.com/viewer/p/SAP_Solution_Manager *SAP Components* *SAP Solution Manager 7.2*.
>
> This document is focuses on a selection of important security-related settings in the SAP Solution Manager system to ensure a greater security during system operation. Due to its compact nature, it is not exhaustive. For more detailed information on SAP security, see the SAP Support Portal, SAP Help Portal, and SAP Developer Network sites.

What is Your Opinion?

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

More Information

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

4 Managing Authentication

4.1 Vulnerability

Authentication management is one of the main concerns regarding the security of your system landscape. Authorization and authentication issues allow external attackers to infiltrate your system. In addition, authorized users may attempt to steal and disrupt the data in your system. Therefore, any leaks or flaws in your authentication or authorization concept, such as exposed user accounts, simple passwords, or default users with unlimited authorizations, can lead to attacks. Any such attack can lead to an exposure of your user accounts. This is especially true for high-privilege accounts. An attacker may start with a user with low privileges and try to obtain higher ones.

The following sections describe in detail recommendations for dealing with default users in SAP Solution Manager, such as `SOLMAN_ADMIN`, or technical users with high privileges, such as `SOLMAN_BTC`. Recommendations include specific authorizations to restrict access to these users, secure password policy, and others.

→ Recommendation

- Protect passwords and encryption keys
- Change default user names and passwords
- Restrict access to credential storage
- Use different credentials in development and productive systems
- Use secure credentials at user level (segregation of duties)
- Store credentials in protected storages

4.2 Overview: All Standard Users Created in Basic Configuration in SAP Solution Manager Configuration

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

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

Technical Users

SAP Solution Manager System

User	User Type	Stack	In System	Created in Scenario	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 batch jobs required 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; for configuration validation
SM_AMSC	System	ABAP	SM	System Preparation	For Automated Managed System Configuration to run update job
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 SAP Solution Manager as managed system
SMB_*	System	ABAP	SM	Managed Systems Configuration	For backward communication from managed system to SAP Solution Manager
Guest (Wily)		Java	SM	Managed Systems Configuration	Built-in user of the Introscope Enterprise Manager

Managed System

User	User Type	Stack	In System	Created in Scenario	Additional Remarks
SMDAGENT_xxx	System	ABAP	MS	Managed Systems Configuration	To connect Wily host to managed systems

User	User Type	Stack	In System	Created in Scenario	Additional Remarks
READ	System	ABAP	MS	Managed Systems Configuration	To read table information from the managed systems
TMW	System	ABAP	MS	Managed Systems Configuration	To read table information from the managed systems and schedule batch jobs in the managed systems
SM_COLL_xxx		ABAP/ Java	MS	Managed Systems Configuration	For data collection in the managed system

BW System

User	User Type	Stack	In System	Created in Scenario	Additional Remarks
SMD_BI_RFC	System	ABAP	BW	Infrastructure Preparation	If a remote BW system is used to load data into the BW system
SM_BW_ADMIN	System	ABAP	BW	Infrastructure Preparation	To initially configure the BW system
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	If a standalone BW system is used to extract data
SM_BOC	System	ABAP	BW	Infrastructure Preparation	Business Objects Cloud

SLD Users

User	User Type	Stack	In System	Created in Scenario	Additional Remarks
SLD_CS_USER	System	ABAP	SLD	Infrastructure Preparation	To collect system landscape information
SLDAPIUSER	System	ABAP	Central SLD		
SLDDSUSER	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 SOLMAN_SETUP	Additional Remarks
DDIC	Dialog	ABAP	SM		This user is required for all SAP system. For more information on this user, see the SAP NetWeaver documentation for the relevant SAP Basis release. **⚠ Caution** This user usually receives the profiles SAP_ALL and SAP_NEW. **Therefore, we highly recommend that you de-activate the user after configuration and/or changing the password.**
SOLMAN_ADMIN	Dialog	ABAP	SM	Procedure Call (Pop-Up)	**Configuration user** relevant for SAP Solution Manager to be used for the following scenarios: *System Preparation*, *Infrastructure Preparation*, *Basic Configuration*, *Managed Systems Configuration*, *EarlyWatch Alert Management*
SAPSUPPORT	Dialog	ABAP	SM, BW, Managed System	Basic Configuration, Managed Systems Configuration	Diagnostics **display** user for SAP Support
SAPSERVICE	Dialog	ABAP	SM, BW	Basic 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	MS	Managed Systems Configuration	For Java stack administration
SA_ADM_XXX	Dialog	ABAP	SM	Basic Configuration	SAP Solution Manager administration

4.3 Overview: All End-Users and Business Partners per Configuration Scenario

For all scenarios in SAP Solution Manager Configuration, 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 SAP Solution Manager system, the managed systems, the BW system, and functions that require business partner users in the SAP Solution Manager system:

Scenario	User in SAP Solution Manager	User in Managed System	User in BW System	Business Partner Required
Implementation	X	X (Customizing Distribution)		X
Test Suite	X	X (Test Execution)		X
ITSM Incident Management	X			X
Technical Administration	X	X		
Application Monitoring	X		X	X
Business Process Operations	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

4.4 Using Solution Manager User Administration

SAP Solution Manager Administration Views: Security, Users

SAP Solution Manager Administration contains views that are relevant for the administration of the SAP Solution Manager system. Here, the *Security* and *Users* apps are mentioned in detail as they relate to the security of your system.

You can access the tiles using transaction `SM_WORKCENTER` and the SAP Fiori launchpad.

Security

As of SAP Solution Manager Release 7.2 SPS 5, steps and activities in the basic configuration of SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`) that are relevant for the overall security of your system, are flagged as security-relevant. You can display them all by choosing the *Security* app in the *SAP Solution Manager Administration* launchpad group. For more information about specific topics of these steps, see the following sections in this guide.

User Administration

The *User Administration* app gives you access to *Solution Manager User Administration (SMUA)*. This tool is described in detail in a following section of this guide.

How to Access the Overview

You can access the overview of all security-related activities in the corresponding tile from the *Solution Manager Administration* launchpad group on the SAP Fiori Launchpad.

The tile is not displayed by default.

> ℹ Note
>
> If you require the tile, you have to personalize the SAP Fiori launchpad accordingly.

Required Authorization

To be able to use the tile, you must have at least the following roles:

- `SAP_SM_SECREL`
- `SAP_SOLMAN_SETUP_ADMIN_ALL`
- `SAP_SMWORK_SM_ADMIN` - access
  You can also create a user from the SAP Solution Manager Administration use case ID *SA_DIS_<System ID>*, in the basic configuration procedure in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`).

> → Recommendation
>
> We recommend that you use a dialog user created from the template user `SOLMAN_ADMIN` to use the application in edit mode.

4.5 How to Handle Default Standard Users - SOLMAN_ADMIN, SMC* Users, and Template Use Case IDs

General Considerations

Any standard user in a system can pose a serious risk to your system landscape. SAP Solution Manager ships with several **default users** for convenience, such as dialog user `SOLMAN_ADMIN`, which is used for the basic configuration of SAP Solution Manager, or users starting with naming convention `SMC*`, to which all the necessary roles and authorizations to run a guided procedure configuration are assigned. See below a detailed explanation of how to handle these users.

> → Recommendation
>
> In general, we recommend that you use one of the dialog standard users delivered with SAP Solution Manager as a template only, and create a dialog user with a unique name. You can do this with all relevant standard default use case IDs shipped with SAP Solution Manager. This allows you to directly track all actions of this user in the system, which is not the case if you leave them as default users. **In production, either remove any created default users from the system, lock them, or remove their role assignment, and so on.**

Avoiding Profile SAP_ALL with Dialog User SOLMAN_ADMIN

> i Note
>
> Avoid users with profiles `SAP_ALL` and `SAP_NEW` for configuration.

Handling User Roles for SOLMAN_ADMIN

The only task of the dialog template user `SOLMAN_ADMIN` is to be able to configure the *Basic Settings* for SAP Solution Manager system landscape to run Infrastructure, Prerequisites, Managed Systems, and Cross-Scenario settings, as well as the mandatory scenario SAP EarlyWatch Alert management. It is not designed to run any application or other configuration procedure. The user is assigned a set of roles that allow the configuration of the guided procedures mentioned above. The authorizations are a minimal set. However, the number of authorization objects and the combination of these objects make this user a security issue in its own right. Therefore, we recommend you handle this user as follows:

> → Recommendation
>
> - To be able to track historical documents for forensic purposes, use this user as a template to create a named dialog user.
> - To control the activities of such a powerful user, create separate users with segregation of duties, such as a user for configuration, a user for user management, and a user for role assignment.
> - When you update your SAP Solution Manager system configuration, check the user authorizations for this user again, and update its authorizations.

- Use the default user SOLMAN_ADMIN to create any of the scenario-specific configuration users SMC* and technical users. Then, immediately remove the SAP_SM_USER_ADMIN role from the user.
- Only allow the configuration users to be active in the system for the time of configuration. Lock them afterwards or set a limited *Time Validity*.
- If you require a user to display and check specific configuration settings, replace all roles with full authorization with individual display roles.

Using and Adapting Predefined Authorization Roles

All roles assigned to users created in transaction SOLMAN_SETUP are fully maintained. For authorization fields that cannot be prefilled with default values delivered by SAP, an asterisk (*) is maintained to allow full authorization for this field. For example, the system ID field in authorization object AI_LMDB_OB cannot be prefilled by SAP due to its generic nature.

→ Recommendation

We strongly recommend that you maintain all fields in authorization objects in delivered roles to maintain according to your security guidelines.

Update Users When Roles Have to be Updated

Update your users when roles/authorizations have to be updated. In addition, you can use the update function to update/enhance existing users with additional role assignments. For example, you can update/enhance the user SOLMAN_ADMIN with configuration roles for scenario-specific guided procedures in SOLMAN_SETUP.

You can upload the authorization roles for the READ user and the TMW user from SAP Solution Manager to the managed systems.

Handling Password Changes

⚠ Caution

If you change or reset the password for the user SOLMAN_ADMIN, you also have to change the password in the SAP Solution Manager User Administration (SMUA) app, which is accessible through transaction USR_MNGT. The system then pushes the information to GENSTORE.

→ Tip

If you have changed the password for the user SOLMAN_ADMIN and are experiencing frequent locks, it is likely that the user is being used in multiple configuration scenarios. We highly recommend that you use this user only for configuration purposes, and deactivate it after configuration. For more information, see the section on this user in the *Secure Configuration Guide for SAP Solution Manager*.

Use the following tracing options:

- The audit log trace using transactions SM19 and SM20 to determine the source address from which the user is trying to access the system.
- The change documents using transaction SUIM to determine the reason why a user is locked.
- See SAP Note 1493272 - A user gets locked automatically for information on how to check on Java stacks.

Use Case ID: SMC_*** Configuration Users

All SMC_**Configuration Users* receive the following roles and corresponding authorizations:

- SAP_*_CONF* role: Contains all relevant application-specific authorizations for both mandatory and optional activities. See also the following link for the difference between mandatory and optional configuration settings in ITSM "Quick Setup": https://blogs.sap.com/2017/08/14/sap-solution-manager-7.2-it-service-management-quick-setup/

  > → Recommendation
  >
  > If you want to configure only the minimum settings for your scenarios and want to reflect this in your roles as minimum authorization, you have to run a specific trace for only mandatory activities and then either create your own roles or remove unnecessary authorization objects from the roles delivered by SAP. We recommend that you run the configuration with the standard roles delivered by SAP and either set the user inactive or remove (substitute or set inactive) the assigned roles after configuration. Do not keep the configuration user in an active state in your system.

- 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 Adjustment* tool in transaction SOLMAN_SETUP.
- SAP_SM_USER_ADMIN role: Contains full authorization for *User Management* (transaction SU01) and *Role Management* (transaction PFCG).

> → Recommendation
>
> We recommend that you use the predefined configuration user template to create a named configuration user for the configuration, as the authorizations assigned to these users are specifically tailored to the individual procedure. This ensures that the user cannot be misused for any other tasks.

SOLMAN_SETUP User Generation Dialog Popup

General Information

Each scenario in SAP Solution Manager has to be configured using the Guided Procedure (GP) for configuration of it in transaction SOLMAN_SETUP. To avoid a configuration user needing profile SAP_ALL, specific configuration user templates are shipped with minimal authorizations assigned (template user name convention: SMC*). Whenever a new dialog user starts to configure a new GP in transaction SOLMAN_SETUP, this user is automatically checked by the system for correct authorizations. If the user in question does not have the required roles, the system displays a popup in which the user can be created with the required authorizations.

> → Tip
>
> If you do not assign transaction SU01 (or corresponding role SAP_SM_USER_ADMIN) to your user, but the authorization object SM_SETUP with ACTVT 02, the system automatically displays a popup the option to *Request Authorizations* for a guided procedure. In this case, the system generates an HTML report with the required authorization roles for the specific Guided Procedure.

How to Deactivate the Authorization Request Dialog

There are several ways to disable a popup:

- Call transaction `SOLMAN_SETUP` by ignoring the popup *Always*
- Set a personal setting for it.

  > **i** Note
  >
  > Any user can use the *Personalization* link to disable this popup whenever roles are updated with authorization objects by SAP. This does not work for newly shipped roles.
  >
  > 1. In the transaction, choose *Personalization*.
  > 2. Mark the box for **Logged on User**.

- Add the user parameter `SETUP_HIDE_PERMCHECK` to the user profile of the configuration user.

  > → Recommendation
  >
  > We recommend this version to be used and set by your system administrator in advance to configuration.

Restricting Access to Transaction SOLMAN_SETUP by Using Critical Authorization Object SM_SETUP

The authorization object `SM_SETUP` controls whether a user can access the transaction `SOLMAN_SETUP`. It also controls which functions the user `SOLMAN_ADMIN` can use in this transaction.

Overview on Specific Role Restrictions During Administration and Operation

After configuring or updating SAP Solution Manager, you can restrict the authorizations for the dialog user `SOLMAN_ADMIN`. For example, the role `SAP_J2EE_ADMIN` allows administration authorization for all areas of `J2EE`. To separate and/or restrict this authorization, you can remove this role from the `SOLMAN_ADMIN` user and assign the corresponding restrictive roles. In addition, the following roles should be removed after configuration:

- `SAP_SM_USER_ADMIN`: Remove or restrict. The role contains the authorization object `S_USER_GRP` with `ACTVT 05` (unlock). This authorization is used to unlock locked users during the configuration of users (creation, update). `ACTVT 03` (display) is added for the user to check the status of the BACK RFC-user.
- `SAP_SM_GATEWAY_ACTIVATION`
- `SAP_SM_ROLECMP_ALL`
- `SAP_SM_SMUA_ALL`
- `SAP_SM_RFC_***`: The object `S_RFC_ADM` allows the user to access transaction `SM59` (coupled with authorization object `S_TCODE: SM59`). 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.

> **Note**
>
> If the authorization object S_RFC_ADM 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 example, for the user interface for creating READ or TMW managed system users.

- **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 corresponding security guide for NW Java
	SAP_RCA_AGT_ADM_VIA_SLD	This role enables the Expert User Interface in Java for Agent Candidate Management. It should only be assigned to specific users.
	sap.com/tc~monitoring~systeminfo*sap_monitoring/SystemInfo_Support_Role	No Help Text ID, see the corresponding security guide for NW Java
	sap.com/SQLTrace*OpenSQLMonitors / OpenSQLMonitorLogonRole	No Help Text ID, see the corresponding 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 the authorization object AI_LMDB_OB, a user with access to SLD and role SAP_SLD_GUEST can read all system information in SLD.

Dedicated Role Adjustment after Support Package Update with Role Adjustment Tool

Part 1: Customer Authorization Value Table Adjustment

When roles have to be updated, you first have to run transaction SU25 points 2a) and 2b). This is reflected in an activity in the Basic Settings Configuration in transaction SOLMAN_SETUP. Alternatively, see SAP Note 368496.

Part 2: Update Your Own Roles

Whenever a new SAP role is shipped, the existing SAP role is overwritten in the system. Therefore, we strongly recommend that you copy any SAP role that you customize to your own namespace. This is not relevant for the following roles:

- Roles for technical users in ABAP. These roles are shipped with the authorization objects and their values intended for this purpose only. They should not be maintained and can be used as shipped by SAP.
- As Java relevant roles are assigned to users in the ABAP stack, they do not contain any authorizations and should not be copied to any namespace.

> **i Note**
>
> All ABAP roles referring to J2EE security (UME) are shipped in the SAP namespace. These roles should not be copied to any other namespace as they their technical names link the user management of the ABAP stack with the user management of the Java stack.

- To update individual authorizations and authorization values, choose the *Role Adjustment Tool*.

  > **⚠ Caution**
  >
  > The use of this tool can be critical, as it allows the manipulation of any customer roles if authorization is given. **Authorization should only be assigned to a specified user responsible for role adjustment**. You can use `SOLMAN_ADMIN` user to use the *Role Adjustment 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`.
  >
  >   > **i Note**
  >   >
  >   > Role `SAP_SM_ROLECMP_ALL` is assigned to all configuration users, created in *Basic Configuration* in transaction `SOLMAN_SETUP`, technical names: `SMC_***`.
  >
  > - `SAP_SM_USER_ADMIN`
  > - In addition, you have 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` specifically assigned for the *User Creation* step.

4.6 How to Handle Technical Users

Specific Roles for Technical Users

Technical users in SAP Solution Manager are assigned specific roles. A role contains the minimum authorizations required for the task for the corresponding software component. Due to the deployment of software components in ABAP, ST, and ST-BCO, and the addition of the Java stack, there are three possible role assignments for technical users.

→ Recommendation

See the *Secure Configuration Guide* for more details on the technical user roles. The guide describes which critical authorizations are contained in the roles and what you have to consider for secure configuration.

One or Two Roles Assigned (ST: ABAP / Java)

If the ST and ST-BCO components are in a separate system due to a remote BW, each technical user with tasks in the ABAP stack receives a single role with minimum authorizations in SAP Solution Manager. If the user has additional tasks within the Java stack, an additional role may apply.

Two or Three Roles Assigned (ST: ABAP / Java and ST-BCO)

If you are using standard BW, some technical users are assigned more than one role due to the combined use of software components ST and ST-BCO. For example, the technical user SOLMAN_BTC is assigned a role for software component ST SAP_SM_BATCH and a role for software component ST-BCO SAP_BI_E2E.

Several Roles According to Critical Authorization Separation

An exception to the two use cases above is technical user SM_TECH_ADM. This technical user SM_TECH_ADM is used to perform various activities for setting up the managed system. The code is shipped with software component ST. Therefore, this technical user is assigned one single role with specifically-maintained authorization objects that form the minimum authorization required in the ABAP stack SAP_SM_TECH_ADM. The SAP_J2EE_ADMIN role is assigned based on the activities of the user in the Java stack. In addition, the single role SAP_SM_USER_ADMIN is assigned because the user has to be authorized to create users in the managed system separately.

→ Recommendation

We recommend that you remove the role SAP_SM_USER_ADMIN if you manually create managed system users in the managed system. In addition, if you do not set up Java systems, you can remove the user role SAP_J2EE_ADMIN, as it is the administrator role for the Java stack and is critical to security. After configuration, deactivate this user and reactivate only when you update the managed system setup.

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.

→ Recommendation

The user should be locked after completing the configuration tasks. If you want to upgrade the configuration, you need to unlock the user again.

Operations/Upgrade Mode

When upgrading the system, you have to check all upgrade-relevant activities in transaction `SOLMAN_SETUP`. Therefore, check all the technical users required for any necessary role updates. Update the users with the roles shipped by SAP. If you want to control which authorizations are updated by SAP, you can use the tool *Role Adjustment Tool* for analysis.

4.7 Removing Obsolete Users

→ Recommendation

We recommend that you regularly check for obsolete users and remove them accordingly. For more information on regular reporting and tools, see the *Useful Tools* section.

Removing Obsolete Technical Users

Obsolete Technical Users

Technical User Name	Obsolete since 7.2 SP	Additional Remarks
`SMDS***`	6	Changed user name from `SMDS_***` to `LMDB_DS_***`
`SMD_AGT`	5	

4.8 Check and Secure Dialog Users

Default Users and Passwords

SAP-wide default users such as `DDIC, SAP*` are critical for security. Default users are subject to the general SAP password policy. After configuration, change the password for these users, or deactivate them. For more information, see the SAP NetWeaver Security Guide.

→ Recommendation

We recommend that you check the report `RSRFCCHK`. With this report you can do the following:

- Check the complete logon info with a connection test for a specific user
- Check the type of user
- Check and monitor users
- Conduct a security measure

Consider using *Configuration Validation* on a regular basis. See the corresponding *Useful Tools* section in this guide.

Logging Off Inactive Users

For more information, see User Administration Functions

Update Passwords

If you manage users and their passwords exclusively with transaction `SOLMAN_SETUP`, the passwords are automatically adjusted in transaction `SU01` and the RFC destination. In case of CUA, `SOLMAN_SETUP` can not adjust passwords accordingly. For more information on CUA, see the *Secure Configuration Guide for SAP Solution Manager*.

4.9 Using Secure Policy for Passwords and Login

Security Policy Parameters to be Used

> **i Note**
>
> With SAP Solution Manager 7.2 and SAP Basis 7.40, you can define group-specific security policies for logons and passwords for your users. For users who should not use the default attributes, you can define individual security policies in transaction `SECPOL` and assign them to users in transaction `SU01` (transaction `SU10` for mass maintenance). For more information, see http://help.sap.com/saphelp_nw70ehp1/helpdata/EN/7f/c52442ad9f5133e10000000a155106/content.htm

Parameter	Description	Default Value
`CHECK_PASSWORD_BLACKLIST`	Check the Password Blacklist	1
`DISABLE_PASSWORD_LOGON`	Disable Password Logon	0
`DISABLE_TICKET_LOGON`	Disable Ticket Logon	0
`MAX_FAILED_PASSWORD_LOGON_ATTEMPTS`	Maximum Number of Failed Attempts	5

Parameter	Description	Default Value
MAX_PASSWORD_IDLE_INITIAL	Validity of Unused Initial Passwords	0
MAX_PASSWORD_IDLE_PRODUCTIVE	Validity of Unused Productive Passwords	0
MIN_PASSWORD_CHANGE_WAITTIME	Minimum Wait Time for Password Change	1
MIN_PASSWORD_DIFFERENCE	No. of Different Chars When Changing	1
MIN_PASSWORD_DIGITS	Minimum Number of Digits	0
MIN_PASSWORD_LENGTH	Minimum Password Length	6
MIN_PASSWORD_LETTERS	Minimum Number of Letters	0
MIN_PASSWORD_LOWERCASE	Minimum Number of Lowercase Letters	0
MIN_PASSWORD_SPECIALS	Minimum Number of Special Characters	0
MIN_PASSWORD_UPPERCASE	Minimum Number of Uppercase Letters	0
PASSWORD_CHANGE_FOR_SSO	Password Change Req. for SSO Logons	1
PASSWORD_CHANGE_INTERVAL	Interval for Regular Password Changes	0
PASSWORD_COMPLIANCE_TO_CURRENT_POLICY	Password Change After Rule Tightening	0
PASSWORD_HISTORY_SIZE	Size of the Password History	5
PASSWORD_LOCK_EXPIRATION	Automatic Expiration of Password Lock	0

Authorization objects S_SECPOL and S_SECPOL_A

If you are using security policies for your users, maintain authorization object S_SECPOL. If necessary, also maintain authorization object S_SECPOL_A to control which actions a user can perform in transaction SICF_SESSIONS. This authorization object is security-critical when assigned to a user and must be carefully considered. Authorization object S_SECPOL is delivered in its *Inactive* state in role SAP_SM_USER_ADMIN.

Password and Certificate Policy Recommendations

- Maintain a strong password policy
- Do not send passwords over email to your users
- Change passwords regularly
- Regularly check and update certificates

Authorization Object SM_GENSTOR (Generic Protection on Genstore)

Authoriaztion object `SM_GENSTOR` is used for generic password protection. It is used to protect the relevant function modules that are called during configuration. If you want to filter the access to GENSTORE data, you have to restrict the authorization object `SM_SETUP` in transaction (`S_TOCDE`) `SOLMAN_SETUP_ADMIN`.

5 Managing Authorizations

5.1 Vulnerabilities

→ Recommendation

We strongly recommend that you strictly separate the responsibilities for role management and user management, or implement a four-eye-principle workflow. In addition, carefully consider and regularly monitor your authorization concept. For more information on monitoring and reporting possibilities, see *Configuration Validation* in the *Useful Tools* section of this guide. In addition, get familiar with SAP NetWeaver Identity Management, which is used in SAP Solution Manager: https://help.sap.com/saphelp_nw70ehp2/helpdata/en/e1/120024e74011d2962b0000e82de14a/frameset.htm

Quick recommendations

- Implement segregation of duties as part of your authorization concept
- Implement strict access control with minimal authorizations for the task at hand
- Protect authorization and authentication access
- Align different authorization concepts as closely as possible
- Update user authorization regularly
- Allow limited log access

5.2 Configuration Transaction SOLMAN_SETUP - Segregation of Duties

SOLMAN_SETUP - Segregation of Duties (SoD)

Transaction `SOLMAN_SETUP` displays transaction `SU01` (*User Management*) and transaction `PFCG` (*Role Management*) in a single user interface. User management and role management should be handled separately by different users.

You can distribute the tasks to various users. This is possible by using authorization and role restrictions:

- *Access* mode restriction: You can allow a user to access the procedure only 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`.

- *Step* restriction: You can use authorization object SM_SETUP to allow access to only specific steps within the procedures. For example, you can allow for a specific administrator (such as for users and authorizations) to be able to edit only user-specific steps and display others. Similarly, you can make an administrator responsible for only BW-related setup and allow him to access only those steps in *Edit* mode.
- *Topic* restriction: You can grant administrator users access to specific topics, such as users and roles, BW configuration, or managed system configuration. Do this by restricting user role assignments. For more information on which roles are assigned to the dialog user SOLMAN_ADMIN and what authorizations they contain, check the *Secure Configuration Guide* for this user.

User and Roles Administration Role SAP_SM_USER_ADMIN

Role Assignment

The role SAP_SM_USER_ADMIN contains administrative authorizations for both transactions:

- SU01
- PFCG

This role is assigned to all SMC_*** users and SOLMAN_ADMIN by default, but marked as being **optional**. The role allows for full authorization, which can be a security risk. SMC_*** users are required to create template users. Therefore, if you do not use template users, this role is not required for configuration. **Before generating an SMC_*** user, carefully consider the assignment of this role.** It contains authorization for *User Management* (transaction SU01) and *Role Management* (transaction PFCG).

→ Recommendation

- If you work with an SoD between role assignment and user generation, we recommend that you copy the role manually in transaction PFCG. Use a menu entry to distinguish between a role for user assignment and role assignment. You can do this, for example. by removing the access transaction PFCG in one role and access transaction SU01 in the other. If this causes too much overhead, we strongly recommend that you remove the role from your user after configuration, or set a specified time frame validity date for this role. In any case, assignment of the role is a security risk and should be considered carefully.
- We strongly recommend that you regulate the use and assignment of this role to your configuration users. In case of dialog user SOLMAN_ADMIN, it is required for all technical users and basic dialog users. After you have created all technical users, permanently remove this role from your SOLMAN_ADMIN user until you need to update the roles as part of an SP update for your system.
- For SMC_*** users, it is required to create template users. If you do not require your users to create any template users during SOLMAN_SETUP configuration, this role can be dismissed and must not be assigned.

Authorization Objects S_USER_***

→ Recommendation

If you assign any of these objects to a user outside the use of the roles SAP_SM_USER_ADMIN and SAP_SM_USER_DISPLAY, carefully consider how to maintain the values for these objects. We recommend that you have minimal authorizations such as ACTVT 03 and 08 for display purposes together with transaction SU01D (strict display).

Using Role Namespace and User Group to Separate Users

The *Expert Mode* allows you to use the following features for user creation, role creation as well as assignment:

- Define namespace for roles
- Define and assign the user to a specific user group

You can set a specific namespace for the roles that the system assigns to a user. The default namespace is *Z*.

> ℹ Note
>
> All roles assigned to the predefined users:
>
> - `SAPSERVICE` receive namespace `ZSD`.
> - `SMC_MIG_*` receive namespace `ZM`.
>
> This namespace is set because the authorizations for these users are predefined and should not be changed.

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

> → Recommendation
>
> - We recommend group users. You can then easily search for them and restrict access to them using authorization object `S_USER_GRP`.
> - Any predefined users such as `SAP*, DDIC, EARLYWATCH,` or `TMSADM` should be assigned to a separate user group such as `SUPER`. For more information on these users and how to protect them, see https://help.sap.com/saphelp_nw70ehp1/helpdata/en/3e/cdaccbedc411d3a6510000e835363f/frameset.htm. In addition, see the section *Configuration Validation* for ConfigStore `STANDARD_USERS` in this guide.

5.3 Roles and Authorization Management

User Creation Interface in SOLMAN_SETUP and SMUA

You can create users and update user roles in transaction `SOLMAN_SETUP` and in the SMUA app. The *Role Adjustment* tool helps you to compare the authorization objects and authorization values of your customized roles with newly-delivered SAP roles. This tool is delivered with the `ST` software component.

How does the system role copy work?

When you update a user with user roles in `SOLMAN_SETUP`, the system performs the following steps:

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

> **i Note**
>
> When you modify any authorization field in your copied role, this modification is lost with a system copy role. If you want to keep the modification, you can compare your copied role with the newly-delivered SAP role update, and then decide how to update your modified role.

How to access the role adjustment?

The *Role 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 there are differences between the target role to the SAP role. By checking these differences, you can decide whether to replace or adjust the authorization objects and authorization fields in the copied role.

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

Constraint: Adaptation of Authorization Objects

The following authorization objects can be customized using transaction `PFCG`:

- Authorization objects `S_TCODE`, `S_SERVICE`, and `S_START`: Each start transaction authorization object can be maintained the *Menu* tab in a role using transaction `PFCG`.
- Authorization object `S_RFC`: `S_RFC` can't be maintained using the standard values. You have to either adjust the authorization object for the application in transaction `SU24` or add a manually-created authorization object maintenance in transaction `PFCG`.
- Authorization object `PLOG`: Organizational units (such as those maintained in authorization object `PLOG` for `HR`) have to be maintained in transaction `PFCG`.

Edit Authorizations for SOLMAN_SETUP, SMUA, and Role Adjustment Tool

Transaction SOLMAN_SETUP

The authorization for *General User Management* and *Role Assignment* is granted by the authorization object `SM_SETUP`. This authorization is contained in all `SAP_SETUP_BASIC_***` configuration roles and roles.

Application SMUA

Authorization object `SM_SMUA` has to be assigned. This authorization object is contained in the single role `SAP_SM_SMUA_*`.

Role Adjustment Tool

Authorization object `SM_ROLECMP` has to be assigned. This authorization object is contained in the single role `SAP_SM_ROLECMP_*`.

> **→ Recommendation**
>
> We recommend that you assign these authorizations carefully.

Inactive Authorization Objects

Some navigation role menus contain additional transactions. These transactions have to be available in the *Menu* tab as they define the transaction navigation in the launchpad group. Having transactions in the *Menu* tab allows the system to automatically track all relevant authorization objects that are connected to that transaction. The authorization objects for these transactions are set to inactive.

> ⚠ Caution
>
> Do not activate inactive authorization objects in the shipped navigation roles. Doing so may override your existing authorization concept.

Documentation Possibilities

In transaction `SOLMAN_SETUP` as well as the Solution Manager User Administration (`SMUA`) app, SAP provides documentation on users and assigned roles through a link in the *Documentation* column on the user interface of the app. 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`.

For more information on any specific role, or if you want to adapt the original to your own requirements, follow these steps:

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 *Display*. The system displays the text that is also linked in the setup screen.

> ℹ Note
>
> - All documents for authorization roles description shipped by SAP have the naming convention `AUTH_*`. Consider using your own naming convention.
> - All documents for user descriptions shipped by SAP have naming conventions either `TP*` or `USER_*`. Consider using your own naming convention.

5.4 Restricting Roles to Allow Minimal Authorization

> → Recommendation
>
> We strongly advise that you maintain copied SAP-delivered roles according to your requirements. Consider which scenarios you use and which requirements you need to fulfill.

Restrict Authorizations for System Administrators

We strongly recommend that you restrict authorizations for system administrators to the required minimum. System administration typically have more and also more critical authorizations than any other end user in your organization. We recommend that you distinguish between system administrator tasks, such as *User Administration* as opposed to *Role Administration*. You can use roles (such as `SAP_SM_USER_ADMIN`) and authorization objects (such as `SM_SETUP` or `AI_LMDB_OB`) to limit the authorizations per system administrator.

Restrict Extractor Authorization

The role `SAP_SM_INC_EXTRACTOR` also contains the authorization object to allow for PPM extractor runs `ACO_SUPER` with values `DPO` and `PPO`. If you do not use PPM and the cProject integration, you can set the authorization object to inactive.

Restrict Access to Dashboards

If you want to minimize authorizations of the role `SAP_SM_DSH_DISP` for specific applications, such as `ITPPM`, you have to specifically maintain the authorization objects `SM_DSHO` and `SM_DSH_CAT`.

5.5 Transporting Roles from Development to Production

> → Recommendation
>
> For your development systems, we strongly recommend that you create roles for dialog users with specific maintenance of authorization field. Transport these roles to your production system. If your security protocol requires a certain authorization level for technical users, we recommend also transporting these roles. Note that some authorization objects, such as `AI_LMDB_OB` or `SM_SDOC`, may have to be adjusted in the productive system due to required IDs that are dynamically-generated. For more information, see the *Protecting Systems and Processes* section.

Activating the Transport Request Tool

For documentation purposes, you can activate automatic transport request.

Prerequisites:

- Configured *Automatic Recording of Changes* in transaction `SCC4`

- Configured *Transport Management*
- Maintain table `PRGN_CUST`, adding value `CLIENT_SET_FOR_ROLES`

> **i** Note
>
> This function is only available in the SAP Solution Manager system. In your managed systems and a remote BW system, you have to add your roles to a manually-created transport request. If you transport roles to your productive system, you should remove any access to transaction `PFCG`.

Required Transport Authorizations

For a successful transport, you require at least the following security-critical 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`

5.6 Function Calls

General Issues

In the context of security of `RFC` calls, consider the following three areas:

- *Authentification*
  Incoming `RFC` connections have to authenticate in the system. For example, the `READ RFC` call is an incoming `RFC` call in the managed system. Therefore, a user has to be present in the managed system to authenticate the `RFC` call. A user of type *system* is used here. From the point of view of the SAP Solution Manager system, the `READ RFC` connection is an outgoing `RFC`. Outgoing `RFC` connections are maintained in transaction `SM59` in this system. The user is maintained in the `RFC` itself. When you set up managed systems in SAP Solution Manager, most `RFC`s are automatically created, along with the users in the managed systems, and the authorizations assigned to this user. The `RFC`s are automatically added to transaction `SM59`. `RFC` traces (transaction `ST05`) and the Security Audit Log can be used to evaluate and monitor them.
- *System Profile Parameter*
  The `RFC` authorization check can be activated/deactivated with the system profile parameter `auth/rfc_authority_check`. This parameter must not be set to '0'. If you set the value to 9, the system only accepts the values of `FUNC` (function module) in the authorization object. Make sure, that all roles only contain `FUNC` (except for function group `SRFC`). For more information, see SAP Note 931252.
- *Transaction Code SE37*
  We strongly advise not to assign transaction code `SE37` to any dialog user. The authorization for this transaction should be handled very carefully and assigned only to specific users. The combination of this transaction code with the authorization object `S_RFC` is security-critical.

Authorization Object S_RFC

A remote function call (RFC) calls a function module in another system. Due to the nature of SAP Solution Manager, the number of RFC calls to and from other systems is high. Therefore, a large number of function modules are affected.

> **Example**
>
> The SYST function group is required to call SM59. If it is missing, the *remote logon* in transaction SM59 causes the RFC_NO_AUTHORITY ABAP runtime error in the target system.

For S_RFC value changes for the technical RFC users for READ and TMW RFC connection, see SAP Note 1572183.

Since SAP_BASIS 7.02, you can maintain the authorization object for certain function groups but also for function modules. In SAP Solution Manager, the authorization object is maintained according to this differentiation.

The authorization object S_RFC can be traced with the audit log trace in transactions **SM19** and **SM20**. To protect the deletion of traces, maintain the field *ACTVT* with the value **36** of authorization object S_RFC_ADM.

> **Caution**
>
> Currently, RFC function modules in function group /SSF/INTRFC do not have their own authorization checks.

> **Note**
>
> For more information on RFCs and how to secure them, see http://scn.sap.com/docs/DOC-60425 and SAP Note 14113011.

Authorization Object S_DEV_REMO

In managed systems as of SAP_BASIS 8.03 and higher, the function group RFC1 is additionally protected by the authorization object S_DEV_REMO. Therefore, all relevant roles for setting up managed systems using transaction SOLMAN_SETUP contain authorization object S_DEV_REMO.

5.7 Start Authorizations

Transactions, Web Dynpro apps, and OData services have so-called start authorization objects. These authorization objects are called when the user calls a transaction, a Web Dynpro app, or an OData service.

Authorization Object S_TCODE for Transaction

To run a transaction in an SAP system, the system calls the authorization object `S_TCODE`, which has to be assigned to the user who runs the transaction.

> ⚠ Caution
>
> `S_TCODE` should only contain the transaction codes that the user is allowed to run.

Authorization Object S_START for Web Dynpro App

S_START substituting S_SERVICE

Web Dynpro apps have the start authorization object `S_START`. `S_START` is delivered with SAP Basis Release 7.40. This authorization object replaces the authorization object `S_SERVICE` as the start authorization object.

> i Note
>
> In addition to the authorization object `S_START` with SAP Basis 7.40, the authorization object `S_USER_STA` is required if a user wants to add a new Web Dynpro app to the menu of an authorization role.

Authorization Object S_SERVICE for OData Services

OData services have the start authorization object `S_SERVICE`.

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

5.8 User Security

With SAP Solution Manager 7.2 and SAP Basis 7.40, you can define group-specific security policies for *Logons* and *Passwords* for your users. For users who should not use the default attributes, you can define individual security policies in transaction `SECPOL` and assign them to users in transaction `SU01` (transaction `SU10` for mass maintenance). For more information, see http://help.sap.com/saphelp_nw70ehp1/helpdata/EN/7f/c52442ad9f5133e10000000a155106/content.htm

Security Policy Parameters to be Used

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

Parameter	Description	Default Value
PASSWORD_LOCK_EXPIRATION	Automatic Expiration of Password Lock	0

Authorization objects S_SECPOL and S_SECPOL_A

If you are using security policies for your users, maintain authorization object S_SECPOL, and if required, authorization object S_SECPOL_A. The authorization object S_SECPOL is delivered as *Inactive* in role SAP_SM_USER_ADMIN.

5.9 SAP Basis Critical Authorizations and Combinations

System Authorization S_ADMI_FCD

This authorization object controls access to several SAP Basis functions, such as spool administration and monitoring. It is a security-critical object. It has to be checked carefully in combination with the following transactions:

- SM13
- SCC4 with S_ADMI_FCD value T000, which allows creation of client authorization.
- SARA for archiving
- SP01
- SM30, SM31, SE16N, STRUST
- SM01
- STAT, STAD, STAUTHTRACE
- SP11, SP12
- SICF
- SM50, SM51, SM04, SMICM
- SM59
- SLICENSE
- SM54
- SM55
- SM18 and SM19

> **i Note**
>
> The transactions provide access to the security audit lock with values AUDA or AUDD. We strongly recommend that you don't assign these values to any end user roles.

File Access Authorization S_DATASET

Use this object to assign authorizations for accessing operating system files. This object can also be used to assign the authorization to use operating system commands as file filters.

> ℹ Note
>
> Always make sure that a specific program name and physical file name are specified. All SAP Solution Manager standard roles are shipped with program specification, but not with values for the physical file name. In addition, `ACTVT 06` for deletion is security-critical. In general, the corresponding section in the app-specific guide provides an indication of why this activity may be required in the respective app.

ABAP Workbench Authorization S_DEVELOP

`S_DEVELOP` is the general authorization object for ABAP Workbench objects. Use it to grant access authorizations for all ABAP Workbench components, including the following:

- ABAP development tools
- ABAP Dictionary and Data Modeler
- Screen Painter and Menu Painter
- Function Builder
- Repository Browser and Info System
- SAP SmartForm

> → Recommendation
>
> From a production perspective, it is critical that users are assigned the authorization object `S_DEVELOP`. In general, the authorization object `S_DEVELOP` with more than display access (`ACTVT 03`) is not required by any user in production.

> ℹ Note
>
> The authorization object is assigned to the `SOLMAN_ADMIN` user in role `SAP_SETUP_BASIC_S_DEVELOP` for maintaining transaction `SNOTE` during the SAP Solution Manager basic setup. After implementing all required SAP Notes in the system, you can set the corresponding authorization object to inactive. For more information, see the guided procedure for the automated setup.

The authorization `S_DEVELOP` defines the access to objects in the ABAP Workbench. The object is shipped in the standard SAP Solution Manager roles. If `ACTVT 16` (execute) is added to the object, this is described in the role description tab and in the security guide for the specific application.

> → Recommendation
>
> The following recommendations apply to critical authorization combinations:
>
> - Do not assign debugging authorization in the productive system. `S_DEVELOP` with value `DEBUG` often appears in authorization traces, although it is not required as an authorization for the user. You can ignore it.

- Do not assign transaction SE38, instead use SA38. Transaction SA38 automatically calls authorization object S_PROGRAM. In combination with S_DEVELOP value PROG and ACTVT 16, this is security-critical.
- To disable authorization checks for transactions, do not assign transaction SU24 to any user. A combination of this transaction with S_DEVELOP ACTVT 02 and value SUSK plus authorization object S_USER_GRP change authorization is highly security critical.
- Carefully check the assignment of transactions SE11 or SE13, as it may allow data dictionary maintenance (ACTVT 02 and values STRU or TABL) or table modification if assigned with S_DEVELOP ACTVT 02 and value TABL.
- Carefully check the assignment of transaction SE37, as it may allow RFCs via function calls if assigned with S_DEVELOP ACTVT 16 and value FUGR.
- Transaction SE93 and S_DEVELOP ACTVT 01/02 with value TRAN allows the maintenance of transaction codes.
- Transactions SE16/SE16N and in S_DEVELOP ACTVT 02 with TABL together with object S_TABU_DIS ACTVT 02 (change): This allows you to replace and debug tables in SAP Solution Manager. Transaction SE16 automatically calls S_TABU_DIS. Therefore, table maintenance and development authorization other than ACTVT 03 is critical.

S_DEVELOP in a BW Environment

When you activate content in BW, the authorization object S_DEVELOP is requested with a temporary package assignment $tmp. This is a specific feature for BW. The concept is that the activation is performed in a specific system. If you want to transport, you can change the package in the transport request.

Documentation Maintenance Authorization S_DOKU_AUT

The authorization object S_DOKU_AUT is required to maintain online documentation in transaction SE61

Authorization for GUI Activities

Authorizations for activities with reference to GUI objects. With this object, you can, for example, assign the authorization to save lists to local files (download lists).

Administration for Internet Communication Framework S_ICF_ADM

Authorization check for activities in the Internet Communication Framework (ICF). It allows administration in the ICF, which is considered as security critical.

Number Range Maintenance S_NUMBER

Authorization to maintain number ranges or to change the number of the last number range used. You do not require authorization to display number range objects. This authorization is contained in the SAP Solution Manager roles for *Requirement Management* and other CRM-related roles.

File System Access via ABAP/4 Authorization S_PATH

Authorization groups for the file system are defined in the table `SPTHB`. This table assigns authorization groups to paths in the file system.

ABAP: Program Flow Checks Authorization S_PROGRAM

Authorization to run ABAP programs by program group.

> **i** Note
>
> You can define authorization groups for a group of programs.

CCMS: System Administration Authorization S_RZL_ADM

Authorization object for R/3 System administration using the Computing Center Management System. Although the object is rarely used in the SAP Solution Manager standard roles, check if the object is used for appropriate assignment to users.

TREX Administration Authorization S_TREX_ADM

With this object, you can use the TREX administration tool. It is contained in the SAP Solution Manager standard role for TREX Admin `SAP_SM_TREX_ADMIN`, which is assigned to the user `SOLMAN_ADMIN` in transaction `SOLMAN_SETUP`. The `SOLMAN_ADMIN` user is authorized to set up the TREX tool. If you do not require this authorization, remove the role from the `SOLMAN_ADMIN` user.

Transport Management Authorization S_SYS_RWBO and S_TRANSPRT

Both authorization objects are relevant for Transport Management. For more information on these authorization objects and combinations, see section *Change Control Related Issues*.

> **i Roles**
>
> Role SAP_SM_GP_ADMIN contains this critical authorization combination.

ABAP Function Call Authorization S_RFC

The authorization object S_RFC can be found in many roles for SAP Solution Manager. With this object, you can run Function Modules. The combination of this authorization object with transaction SE37 is security critical. We recommend that you only assign transaction SE37 to specific users.

5.10 Configuration Authorization

You can use the authorization object SM_SETUP to protect the SAP Solution Manager configuration transaction SOLMAN_SETUP. When you run transaction SOLMAN_SETUP, you can restrict access at the following levels:

- Activities
- Scenarios/Procedures
- Steps within a procedure

Note the following conditions:

- If you grant display authorization (ACTVT 03) for any scenario, the user is not allowed to edit any step within the relevant procedure.
- If your security policy only allows certain users to maintain a specific set of steps within the procedures, you can restrict at the procedure and step level.
- If a user is not assigned this authorization object, but still has access to the transaction via authorization object S_TCODE by using the work center for SAP Solution Manager configuration (also using WDA: AGS_WORKCENTER), the system does not display any data on the user interface.

5.11 Updating Authorizations and Roles

Authorization Adjustment

Each time an authorization object is changed and customized, you can use the report REGENERATE_SAP_NEW to generate the SAP_NEW profile. You can then assign this profile to your users, so that your business is not interrupted.

Role Comparison after Updated Roles

Roles are shipped in the software components `ST, ST-BCO, ST-PI, ST-UI,` and `ST-ICC`. In the SAP Solution Manager system, all required users and template roles are available in transaction `SOLMAN_SETUP`. Here, the system displays all roles and users that have to be updated by assigning an *Update Flag*. This is not possible for users and roles transported to managed systems or separate BW systems in your landscape. To find out about any changes to these roles that are shipped with new SPs, proceed with the following steps:

Role Description Tab

1. When you have upgraded your system to a new SP level, check the documentation history in the *Secure Configuration Guide for SAP Solution Manager* for that SP. Here, you can find the latest changes for roles for this SP. If you find the ST-PI roles for the users of the managed system as changed, proceed with the next step. If not, you don't have to do anything.
2. In your managed system, check the SAP role mentioned in the guide. On the *Description* tab of the role, you can see all the changes to authorization objects and authorization fields that have been shipped. You can adapt your role in the development system according to this information and transport the changes.

Tool Support Transaction SUIM

1. Go to transaction `SUIM`.
2. Go to `COMPARISONS -> OF ROLES`.
3. In field *role A*, enter the role in the SAP namespace. In the other field, enter your current copy of this role.
4. Based on the results, customize your copied role and transport the new version.
   The system displays all differences between the two roles. You can also use this view to display relevant field values.

5.12 Modifying Values in Authorizations (CRM)

The following section provides an overview of all relevant authorization objects and roles for apps that are based on CRM software components, such as *Change Request Management* or *Incident Management*. Here, changes in the customizing of the transaction types result in modifications necessary in the authorization objects. Below is a list of relevant authorization objects that you need to modify:

- `CRM_ORD_PR`
- `SM_TIMEREP`
- `SM_FIELD`
- `SM_APP_AP`
- `SM_BPCA`
- `B_USERSTAT`
- `B_USER_ST`

6 Securing Your Systems

6.1 Vulnerability

> **i Note**
>
> For guidance on secure configuration for SAP Solution Manager, see the *Secure Configuration Guide*. As configuration of SAP Solution Manager is executed using transaction `SOLMAN_SETUP`, carefully read the relevant documentation for the individual activities. See also the *Security Flags for Relevant Activities in SOLMAN_SETUP* section in this guide. Repeated checks and monitoring can easily detect infiltration during operation. We also strongly recommend that you set up a multi-tiered environment of systems, where users with the same purpose receive different passwords for each landscape and environment.

A secure configuration of your system and system landscape is a prerequisite for a secure operation of all relevant applications running on that system. If it is not secured, it exposes all your applications running on your system, as well as the system itself, to vulnerabilities. Therefore, the entire stack must be configured in a secure manner. If your system configuration is not secured, it is open to any attacker to misuse user accounts (such as default user accounts; see section *Managing Authentication*), unused apps that are still running, known but unpatched flaws, unprotected files and documents, and so on. By using a misconfigured system, an attacker can easily remain in a system undetected, modify your data, and gain access to your business data without your knowledge. Similarly, authorized users may abuse an insecure configuration. In the worst case, this can lead to a complete compromise of your system and your system landscape. Considering the SAP Solution Manager system's approach as a single point of entry to your system landscape, this is especially true for this system.

Often, various vulnerabilities resulting from misconfiguration can lead to a security breach in your system, such as an unprotected administration page coupled with a default user account that was not disabled after configuration. Alternatively, a lack of post-configuration restriction on error logs can lead to data vulnerabilities, such as stack information from your system landscape, resulting in information leakage.

Secure Configuration applies to your operating system, server landscape, databases, applications, APIs, and any other components you use. For relevant information on the security of your server and databases, see the *SAP Netweaver Guide* for security guidelines. The following section deals only with apps of the software component *ST* for SAP Solution Manager and its managed systems (`ST-PI, ST-BCO`).

Secure Configuration also means that after your configuration or update of configuration is completed, all relevant default accounts are checked for restrictions during operation. For more information, see the sections *Managing Authentication* and *Useful Tools* in this guide.

> **→ Recommendation**
>
> Quick recommendations checklist of the most common issues. In addition, read SAP's Security Recommendations: A Practical Guide:
>
> - Secure your network
> - Close ports

- Issue: Unencrypted communication between SAP solutions. We highly recommend using the TLS protocol
- Separate productive systems from development and test systems
- Configure and update securely
- Issue: Lack of an established patch process. We highly recommend regularly deploying available security patches
- Ensure that SAP components are not exposed to the internet.

6.2 Checking SAP Basis Infrastructure Security - Settings

Additional Documents

→ Recommendation

- Get familiar with the *White Paper on SAP Security Recommendations* for SAP NetWeaver systems: http://scn.sap.com/docs/DOC-17149
- Read the *SAP Netweaver Security Guide*: https://help.sap.com/saphelp_nw70ehp1/helpdata/en/3e/cdaccbedc411d3a6510000e835363f/frameset.htm to protect for instance functions like:
  - Gateway
  - Security Audit Log
  - RFCs between your Business Systems
  - and others

Read the System Security Advice from SAP NetWeaver: https://help.sap.com/saphelp_nw70ehp2/helpdata/en/cd/14c93ec2f7df6ae10000000a114084/frameset.htm

Secure Settings for SAP BASIS 7.40

Many mandatory security settings are SAP NetWeaver-specific, and although they are mentioned in transaction `SOLMAN_SETUP` in the SAP Solution Manager configuration, they are basic settings that have to be made when you set up the NetWeaver system itself, such as secure HTTP(s) https://help.sap.com/viewer/e73bba71770e4c0ca5fb2a3c17e8e229/7.4.17/en-US/5dcb88b33cad4f5da9dd77a3802e172f.html or specific system parameters.

6.3 Security Checks of SOLMAN_SETUP

SAP Solution Manager can become a target for attacks due to its importance as an administration platform. The transaction SOLMAN_SETUP_ADMIN contains specific guided procedures for protecting certain functions.

> **i Note**
>
> All authorization objects and respective roles in this section are security relevant.

SOLMAN_SETUP Administration

To manage the configuration completed in the SOLMAN_SETUP_ADMIN transaction, use the SOLMAN_SETUP transaction. It contains several views that are described in the user interface help texts.

> **i Note**
>
> The transaction SOLMAN_SETUP_ADMIN is not part of any work center. To access all views except *Log Archiving*, manually assign the following roles to a dedicated user:

You have to manually assign the following roles (which allow access to all views, except *Log Archiving*) to a dedicated user:

- SAP_SOLMAN_SETUP_ADMIN_ALL
- SAP_SOLMAN_SETUP_ADMIN_DIS

6.4 Using Authorizations to Restrict System (LMDB) Data

To protect your systems and all data connected to those systems (such as users, processes, or sensible data), we recommend restricting the access to your systems accordingly. All systems used by SAP Soltuion Manager are documented in the LMDB. Therefore, this store is protected by authorization objects for the LMDB. They are contained in roles SAP_SYSTEM_REPOSITORY_*** only, which are assigned to most of the template users that you can create in SOLMAN_SETUP and application SMUA.

> **i Note**
>
> For technical users, the objects are contained in the assigned user role for software component ST. If you follow a strict security protocol, we advise restricting the relevant authorization objects AI_LMDB_***. In this case, consider updating such a modified technical user role with the *Role Adjustment Tool*.

Roles SAP_SYSTEM_REPOSITORY_***

The roles SAP_SYSTEM_REPOSITORY_*** are the only roles assigned to dialog users containing the main system restricting authorization objects for the LMDB. Underneath, find a short overview on these roles and additional authorization objects, which are included in the roles.

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

Authorization Object AI_LMDB_OB

The object allows you to restrict systems and client information.

Using remote WBEM client

When using a remote WBEM client in the LMDB, authorization checks are also performed. WBEM standard defines a communication protocol that is implemented by both the SLD and LMDB. Any standard-compliant WBEM client implementation can be used to communicate with SLD or LMDB via intrinsic methods defined in the WBEM specification. As it is a generic access to LMDB objects, the user must have assigned the fields LMDB_MTYPE, LMDB_STYPE and LMDB_OBJID with an asterisks * in the user data. In this use case, for activities only using display functionality you can use activity display ACTVT 03 for further activities you have to use activity change ACTVT 02.

This implementation leads to an authorization trace information with a Return Code = 4 for the LMDB object. The trace information itself refers to ACTVT 02 as seemingly required for the application, even though you may

only require `ACTVT 03` display for your user. The information appears in the trace, but has no influence on the system's function.

LMDB and SLD Compatibility

> ⚠ Caution
>
> This authorization object allows you to restrict your users for systems to display, edit, and so on. If you restrict `AI_LMDB_OB`, do not allow System Landscape Directory (SLD) authorizations at the same time. Minimal SLD authorizations have complete read access. For more information, see the *SLD security guide*.

Authorization Object AI_LMDB_PS

This authorization object is relevant for the restriction of Product Systems in Release 7.1. It is only relevant in Release 7.2 for migration purposes. When you have finished migration, you can remove the object from the role.

Authorization Object AI_LMDB_TM

The authorization object `AI_LMDB_TM` protects the transport domain entry in transaction `LMDB`. The *Transport Management* provides a disjoint possibility to store information about systems. In many cases, the systems stored in the *Transport Management*LMDB Web User Interface allows users to access the information about the relationship between Transport Management System (TMS) information and technical system information. You can list all systems (system data) provided by TMS via the domain controller data supplier, and you can maintain (assign/de-assign) a link between TMS system information and technical system information. TMS information is not created or modified – only the links to LMDB information are displayed/created/deleted.

Authorization Object AI_LMDB_AD

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

Authorization Object AI_LMDB_RE

This authorization object is relevant for the remote access to the LMDB. It is contained only in role `SAP_SYSTEM_REPOSITORY_ALL`.

> → Recommendation
>
> If you do not require this object, we recommend removing it or setting it inactive in the role.

6.5 Updating Managed Systems in SOLMAN_SETUP

If there is 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.

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 SAP Solution Manager system. For more details, see the section on *Technical User SM_AMSC* in this guide.

In Case of SLD Changes

Use Case

If there are system updates in the System Landscape Directory (SLD), a configuration update job runs in the SAP Solution Manager with a dedicated technical user SM_AMSC.

6.6 Checking Security Flags for Relevant Activities in SOLMAN_SETUP

Activities that are security-critical are flagged as security-relevant and displayed in transaction SOLMAN_SETUP_ADMIN or in the *Security* app, which is part of the *SAP Solution Manager Administation* launchpad group.

> **i Note**
>
> SAP role SAP_SETUP_SECURITY_REC contains the object CRM_ORD_PR with full authorization.

6.7 Using System Recommendations Application

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

Prerequisites

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

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

Template End Users

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

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

Administrator User SYR_ADM_XXX (Help Text ID: TP_SYR_ADM)

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

Display User SYR_DIS_XXX (Help Text ID: TP_SYR_DIS)

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

Main Authorization Objects

S_TABU_DIS: Authorization Group for Tables

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

SM_FUNC: Restricting Tabs

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

> **i** Note

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

7 Securing Channels and Destinations

7.1 Vulnerability

One of the most prominent features of the SAP Solution Manager system as an administration platform is its tight integration with almost any system in your system landscape. This sets the SAP Solution Manager within your system landscape at high risk. It becomes a profitale target for any attack if successful, as it contains administrative data about your complete infrastructure and system landscape. The system connection is managed by RFC connections and HTTP connections. If intercepted, they can allow attackers to penetrate your system landscape easily. Therefore, a close protection of these connections is strongly recommended. The following section explains such measures in detail.

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

For **trusted RFCs**, see the section Overview: Communication Channels and SAP Solution Manager Technical Users per scenario.

7.3 Secure RFCs with Authorizations

Overview

To protect RFCs with authorization restrictions, check the following topics:

- Securing Trusted RFCs by correctly assigning and maintaining authorization objects `S_RFC_TT`, `S_RFCACL`, and `S_ICF`.
- Restricting access to transaction `SM59`, which is contained in role `SAP_SM_RFC_ADMIN`.
- Securing RFCs by restricting authorization objects `S_RFC, S_RFC_ADM` as well as profile parameters.

For additional information, also see https://help.sap.com/saphelp_nw70ehp1/helpdata/en/57/e100438a189c45b6290c2a1d0614bc/frameset.htm

The Trusted - Trusting Relationship (RFC)

The Trusted - Trusting RFC destination has the *Current User* settings, and *Trust Relationship Yes* in transaction SM59.

> → Recommendation
>
> A trusted relationship in SAP Solution Manager should only be one-sided. We recommend, you only create a trusted relationship between the managed system to SAP Solution Manager, but not SAP Solution Manager to the managed systems. This means that you should only allow trusted calls from SAP Solution Manager to a managed system but not vice versa.

Authorization errors in the use of an RFC destination flagged as a *Trusted System* cause the following message to be sent: `No Authorization to logon as Trusted System (Trusted RC = #)`.

Every authorization error when using an RFC destination flagged as a *Trusted System* is a RABAX (ABAP exception). The RABAX contains detailed error information. To analyze the error:

1. Choose transaction ST22 and the selection period.
2. Choose the entry under the user SAPSYS and the program name `CALL_FUNCTION_SYSCALL_ONLY`. The paragraph *Troubleshooting*, contains the information necessary to correct the error.

Return Code

Return Code	Explanation	To Do
0	Invalid logon data (user and client) for the trusting system	Create a corresponding user in the client system for the user in the server system (trusting system).
1	The calling system is not a trusted system, or the system security ID is invalid.	Create the trusted RFC connection again.
2	The user has no authorization containing the authorization object S_RFCACL, or is logged on as the protected user DDIC or SAP*.	Give the user the authorization, or do not use the protected users DDIC or SAP* (see: profile parameter and value: `login/no_automatic_user_sapstar = 0`)
3	The timestamp of the logon data is invalid. Check the system time in the client and in the server, and the validity date of the logon data.	Synchronize the system times

Creating a Trusted Relationship - Authorization Object S_RFC_TT

Authorization object S_RFC_TT is only required for creating trusted relationships for managed systems in transaction SMT1, as of SAP_BASIS_7.02 SP03 and higher, see SAP Note 1734607.

Securing a Permanent Trusted Relationship - Authorization Object S_RFCACL

If you use an already existing trusted RFC connection, you need to have the authorization object S_RFCACL in the SAP Solution Manager system and in the managed system assigned to your user. This authorization object **is not contained in profile** SAP_ALL due to its highly critical nature.

Usage in Transaction SOLMAN_SETUP

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

→ Recommendation

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

How to Maintain S_RFCACL

→ Recommendation

How to maintain the object:

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

  i Note

  If you use other remote scenarios that are based on a Trust relationship, then it might be the case that you activate the transaction flag in transaction SMT1, for instance for the GRC FireFighter application, which requires you to activate this flag. In this case, you should change the value for field RFC_TCODE from `' '` to *. Despite the fact that we do not recommend that you install the central GRC on the SAP Solution Manager system, you should be aware that this requirement is relevant if you install the central GRC elsewhere but use GRC FireFighter in local mode.
- `RFC_INFO : <Installation Number of the Solution Manager>`
- `ACTVT : 16`

How to Maintain the Authorization Object for SAP Fiori Apps

> ⚠ Caution
>
> Specifically for all SAP Fiori apps, make sure you maintain the authorization object with only the required values for the user and the system IDs in question. Do not use any generic values (such as '*') for `RFC_SYSID, RFC_CLIENT`, and `RFC_USER`. For more information, see SAP Note 128447.

Securing a Temporary Trusted Relationship - Authorization Object S_ICF

Use authorization object `S_ICF` for a tempory Trusted RFC.

Authorization Roles SAP_SM_RFC_*** for Dialog Users

RFC connections are created and maintained in transaction `SM59`. When you create RFCs using transaction `SOLMAN_SETUP`, the system references transaction `SM59`. Roles `SAP_SM_RFC_***` contain all relevant authorization objects for transaction `SM59`, such as `S_RFC***`. For technical users, some roles also contain `S_RFC***` authorizations, but maintained according to the task of the respective technical user.

RFC Maintenance Role SAP_SM_RFC_ADMIN

This role contains authorizations for creating RFC connections using transaction `SM59`. It is therefore considered highly security-relevant. By default, the role is assigned to user `SOLMAN_ADMIN`.

> → Recommendation
>
> We recommend that you remove this role from the user after finishing the basic configuration from the SAP Solution Manager system landscape, managed systems, and remote BW system.

Role	Included Authorization Objects
SAP_SM_RFC_*	• S_RFC_ADM • S_ADMI_FCD • S_RFC_TT manually added due to its criticality Additional authorization objects S_TCODE for transaction SM59 and S_SERVICE

Securing General RFC - Connections

A remote function call (`RFC`) calls a function module in another system. Due to the nature of SAP Solution Manager, the number of `RFC` calls to and from other systems is high. Therefore, a high number of function modules are affected.

In the context of security of RFC calls, consider the following three areas:

- *Authentification*
  Incoming RFC connections must authenticate in the system. For instance, the READ RFC call is an incoming RFC call in the managed system. Therefore, a user must be present in the managed system to authenticate the RFC call. Here, user of type *system* is used. From the SAP Solution Manager system's point of view, the READ RFC connection is an outgoing RFC. Outgoing RFC connections are maintained in transaction SM59 in the present system. In the RFC itself, the user is maintained. During the Solution Manager setup of managed systems, most RFCs are automatically created, as well as the user in the managed system, and the assignment of according authorizations for this user. The RFCs are added automatically to transaction SM59. For their evaluation and monitoring, RFC traces (transaction ST05) can be used as well as the Security Audit Log.
- *System Profile Parameter*
  The RFC authorization check can be activated / deactivated with the system profile parameter auth/rfc_authority_check. This parameter must not be set to the value '0'. If you set the value to = 9, the system only accepts the values of FUNC (function module) in the authorization object. Make sure, that all roles do only contain FUNC (except for function group SRFC). For more information, see SAP Note 931252.
- *Authorization Objects S_RFC and S_RFC_ADM*
  The authorization object S_RFC is used to check, whether the called RFC user is authorized to execute RFC function modules. The authorization object is delivered with dedicated values for function modules.

  > **Example**
  >
  > The SYST function group is needed to call SM59. If it is missing, the *remote logon* in transaction SM59 causes the RFC_NO_AUTHORITY ABAP runtime error in the target system.

  For S_RFC value changes for the technical RFC - users for READ and TMW RFC connection, see SAP Note 1572183.
  Since SAP_BASIS 7.02, you can maintain the authorization object for certain function groups but also function modules. In SAP Solution Manager, you may find the authorization object maintained according to this differentiation.
  Authorization object S_RFC can be traced with audit log trace in transactions **SM19** and **SM20**. To protect the deletion of traces, maintain field *ACTVT* with value **36** of authorization object S_RFC_ADM.

  > **Caution**
  >
  > Currently, RFC function modules in function group /SSF/INTRFC have no own authorization checks.

> **Note**
>
> For more information on RFCs, see http://scn.sap.com/docs/DOC-60425, SAP Note 14113011 and SAP Note 2008727. For more information on how to analyze and secure RFCs, see https://wiki.scn.sap.com/wiki/display/Snippets/Show+RFC+Workload+Statistic+to+build+authorizations+for+authorization+object+S_RFC.

S_RFC and Additional S_TABU_NAM

In case a generic function module is called, this function module is protected by the additional authorization object S_TABU_NAM. For more information on specific table protection, see section *Tighten Table Read and Write Access/Table Protection*.

Authorization Object S_DEV_REMO

In managed systems as of `SAP_BASIS 8.03` and higher, function group `RFC1` is additionally protected by authorization object `S_DEV_REMO`. Therefore, all relevant roles for the setup of managed systems using transaction `SOLMAN_SETUP` include authorization object `S_DEV_REMO`.

7.4 SAP's Support Backbone Destinations

To securely run SAP's support backbone communication, ensure that you have done the following:

- activate a new technical communication user for the destinations
- establish an HTTPS communication channel
- enable server certificates to use SSL
- check the correct kernel version. You require kernel release `<742`, which allows for remote HTTPS connection
- configure `STC01` and `STC02`

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.

Technical Communication User

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.

Specific Relevant Authorization Objects

Authorization Object S_LOG_COM

S_LOG_COM is required to run the TLS version check for 1.1 in the task list SAP_SUPPORT_HUB_CONFIG. With this authorization check, the system checks whether or not the user can execute the external command in a background job. Role SAP_SETUP_SYSTEM_PREP contain the correct maintenance for the object, which should not be changed:

- COMMAND: SAPGENPSE
- OPSYSTEM: ANYOS
- HOST: *

Connected authorization objects:

- S_RZL_ADM with the possibility to create
- S_ADMI_FCD with value PADM

Transaction S_TCODE: SBGRFCCONF

S_TCODE for transaction SBGRFCCONF is required to create the supervisor RFC destination for the SOAP runtime framework. Attached authorization object is S_BGRFC

RFC Relevant Authorizations

- S_RFC_ADM for RFCs SAPOSS, SAPSNOTE with ACTVT 01 (generate), 02 (change), 03 (display) for destinations ABAP (03) as well as L (Reference Entry) and T (Start External Program) as RFCTYPE
- S_RFC with FUGR SYST

Authorization Object S_DATASET

S_DATASET with program SAPLSSFM is required.

Authoriaztion Object S_TC

S_TC with ACTVT 03, 16 is required to execute the task list specifically for RFC SAP_SUPPORT_HUB_.

7.5 SNC Check

Use report RSRFCCHK to analyze whether RFC destinations are with or without SNC. Check existing entries in table USRACL.

> ⚠ Caution
>
> For SNC for Java check SAP Note 2895836.

SAP Solution Manager

SAP solution Manager uses SNC protection.

Webadmin JCo Destination

Since SP09 Webadmin JCo destination on JCo 3.0 runs via SNC.

Wily Introscope

For Wily Introscope see SAP Notes:

- 1690662 - Option: Blocking unencrypted SAPGUI/RFC connections
- 1701870 - RFC client communication supporting SNC without SSO

8 Securing Access to Applications

8.1 Vulnerability

If applications or APIs do not verify the user authorized for a target source or if the authorized user has far too many priviledges, there is a security vulnerability in your system landscape. This can result in the possibility of the unintended user to manipulate your system and its parameters in a way which is not registered by you. A careful consideration of access control is necessary from your side to effectively protect your business.

Access Control to SAP apps is given by the assignment of so-called start authorization objects. For SAP Solution Manager, they are assigned for all OData Services (authorization object `S_SERVICE`), WebDynpro apps (authorization object `S_START`), and transactions (`S_TCODE`). The automatic assignment of these objects is managed within the menu tab of an SAP role due to assignment of these applications there. These menu entries reference attached authorization objects, which belong to the app as a minimum protection. This principle allows you to remove app access and referenced objects or add new apps with an automatic access control authorization. For more information on this concept, see the *Authorization Concept Guide for SAP Solution Manager*.

> → Recommendation
>
> We strongly recommend that you add newly created apps only in the menu tab of a role to automatically have access protection in place. Avoid directly adding field values to authorization objects `S_TCODE, S_START, S_SERVICE`.

Especially administration users are assigned security-critical authorizations, which can lead to escalation of priviledge if a vulnerability occurs. Any administrative application that is accessible to a non-administration user is exploitable. Considering that SAP Solution Manager is also a platform for adminnistrators, this is especially applicable.

> → Recommendation
>
> We strongly recommend that you implement a four-eye principle for administrative access to your system as well as a careful implementation of security-critical authorization objects and their assignment to users. This applies especially to critical authorization combinations. Some of these objects and their critical combinations are outlined in this section. In section *Useful Tools*, you can find more information on how to optimize and monitor these access restrictions.

8.2 Restrict Access to Transaction SOLMAN_SETUP

> → Recommendation
>
> For secure configuration, see the *Secure Configuration Guide*.

Access Protection with Authorization Object SM_SETUP

Authorization object `SM_SETUP` allows you to protect SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`). It controls if a user can access SAP Solution Manager Configuration. You can restrict access on the following levels:

- Activities

  > **i Note**
  >
  > `ACTVT 02` (edit) is required for both accessing the transaction in change mode and being able to set the lock for the guided procedure. If edit authorization is not assigned, the *LOCK* button is not displayed. Once a guided procedure has been locked, a configuration user can unlock it by using the *Locked Guided Procedures* function in transaction `SOLMAN_SETUP_ADMIN`.

- Scenarios/Procedures
  Every configuration user role `SAP_<scenario>_CONF***` contains the object with authorization for the relevant guided procedure.

  > **i Note**
  >
  > Some roles contain access authorization for other guided procedures for specific configuration purposes. Consider these extra access authorizations carefully. If it is not required for your business case, deactivate the respective authorization or remove it from the role completely. In general, the scenario ID for the *Overview* of transaction `SOLMAN_SETUP` is assigned in every configuration role by default.

  > **Example**
  >
  > `SAP_CHARM_CONFIG` role contains access authorization for Change Request Management procedures as well as access for specific steps in Job Scheduling Management with read access or ITPPM.

- Steps within a procedure

- If you allow display authorization (`ACTVT 03`) for any scenario, the user is not allowed to edit any steps within the procedure in question.
- If your security policy only allows certain users to maintain a specific set of steps within the procedures, you can restrict on procedure and step level.
- If a user does not have this authorization object assigned but still has access to the transaction via authorization object `S_TCODE` using the launchpad group for SAP Solution Manager Configuration (also using `WDA`: `AGS_WORKCENTER`), the system does not display data.

Restricting Launchpad Group Navigation View Panel - Authorization Object: SM_WC_VIEW

> **i Note**
>
> See SAP Note 2211213 - How to maintain the authorization for `SM_WC_VIEW` in a `PFCG` role.

All launchpad group home page apps are based on ABAP Web Dynpro. *Launchpad Group Views*, any sub-views, and the *Common Task* level can be restricted by the authorization object `SM_WC_VIEW`. This authorization object is contained in the specific core role for the application. If the authorization object is not granted, the according view, sub-view or common task is hidden on the user interface by the system.

You may need to adapt this authorization object, for example, in scenarios in which the user can select copied transaction types in sub-views or views, such as *ITSM Incident Management* or *Change Request Management*. To adapt this authorization object, proceed as follows:

1. Choose transaction `SM30`.
2. Choose table `AGS_WORK_VIEW`.
3. Copy the according entry for the transaction type.
4. Adapt the copied entry.

Table `AGS_WORK_VIEW` is used as the value help for the authorization object. You can add views and tasks to your launchpad groups and control them using this authorization object. Activate the BAdI implementation in the IMG for SAP Solution Manager in transaction `SPRO`.

The BAdI implementation fills the value help table for the authorization object. To use the trace, you must activate the BAdI and go to the launchpad group. The system enters the launchpad group IDs in the value help table `AGS_WORK_VIEW`. You can then adjust the authorization object in the role. In summary:

1. Activate BAdI `AGS_WORK_AUTH_SM_WC_VIEW` in enhancement `EHN_AGS_WORK_AUTH_UI` (activate via transaction `SOLMAN_SETUP`).
2. Activate BAdI `AGS_WORK_AUTH_F4_TRACE` in enhancement `EHN_AGS_WORK_AUTH_TRACE` (activate via transaction `SPRO`).
3. Go to transaction `PFCG` and call role the according core role.
4. Change the values in the authorization object, for example only add the views that you want to see, leave out those you do not want to see.
5. Generate the profile, and assign the role to the user.

i Note

Authorization object `SM_WC_VIEW` is always checked. If the `SM_WC_VIEW` check is successful, the system checks the authorizations for the specific business function required to use the Web Dynpro application, Web Dynpro component or transaction. The additional UI authorization object makes sure that the UI is controlled even when an app does not require specific application-relevant authorization restrictions. In addition, this approach has the advantage that you can use the authorization object to remove, for example, common tasks from a work center, even if the user is technically authorized to use such tasks.

Example

In the *Incident Management* launchpad group, the common task *Manage Substitutes* is not displayed by the system in the following cases:

- If authorization object `SM_WC_VIEW` with the according entry is not granted to the user, but the application-specific authorizations are granted. This may be the case if you only want users to maintain substitutes in transaction `BP` and not in the work center.
- If authorization object `SM_WC_VIEW` is granted, but the application specific authorization object `B_BUPR_BZT` with value `BUR013` is not granted to specific users only.

The common task is only displayed by the system if both authorization objects with the according values are granted to the user.

Adaptation of Related Links in the Navigation Panel

We recommend that you use the delivered navigation roles. You can also define them for your own purposes. This means that you can add new folders with apps in the *Related Links* area in the work center navigation panel. You can also delete defined folders. You cannot change entries in the launchpad group areas *Common Tasks* or *Navigation Panel Views* in the role. You can adapt these areas using authorization object `SM_WC_VIEW`.

8.3 Secure Single Applications in Intranet/Internet

ABAP Web Dynpro Apps and Components

ABAP Web Dynpro is used for most applications in SAP Solution Manager.

Web Dynpro App Versus Web Dynpro Component

Any Web Dynpro app is at least restricted by its start authorization object (`S_START`), and the app itself must be activated as a service in transaction `SICF`. In contrast, Web Dynpro components have no start authorization and must not be active in transaction `SICF`. There is no specific concept as to whether a Web Dynpro app or a Web Dynpro component is embedded into the launchpad groups.

> **i Note**
>
> Transaction `SICF` allows for maintenance of ICF settings. We recommend that you restrict authorization object `S_ICF_ADM` carefully and only assign it to specified users in the system. In addition, avoid assigning authorization object `S_SEC_SESS` with `ACTVT 63` or `HI` in combination with transaction `SICF_SESSION` as it allows activation or deactivation of HTTP Security Session Management.

> **⚠ Caution**
>
> If you need to call any app that is embedded in any work center, to be called standalone, you need to check whether it is a Web Dynpro app or a Web Dynpro component. If it is a Web Dynpro component, check to which app it belongs or create your own app for it and use this app as a standalone app.

> **i Note**
>
> If an embedded web page is a Web Dynpro component, they shouldn't be activated using transaction `SICF`. If you want to display such an app separately outside the work center framework, this can lead to security leaks as some Web Dynpro components might not have separate authorization object checks.

Web Dynpro App - Start Authorization Object S_START

Before SAP Basis Release 7.4, the maintenance of authorization objects for ABAP Web Dynpro in transaction `PFCG` was mainly done manually, due to former restrictions for this type of technology in transaction `PFCG`. The start transaction was authorization object `S_SERVICE`. With SAP Basis Release 7.4, a specific start transaction

authorization object is introduced: S_START. This authorization object is similar to S_TCODE. S_TCODE is the start authorization for transactions. Therefore, in SAP Solution Manager Release 7.4, authorization object S_SERVICE is substituted by authorization object S_START as ABAP Web Dynpro start authorization. For more information, see section *Application Start Authorization Objects*.

> ### Example
>
> For User Experience Monitoring (UXMon), the core single role is SAP_SM_EEM_*.
>
> The role contains all relevant application IDs for the relevant UXMon user role. However, it does not contain the application ID for the dashboard application for UXMon. This ID is included in the core authorization role dashboards for UXMon: SAP_SM_DASHBOARDS_DISP_EEM.

> ### Note
>
> All delivered roles are updated in this regard from release 7.1 to release 7.2.

Restricting Link and Button Access - URL Framework Authorization Objects SM_WD_COMP and SM_APP_ID

In a Web Dynpro app, you can call other applications via a user link. This user link is protected by authorization object SM_WD_COMP. Any new application can be called either from the web page itself or in a separate window. This is protected by authorization object SM_APP_ID. Both authorization objects are used in the following launchpad groups in SAP Solution Manager:

- Technical Administration
- Technical Monitoring
- SAP Solution Manager Configuration
- Solution Manager Administration
- Root Cause Analysis
- Data Volume Management

Both authorization objects restrict views, subviews, URL links, transactions, or buttons leading to separate screens. For all roles delivered as default template roles by SAP, these objects are already maintained according to the user definition by SAP. The authorization objects are included in the applicable core authorization role for the application.

> ### Caution
>
> The use of these two user interface authorizations can lead to misleading ST01 or STAUTHTRACE authorization traces. If you trace one application due to authorization error messages, the analysis of the trace displays all authority checks executed by the system. This also includes user interface authorizations. If there are restrictions to user interfaces by the above-mentioned objects, any missing authorizations for them are marked with return code (RC) = 4. If you are not tracing for the user interface element, you can ignore this entry. We recommend that you do not change the delivered SAP roles.

URL Framework

You can adapt the authorization objects and therefore the user interface for all scenarios of these work centers. To do so, you need to apply the URL framework. Here, you can find the according values for the application you want to restrict. Proceed as follows:

1. Call the URL for service: sap/bc/webdynpro/sap/urlapi_app_manager.

2. Open the links for the work center you want to adapt.
3. Check the application view. The authorization object is displayed on the same page.

Restricting Visibility of Tabs or Logon Screen in the Launchpad Group User Interface

You can restrict individual tabs in any of the user interfaces in the launchpad groups by using general Web Dynpro functionality. For an individual user, proceed as follows:

1. To indicate which tab should be hidden or restricted, bring the cursor to the fields of the tab.
2. Select the menu of options.
3. Choose *More*, and *Hide Elements*. The system hides the according tab on the UI. For more information about restricting a tab system-wide for all users, see http://help.sap.com/saphelp_nw70/helpdata/en/46/98ce61f37d19ace10000000a11466f/frameset.htm.

> **i** Note
>
> If you want to customize your launchpad groups for branding or adapting the Web Dynpro logon screen, see SAP Note 1160651.

CRM WebClient UI Authorization

Authorization Object UIU_COMP

BSP-based technology is used within the WebClient UI, which is called from the work centers, ABAP Web Dynpro apps for ITSM Incident Management, and Change Management apps. Similar to the launchpad group navigation role concept, a CRM navigation role is delivered with the according authorization roles for the authorizations for the user interface. For more information, see section *Using SAP Solution Manager with CRM*.

The authorization object for the user interface for CRM is `UIU_COMP`. It restricts authorizations for CRM components and its used applications. The authorization object controls which components can be called by the user.

SAP delivers specific roles for this authorization object, which are again contained in the respective roles. All roles for the `UIU_COMP` authorization object have the naming convention `SAP_SM_CRM_UIU_*`. They are layered according to the user definition they are defined for. They are additive. For example, if you use the administrator role for Incident Management, you find two `UIU_COMP` roles included, as `UIU_COMP` authorizations in both roles add up. The *Incident Management* role for the processor includes only one `UIU_COMP` role. An `ST01` or `STAUTHTRACE` trace always displays all possible values for this authorization object. Only the objects included in the above-mentioned roles are relevant for SAP Solution Manager apps. For example, a trace may result in about 500 checks for the authorization object `UIU_COMP` of which only about 20 checks are relevant for SAP Solution Manager use. We recommend not to change the delivered SAP roles.

> **→** Recommendation
>
> We recommend not to change the delivered SAP roles.

Authorization Object C_LL_TGT

Authorization object `C_LL_TGT` is required within the WebClient UI for links to ITSM Reporting and HTML mail formats.

Authorization Object S_TCODE for Transaction

To run any transaction in any SAP system, authorization object `S_TCODE` is called by the system and must be assigned to the user running the transaction.

> ⚠ Caution
>
> `S_TCODE` should only contain the transaction codes that the user is allowed to run.

Authorization Object S_START for Web Dynpro Application

Web Dynpro apps have start authorization object `S_START`. `S_START` is delivered with SAP Basis Release 7.40. This authorization object substitutes authorization object `S_SERVICE` as the start authorization object.

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

Authorization Object S_SERVICE for OData Services

OData Services have start authorization object `S_SERVICE`.

> ℹ Note
>
> Note that external services are also protected by authorization object `S_SERVICE`. The service ID is added manually to the respective roles.

8.4 Guided Procedure Framework

If you want to customize your own guided procedure, assign `SAP_SM_GP_ADMIN`. This role contains the critical authorization object `S_SYS_RWBO` with `ACTVT 01, 02, 03`, and critical authorization object `S_TRANSPRT` with `ACTVT 01, 02, 03, 07` for workbench requests and Customizing requests. If you do not want to allow the user to create, change, delete or display transports, then you need to **deactivate** these objects. Additionally, critical authorization object `S_CTS_ADMI` with value `TABL` is included in the role. It should not be assigned in combination with transaction codes `SE80` or `STMS`, as it allows super user authorizations in ABAP development environment and transport environment.

If you need to maintain SAPscript documentation using transaction SE61, you need to assign the following authorization objects to the role:

- S_TCODE with value SE61
- S_DEVELOP with ACTVT 03 (display) for all object types

8.5 Protecting ABAP Development Environment

Authorization Object S_DEVELOP

S_DEVELOP is the general authorization object for ABAP Workbench objects. Use it to grant access authorizations for all ABAP Workbench components, which include the following:

- ABAP development tools
- ABAP Dictionary and Data Modeler
- Screen Painter and Menu Painter
- Function Builder
- Repository Browser and Info System
- SAP SmartForm

> → Recommendation
>
> From a production perspective, it is considered critical if authorization object S_DEVELOP is assigned to users. In general, authorization object S_DEVELOP with more than display access (ACTVT 03) is not required by any user in production.

Critical Authorization Combinations with S_DEVELOP

The combination of field values for S_DEVELOP is critical:

- The object types STRU (structure), TABL (table) , and ACTVT values 07, 40, 41, 42 for S_TCODE SE11 allow maintenance of data dictionary objects.
- The object type FUGR (function group) with ACTVT 16 for S_TCODE SE37 allows RFC via function calls.
- The object types DEBUG (debugging), PROG (program) with ACTVT value 02, and S_PROGRAM with ACTVT value SUBMIT for S_TCODE SE38 allow replacing and debugging of reports. Note that S_TCODE SE38 should never be granted to general end users. In combination with S_TCODE SE80, it allows programming (active in role SAP_DVM_SERVICE (needs access programming tools), see *Application-Specific Guide for DVM*)
- The object type TABLE (table) with ACTVT value 02, and S_TABU_DIS with ACTVT value 02 for S_TCODE SE16, SE16N allows replacing and debugging of tables.

- The object type TRAN (table) with ACTVT value 01, 02 for S_TCODE SE93 allows maintenance of transaction codes.

S_DEVELOP in Transaction SOLMAN_SETUP

The authorization object is assigned for maintaining transaction SNOTE during the SAP Solution Manager basic setup to the SOLMAN_ADMIN user in role SAP_SETUP_BASIC_S_DEVELOP.

> → Recommendation
>
> After implementing all required SAP Notes into the system, you can set the according authorization object to inactive. Documentation is provided in the guided procedure for the automated setup.

8.6 Protecting Functions and Tables

Protecting Functions

Protecting function groups and subsequently function modules is part of protecting your application. In general, for SAP Solution Manager roles, SAP limits authorizations to only the nesessary function modules for the corresponding function in most cases. This is done via authorization object S_RFC. If your security guidelines do not allow for specific function modules, such as RFC_ABAP_INSTALL_AND_RUN (ABAP source code via RFC install and execute) which belongs to function group SUTL, you can remove the corresponding function module from the roles. However, keep in mind that this function module might be mandatory to run a specific function.

> ℹ Note
>
> When you run an authorization trace for S_RFC, the trace shows you both the function groups and the relevant function module of this group. We recommend that you always limit authorizations to function modules instead of function groups.

Protecting Tables

Protecting groups of tables and individual tables is part of protecting your application. For more information, see the section *Tighten Table Read and Write Access* in this guide. As with functions, we recommend that you protect individual tables, such as DBTABLOG, using authorization object S_TABU_NAM than table groups, such as SA, using authorization object S_TABU_DIS.

9 Securing Data, Data Flow, and Processes

9.1 Vulnerability

Proper assignment of authorization checks for apps and APIs is essential to prevent potential security issues in SAP systems. Restrict dialog users' access to only necessary functions and apps to prevent potential security issues. Customize authorization roles provided by SAP to match the specific needs of your organization.

Any dialog user in your system must be restricted to only to the necessary functions and apps for their task. Even read access to apps that are not related to their task can pose a risk as an attacker may use that information to gain access to system. Avoid adding authorizations to a dialog user without understanding the potential consequences.

Authorizations provided in roles by SAP are designed for the SAP standard process, but may not match the specific needs of your company. Customize these roles to match your company's processes and avoid any excess access that could be exploited by attackers. If you use authorizations in your systems which are not restricting access to your system and processes in a controlled and specific manner, this can be easily exploited and may lead to escalation of priviledge and damage to your data.

> → Recommendation
>
> We strongly recommend that you adjust any authorization objects that are delivered with generic field values. Generic field values are all fields in authorization objects that can not be predetermined by SAP.

Uploaded files pose a security threat as they may contain malicious code that can damage your system if not detected. This could lead to system shutdown or takeover, or other types of attacks depending on the code and the attacker's intent.

> → Recommendation
>
> To keep your system safe, regularly check for viruses and limit who can upload files.

9.2 Background Jobs

Background Job Authorizations S_BTCH_***

Batch job scheduling and performing are protected by background job authorizations starting with `S_BTCH_***`.

→ Recommendation

Authorization object S_BTCH_NAM determines the authorized users for running batch jobs. In SAP Solution Manager standard roles, this object is delivered with no specific user maintained. We recommend that you maintain this object for any technical user required, for example SOLMAN_BTC. A combination of transaction SM36, S_BTCH_NAM with full authorization and S_BTCH_JOB with RELE (release) authorization is critical.

Restricting Authorizations of SOLMAN_BTC

For Background Jobs

Technical user SOLMAN_BTC runs all relevant jobs for the basic configuration, as listed in SAP Solution Manager Configuration in the *Basic Configuration* scenario, *Schedule Jobs* step. These background jobs can also be found in SAP Note 894279. If you want to run a job that is not in the list, you have to use a different user or add additional authorizations. Trace the authorization for this job and add it to SOLMAN_BTC at your own risk. We recommend having a separate role and check for critical authorization combinations.

→ Recommendation

In a highly secure environment, we strongly advise creating a single role from scratch for any job or group of similar jobs, using an authorization trace.

Troubleshooting Technical User SOLMAN_BTC in Rapid Content Delivery

The report is protected by authorization object S_PROGRAM with program group RCSU_PREREQ_CHECK. The execution of the report program RCSU_PREREQ_CHECK can be checked in the log in transaction SLG1 using object **RCD** and subobject **TROUBLESHOOT**.

SDCCN - EWA Background User in Managed Systems

When it comes to managing all background jobs related to transaction SDCCN, it is important to use a dedicated technical user. Often, the administrator user for the managed system may have more authorizations than required, which can pose a security risk. To mitigate this, we recommend that you activate SDCCN using a separate technical user specifically for background jobs. This enables you to secure the configuration user SOLMAN_ADMIN after the configuration process is completed, by disabling the user or removing unnecessary authorizations.

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

→ Recommendation

We strongly recommend that you change the user running the jobs to a technical user type, with only specified roles. The specific role that should be assigned is SAP_SDCCN_ALL, which contains

authorizations S_SDCC***. If you choose to run this job with a general batch user for your managed system, either add the role SAP_SDCCN_ALL to your user or the respective authorization objects.

9.3 Securing Attachments, Uploads, and Download

Upload and Download of Files in Various Applications

Uploading and downloading files in various apps can pose a security risk to your system. Unintended data may be downloaded and distributed, or uploaded documents may contain malicious content that can disrupt your business. Both can damage your system and business reputation.

→ Recommendation

We strongly recommend installing a virus scanner for any uploaded data. In addition, make sure that any download possibility is controlled by security measures, such as dedicated users and dedicated authorizations.

Set Size Limits for File Uploads

You can limit the size of uploaded files to protect the application server from a Denial of Service (DOS) attack from large requests. This restriction is set in the Internet Communication Manager (ICM) and applies to all file uploads via the HTTP protocol. Use parameter *icm/HTTP/max_request_size_KB* with an integer value for the maximum file size in kilobytes. If the content length of the request exceeds the specified value of the parameter, the system does not pass the request to the application server and sends an error message to the application frontend.

Download Completion Report of Configuration Process in SOLMAN_SETUP

In SAP Solution Manager, serveral apps allow downloading data and uploading attachments. These actions are protected by authorization activities, such as UPLOAD or DOWNLOAD.

i Note

Due to their criticality, the auhorization activities for uploading and downloading files ACTVT are shipped in an inactive status. Activate these authorization activities to allow users to upload or download files within an app.

Example

Authorization Object SM_SETUP: This authorization allows access to the transaction SOLMAN_SETUP and various activities within the transaction. To enable downloading of completed configuration procedure activities, assign ACTVT 61 (export) to the appropriate user.

Upload of Images in Comments to SOLMAN_SETUP

In the SOLMAN_SETUP comments area for each activity, it is possible to upload images. Uploading images in the SOLMAN_SETUP comments area is protected by the SM_UPLOAD authorization object and its UL activity.

This authorization is included in the SAP_SETUP_BASIC role, as well as in the SAP_SM_GP_ADMIN, and SAP_SM_GP_EXE roles for the GP framework, but is inactive by default.

Virus Scan for Applications and SAP Fiori Apps

In general, any upload functionality in SAP Solution Manager applications is integrated into the relevant application and therefore indirectly protected by the application-specific authorization object. In addition, upload files should always be scanned by a virus scanner.

> → Recommendation
>
> We recommend that you use ABAP Virus Scanning Interface (VSI) to scan attachments for viruses. ConfigureVSI to exclude both executable (.exe) and HTML files from being uploaded. If the VSI is enabled but there is no third-party virus scan in place, the system does not upload any attachments by default. If you do not set the VSI to be active, the system allows you to upload attachments. As this is highly unsafe, we strongly recommend that you use a virus scan product to upload attachments. Check: https://help.sap.com/saphelp_nw70ehp2/helpdata/en/cd/14c93ec2f7df6ae10000000a114084/frameset.htm

Attackers can abuse a file upload to modify the displayed app content or to obtain authentication information from a legitimate user. Usually, virus scanners are not able to detect files designed for this type 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 how of the virus scanner behaves when default virus scanning profiles are enabled, see SAP Note 1693981 (Unauthorized modification of displayed content).

All CRM apps use the following default VSI profiles:

- /SCET/GUI_UPLOAD
- /SIHTTP/HTTP_UPLOAD

/SCMS/KPRO_CREATE, specifically for incidents created via an external interface. In addition, attachments are scanned using the default Knowledge Warehouse profile.

> i Note
>
> Check the basic configuration of the virus scanner settings, either in transaction SOLMAN_SETUP or in the *Security* app, which is part of the *SAP Solution Manager Administration*.

The thread dump analyzer is implemented using the Java Web Dynpro component FileUpload. The Web Dynpro component uses the virus scan profile webdynpro_FileUpload.

Application Log Access for SOLMAN_SETUP

Each app in SAP Solution Manager has a log option. For most apps, the log information can be retrieved by using transaction SLG1 together with the relevant object and subobject for the application. This information is provided in the *Application - Specific Security Guide* by scenario and in the *Application Operations Guide*. From a security perspective, log file information is security-critical because it contains valuable information about your system, your users, performance, and more.

SAP Panks (SAP Note Search within SOLMAN_SETUP Log)

Within the log for each SOLMAN_SETUP step, you have the possibility to search for SAP Notes that are related to any errors that occur in the configuration step. The PANKS search is connected to the SAP support backbone using RFC SAPOSS.

Log Upload and Download in SOLMAN_SETUP

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 related data is 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* launchpad group. Access is granted by the authorization object SM_SETUP – 61 export.

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).

Audit Log

See *Auditing and Logging* in the SAP Support Portal under http://help.sap.com *Search Documentation* . Search for *Auditing and Logging.*. Check:

- https://help.sap.com/saphelp_nw70ehp2/helpdata/en/c7/69bcb7f36611d3a6510000e835363f/frameset.htm
- SAP Note 2080378
- SAP Note 536404

9.4 Processes and Document Management

Process Documentation

Role	Included Authorization Objects
SAP_SM_SL_DISPLAY	The role contains all relevant authorizations for process documentation in display mode.

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

Authorization Objects that were relevant in Release 7.1

Due to the major change in *Process Documentation* architecture, most formerly relevant authorization objects are now obsolete. They are set into authorization class AAAA as obsolete. In case you need to check solutions of Release 7.1, roles SAP_SOLPRO_OLD and SAP_SOLPRO_DISP_OLD contain these authorization objects.

Authorization Object SM_SDOC

This object is relevant for restricting processes/solutions.

Authorization Object SM_SDOC_ADM

This object restricts solutions on the administrative level.

Authorization Object SM_GAL_GO

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

Document Management and Digital Signature

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

Obsolete Authorization Objects

Two new authorization objects are shipped with Release 7.2. They replace authorization objects S_IWB, S_IWB_ADM, and S_IWB_ATTR. Both objects are shipped with software component SAP_BASIS, and are contained in authorization class SMD.

New Authorization Object: S_SMDATT

This object restricts the use of a document depending on the allowed document attributes.

New Authorization Object: S_SMDDOC

This object restricts the activities that can be done on a document.

> **i Note**
>
> - Activity `60` (import) is shipped by default in role `SAP_SM_KW_ALL`. It is used for the migration procedure of documents to import KW documents into the new folders. You can remove the value after having run the migration procedure for documents.
> - Test Suite uses document folders which are specific to Test Suite, as users create Test Notes from Test Documents. The relevant authorization object `S_SMDDOC` is contained in roles `SAP_SM_KW_*` allowing values that are contained in table `SMDFLDGRP`. By default, all folder groups are allowed. Test Notes and Test Results are stored in a KW folder that has the name of the solution added by naming convention `TWB`. If you want to restrict folders specifically to Test Suite documents, make sure that you need to add this naming convention <`.TMW`> in addition to the solution, `<technical solution name>.TWB`.

Digital Signature for Test Suite

Test Suite contains a separate framework for Digital Signature which allows you to use a signature process for Test Plans. All relevant authorizations for object `C_SIGN` for this use case are contained in roles `SAP_STWB_2_***`. For more information, see the scenario-specific guide for *Test Suite*.

Authorization Objects with fields for solution and branch

- `SM_CM_DGPN`
- `SM_CRM_RFIT`

These two objects are used in the area of Change Control. They are used in combination with authorization object `SM_SDOC`, which should only be maintained for display use.

Embedded Search (TREX and HANA based)

Embedded Search supported by TREX or HANA is used in SAP Solution Manager by various scenarios, such as *Process Documentation*, *Change Request Management, Incident Management* or *Q-Gate Management*.

Authorizations

All authorization objects required by this basic function are included in the core role `SAP_SM_ESH*`. You can use role `SAP_SM_ESH_ADM` to configure the view: Embedded Search. For more information, see the *View Embedded Search* section in the *Secure Configuration Security Guide*. All authorization objects related to Embedded Search have the following naming convention: `S_ESH_*.`

9.5 Change Control Related Issues

Batch Job Authorizations (S_BTCH_***)

The authorization object `S_BTCH_JOB` in roles for *Change Request Management* contain the `ACTVT` to delete. During cycle switches, either in continual cycle, phase cycle or release cycle, you can either switch the existing

import jobs or at least remove the old jobs and schedule new ones on the same recurrence basis. While you can close a change cycle and create a successor change cycle, all existing jobs in the closed change cycle need to be finished. As these jobs are not the change manager's or release manager's own jobs, they need to have the authorization to finish any developer's jobs in order to close the change cycle.

→ Recommendation

We recommend that you remove the authorization for any user who should not be able to remove background jobs for this case.

Restricting Change Control Landscapes and Branches/Processes (SM_CM_FUNC)

To be able to differentiate between processes and branches in Change Request Management, you need to maintain authorization object SM_CM_FUNC which is contained in all roles concerning change control. Here, you can refine the solution and branch together with cycle type in combination with specific functions for all Change control related scenarios, such as Change Request Management, QGM, or Requirements Management.

→ Recommendation

If you restrict this authorization object for your scneario, we recommend that you do the following:

- Check that authorization object `SM_SDOC` is maintained with `ACTVT` display for the same solutions and branches. This object is contained in roles `SAP_SM_SL_***`. For more information, ee also section *Processes and Process Documents*.
- Check all roles that contain the object, such as roles for the dialog user, but also for technical users such as `SM_EFWK` or `SOLMAN_BTC`. If you want to know more about how to find out all roles that contain the object, or any other authorization object in question, see the *Configuration Validation* possibilities in the *Useful Tools* section.

Restricting Number Ranges Authorization S_NUMBER

Most of the CRM-related scenarios, such as Requirements Management or Change Request Management, require the maintenance of number ranges with transaction `SNUM`. The object is delivered in roles `SAP_***_CONFIG` but must be maintained accordingly.

Organisational Org Unit Maintenance Authorization PLOG

Authorization object `PLOG` defines an organizational level in HR Management. When you use organisational units with CRM-related scenarios, this authorization object is required. It is shipped inactive in all SAP Solution Manager standard roles and must be set to active.

> ⚠ Caution
>
> The object requires specific maintenance in transaction PFCG. Please see the general documentation for transaction PFCG and Authorization Object Maintenance.

Transaction Type Relevant Authorization Objects

Adapting Transaction Type Relevant Authorization Objects

With standard SAP roles, users in the Change Request Management application are able to display every transaction with read authorizations. As a user in your system should only be granted minimal authorizations that are necessary to perform its intended function, all relevant authorization objects that relate to transaction types must be maintained. The authorization key and status profile depend on the transaction type. For the various scenarios, different transaction types are delivered by SAP, which need to be adapted later due to customizing. If you customize your own transaction types, you need to add them and related entities to the according authorization objects. You can find out which standard SAP transaction type is used for the individual scenarios in the application-specific guides.

> → Recommendation
>
> We strongly recommend that you define a granular authorization concept for users to access transaction types and perform activities in transaction types and diligently document the customizing of any CRM objects and modification of authorization objects in CRM.

All authorization field values delivered are SAP-owned customizing entries. If customizing is executed in a customer system, these values must also be adapted in the required authorization objects. The field values are:

- Transaction Type
- Authorization Key
- Status Profile

The fields are contained in the following authorization objects which relate to each other:

- CRM_ORD_PR checks which transaction type is allowed with access rights
- B_USERSTAT defines the change of status executed by the end-user.
- B_USERST_T defines the change of status executed by the system.
- SM_TIMEREP manages the time recording for messages.
- SM_FIELD checks which UI element can be accessed in an assignment block in the WebClient UI.

Inactive Authorization Object CRM_ORD_LP

For SAP Solution Manager, authorization object CRM_ORD_PR is the main object. You may encounter authorization object CRM_ORD_LP in SAP Solution Manager delivered roles, but here it is set to inactive. Both objects are related due to the CRM authorization check method CRM_ORDER_CHECK_AUTHORITY_ACE, whereas CRM_ORD_LP has a higher ranking than CRM_ORD_PR. Due to the fact, that it is less complicated to maintain authorization object CRM_ORD_PR with two authorization fields, all instances of CRM_ORD_LP are set to inactive.

The following objects are generally assigned:

- CRM_ORD_OE
- CRM_ORD_OP
- CRM_ORD_PR
- CRM_SEO
- CRM_TXT_ID
- B_USERSTAT
- B_USERST_T

Updating Roles With Modified Authorization Field Values

To keep these modified values for roles over a number of SP updates, either add additional values in the roles themselves or create a separate role with the relevant authorization objects and modified values. You can also use the *Role Adjustment Tool* in transaction SOLMAN_SETUP or application SMUA. For more information on the *Role Adjustment Tool*, check the *Useful Tools* section.

9.6 Manage Import Authorization in Change Request Management

Use

Import authorizations are necessary in the Change Management process. They allow business users to automatically create transport requests and import transports from a source system into a target system. The required authorization object is S_CTS_ADMI. If you use cluster or non-ABAP systems in TMS communication systems, we recommend that you use the equivalent authorization object S_CTS_SADM instead. Authorization object S_CTS_SADM allows you to additionally restrict to systems and domains.

Prerequisites

You are using delivered standard roles SAP_CM_MANAGED_* for users in your managed systems. These roles contain specific security-critical authorizations for the individual business users, which should be handled separately.

Procedure

We recommend two alternatives for handling these security-critical authorizations, depending on your level of security protection for your systems:

- Use existing standard roles for managed systems (assigned import authorization).
- Use the delivered import role `SAP_CM_MANAGED_IMPORT`.

Use existing standard roles

Use the existing roles for users with additional import authorizations.

Use delivered import role SAP_CM_MANAGED_IMPORT

This practice allows you to use role `SAP_CM_MANAGED_IMPORT` for any business user. This role contains all required import authorizations.

> ⚠ Caution
>
> The above roles should only be assigned to the following users in the respectively mentioned systems, but never in production systems or security-relevant systems:
>
> - Developers in consolidation systems
> - Testers in all test systems
> - Change managers in consolidation systems
>
> A combination of authorization object `S_DATASET` and `S_CTS_ADMI` with value `IMPA` and `EPS1` can jeopardize the security in your system. You should only use this practice if you require a smooth Change Request Management process.

Security Criticality

The following authorizations are relevant for the imports into test and production systems.

S_CTS_ADMI and S_CTS_ADMS

Both objects protect administration functions in the change and transport system in transaction `STMS`: In contrast to object `S_CTS_ADMI`, authorization object `S_CTS_ADMS` restricts directly to your systems.

> i Note
>
> The value for TMS allowlist cannot be used for Change Control Management (Change Request Management and QGM). Therefore, the value is not activated by default for any shipped roles.

The following combinations are examples of critical authorization combinations, which should be avoided in your system or only assigned to a user for a specified time frame.

- Transaction `SE06` with values `INIT` and `SYSC` for `S_CTS_ADMI` and `S_TRANSPRT` with display authorization.
- Transaction `SPAM` with a combination of `S_CTS_ADMI` value `TABL` and `S_TRANSPRT` value `PATC` for `ACTVT 01` (create).

S_TRANSPRT and S_SYS_RWBO

With authorization object S_SYS_RWBO, you have the option to specify the system destination and domain, which are not available in S_TRANSPRT.

9.7 SAP EarlyWatch Alert Data

For any session, but specifically for EWA sessions, ACTVT 06 (delete) for authorization object D_SVAS_SES is security-critical. This object without delete authorization is contained in role SAP_SETUP_BASIC, which is assigned to user SOLMAN_ADMIN. If you need to remove sessions from your system, you must add the value manually.

9.8 Restricting BI Master Role SAP_BI_E2E

Display Authorization for Role SAP_BI_E2E

Role SAP_BI_E2E contains activation authorizations for all BI reporting scenarios as well as batch authorizations. It is not delivered as a display role, as this use case is very specific. For example, if you want to display performance data in the Alerting Framework in the *SAP Solution Manager Administration* launchpad group, you also have to add role SAP_BI_E2E.

If you want to restrict the role for display purposes, proceed as follows:

1. Copy role SAP_BI_E2E.
2. Restrict the activity field ACTVT for all authorizations to *display* (usually 03).
3. The authorization objects S_BTCH_* should be set to inactive.

9.8.1 Business Partner Data

Business partners are used by many applications running in SAP Solution Manager. These roles contain all necessary authorizations for their usage.

> **i** Note
>
> If this role (or the corresponding authorization objects) is not assigned to a user, this user cannot display the *Business Partner* tab in transaction LMDB, or filter in the POWL queries SMWORK_TSYS_DIAG_REL and SMWORK_DIAG_ALL.

Within transaction `LMDB`, you can go to the *Business Partner detail* screen of the CRM WebClient application. To be able to do so, you need to additionally assign the following two roles to your user:

- `SAP_SM_CRM_UIU_SOLMANPRO` (do **not** copy into your name space) for navigation access
- `SAP_SM_CRM_UIU_SOLMANPRO_PROC` (do copy into your name space) for authorization access

Business Partner

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

10 Data Protection and Privacy Measures

10.1 Vulnerabilities

> **i Note**
>
> In majority of cases, compliance with data privacy laws is not a product feature. SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for simplified blocking and deletion of personal data. SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

The following section deals with:

- Overview of Relevant Applications in SAP Solution Manager and possible safeguard applications
- Reporting on Existing Data to Identified Data Subjects
- Simplifying Deletion of Personal Data
- Tighten Table Read and Write Access/Table Protection
- Change Log Information per Function
- Archiving of Objects
- SAP ILM Tool Support

Each chapter contains relevant information per scenario and/or function.

10.2 Glossary

The following section provides details on terms that are relevant for chapter *Data Protection and Privacy Measures*:

> **i Note**
>
> For simplicity reasons, the following abbreviations are used throughout the chapter:
>
> - Abbreviations for functions are referenced in section *Overview of Relevant Applications in SAP Solution Manager 7.2*. For instance, Service Availability Management is abbreviated as SAM.
> - Business partner as BP
> - End of purpose as EoP
> - Information Lifecycle Management as ILM

Glossary

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person (*data subject*). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Purpose	A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Deletion	The irreversible destruction of personal data.
Retention period	The period of time between the end of purpose (EoP) for a data set and when this data set is deleted subject to applicable laws. It is a combination of the residence period and the blocking period.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorization.
Residence period	The period of time after the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Where-used check (WUC)	A process designed to ensure data integrity in case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent function allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.

10.3 Overview of Relevant Applications in SAP Solution Manager

General Information

The following section gives you an *Overview* of all relevant applications and possible safeguarding measures.

Before You Start: Check the Main Collective SAP Note

> → Remember
>
> Check the main collective SAP Note 2610137, which is also linked in transaction `SOLMAN_SETUP_ADMIN`, view *Security*, step *General Data Protection Regulation*. For personal data stored by the addon `ST-A/PI`, see SAP Note 2638080.

Business Partner Protection

For general information on business partner protection, see Application Help for Business Partners.

BW-Related Information

If not otherwise stated, use standard BW functions as described in the BW documentation Data Protection and Privacy.

CRM-Related Information

CRM access control engine is used. This includes a hierarchy of authorization objects and possible BAdI implementations created by the customer to enforce access, see chapter Using CRM in SAP Solution Manager in the *Authorization Concept in SAP Solution Manager* security guide and *CRM ACE/Authorization Documentation* for further information. In addition, check SAP Note 2354273.

Overview of Relevant Applications

The table below gives you an overview over:

- *Applications*: Functions on scenario level
- *Object*: Personal data used per function
- *Purpose*: Information about which object or document is related to the personal data mentioned in column *Object*
- *Comments*: Specific information relevant for the function
- *Safeguards*: Specific information on protection measures for the function

All information in the following chapters is based on the overview table.

Functions

Application	Object	Purpose, Comments, Safeguards
Business Process Change Analysis		

Application	Object	Purpose, Comments, Safeguards
Business Process Change Analyzer (BPCA)	User IDs, business partner	User IDs are mandatory for **traceability and auditing** on who performed what actions in the system. 1. **Third-party test management tool registry (Customizing activity)** Used to register third-party test management tools for data exchange with BPCA 2. **BPCA analysis** Stores the result of a change impact analysis 3. **Optimization approach** Reusable settings for BPCA test scope optimization 4. **Technical bill of material (TBOM)** Technical bill of materials of an executable object. Stores all objects used while executing an executable unit. 5. **TBOM history** Action log for changes in TBOM per executable object. 6. **TBOM classification** Stores classification of objects types appearing in TBOMs 7. **TBOM criticality** Stores criticality of objects appearing in TBOMs 8. **TBOM filter** Stores rules for excluding objects in TBOMs from BPCA analysis 9. **TBOM options** Settings for TBOM recording 10. **TBOM work items** Used to delegate TBOM creation of business process experts 11. **TBOM work item configuration** Stores the CRM transaction type for TBOM work items The following objects exist in the managed systems where BPCA functions are used: 1. **TBOM options in managed system** Stores options for TBOM recording in managed systems. 2. **BPCA object and key mapping** Stores mapping between transport and runtime objects. The application is protected by authorization object `SM_BPCA`.
Business Process Operations (BPO)		
Business Process Completeness Check (BPCC)	User name	The user name displays who started the **process instance**. The process instance shows the user name in context *Step Context*. Authorization object `SM_APP_ID` with `ACTVT 03` and `URL_APP_ID BPCC` protects the access.

Application	Object	Purpose, Comments, Safeguards
Business Process Improvement (BP Improvement), including: 1. Business Process Analytics 2. Business Process Operations Dashboards (including Setup Application) 3. Progress Management Boards 4. Dependency Diagrams (including Setup Application) 5. BPO Reporting Infrastructure Maintenance (especially Usage Analysis) 6. Maintenance Tool Persistence Browser 7. Automation Rate Cockpit	Responsible person data, user IDs	Maintenance of responsible persons such as name, phone number, e-mail, academic title, and department. These are relevant for application 3. User ID in change log for objects stored in the database. This is relevant for applications 1-5. Change log can be viewed in application 6. User ID in usage log. This is relevant for application 1 and 2. Usage log can be displayed in application 5. User ID in business process improvement KPIs (if provided as characteristic), which can be viewed in application 1 and 2. *Responsible Persons* are used to define who should take care of **issues and action items**. User ID can be available in KPIs as characteristic for **analysis** reasons. User ID is used to track changes within business process improvement configuration objects. User ID is used in usage analysis to measure which people are using which business process improvement applications. *Responsible Persons*: authorization object `SM_BPA_OBJ` with field name `BPA_OBJTYP` = `RESPONSIBLE` and field `ACTVT` with values `01,02,03,06`. Display change log (including User ID) via application 6. Relevant authorization object `SM_BPM_ACF` with field name `ACTVT` = `01`. Display usage analysis (including User ID) via application 5. Relevant authorization object `SM_BPM_ACF` with field name `ACTVT` = `01`. Display user ID as a characteristic in applications 1 and 2. Relevant authorization object `SM_BPM_ANA` with field name `ANALYTICFUNC` = `BENCHMARKING_ADV_USR.` **⚠ Caution** In business process operations, you can write your own monitors that persist data on the managed system. Which kind of data you collect is in your own responsibility.

Application	Object	Purpose, Comments, Safeguards
Business Process Monitoring (BP Mon)	Business partners, user ID, e-mail	For complex notification scenarios, e-mail addresses and business partners can be configured as **recipients of the alert notification** via **notification grouping**. During data collection, a detail list of the relevant business objects is persisted on the managed system. This detail list can include business partners or user names (depending on the functional scope of a key figure). In the usage of BPMon, when accessing the BPMon application or BPO alert inbox, the user has to choose a **solution context**. The last solution context used per application is persisted per user. BPMon configuration can only be displayed if sufficient authorization is assigned. The same authorization governs the access to the notification grouping. For this, Solution Doumentation authorizations as well as BPMon authorizations are checked. The access to the detail list is managed by authorization object `SM_BPM_DET`. **i Note** For some monitoring objects, the detail list is on the managed systems while for others it is on SAP Solution Manager. Additionally, not all monitoring objects have detail lists. **⚠ Caution** In business process operations, you can write your own monitors that persist data on the managed system. The kind of data that you collect is your own responsibility.
Cross-Database Comparison (CDC)	User name	To track who changed a data model (versioning) and by whom and when a certain comparison was executed (history). Relevant authorization object `SM_CDC_OBJ` which displays the data model and its versions. Use the relevant authorization object `SM_CDC_INS` to see the comparison history. Activity *Execute* allows you to run a new comparison and activity *Output* allows you to review the result.
Job Health Check	User name	To be able to understand the user that scheduled a batch job.
Interface Documentation	User ID	User ID for batch input (BI) and file creator in technology file (FILE). Authorization object for transaction `AGS_DCM_IF_DOCU` exists with specific authorization for the custom attributes application `AGS_DCM_CUST_IFDOCU`. To acess OCC Alert Reporting, the user has to choose a solution context. The last used solution context per application is persisted per user.*Solution Documentation* application, you need the relevant authorizations for it.
OCC Alert Reporting	User IDs	
Change Control Management		

Application	Object	Purpose, Comments, Safeguards
BW Reporting: • ITSM BW Report • ChaRM BW Report	When accessing the OCC Alert Reporting, the user has to choose aText of the business partner names and business partner IDs	The text and ID of business partners is essential information in the reports, like the processor of a ticket or the tester of a test case. End users can filter, drill down, and aggregate on business partners. For **ITSM BW Report** and **ChaRM BW Report**, BW infoobject `0SPRBPNO` contains the text of the business partner. The following applications are relevant: 1. **ITSM BW Report** • SOLMAN_WORKCENTER -> IT Service Management -> Incident and Problem Dashboard • SOLMAN_WORKCENTER -> IT Service Management -> Incident and Change Dashboard • SOLMAN_WORKCENTER -> IT Service Management -> Service Order Dashboard • SOLMAN_WORKCENTER -> IT Service Management -> Service Request Dashboard • SOLMAN_WORKCENTER -> IT Service Management -> Incident Dashboard 2. **Change Request Management BW Report** SOLMAN_WORKCENTER -> Change Management -> IT Service and Change Management Dashboard All reports in the Dashboard Builder (see also information on *Dashboard Builder* in scenario *Infrastructure*) are protected by authorization objects `SM_DSHCAT` and `SM_DSHO`. SAP Solution Manager-related data in BW is protected by authorization objects in the `RS` object class.
Change Request Management (ChaRM)	Business partner and user ID	Compliance of software change management processes; all participants in the change process have to be tracked. The standard CRM authorization concept for all CRM documents applies.

Application	Object	Purpose, Comments, Safeguards
Configuration Validation and CCDB	User ID	**Configuration stores** can contain confidential and personal data to allow for the analysis of any configuration data in any of your systems in the system landscape. The purpose is to get an overview of configuration data on the managed systems, to detect changes, and to validate configuration against a customer defined policy (target system). **ConfigStores** The ConfigStores are protected by authorization objects SM_CV*. Data of ConfigStores that do have user IDs are secured by authorization object AI_CCDB_SC using field CONT_AUTH with value SECURITY. **Example** The ConfigStore AUTH_PROFILE_USER is an example that has the user ID stored. It contains all the user IDs that contain the SAP_ALL profile assigned in the managed systems client. The tables that hold the configuration data are secured by the DIAGST table authorization group. **CCDB** The CCDB tasks and data are monitored in CCDB administration. CCDB uses the Extractor Framework (for more information, see function *Extractor Framework* in scenario *Infrastructure*) to transfer technical data of the connected managed systems into the configuration and change database (CCDB). CCDB is a set of tables stored in the database of SAP Solution Manager. Some of the configuration data contain user IDs. **Note** The application configuration validation has a feature called *Trend Analysis*. This feature offers to store the result of the validation by using a periodic job. By default, no job is scheduled. This means that no data for *Trend Analysis* is stored. You can schedule a job for a report for *Trend Analysis*. Then, the data is stored in BW InfoCubes. CCDB administration can be started via: *Fiori Launchpad → SAP Solution Manager Administration → Configuration Change Database Store Administration*.
Incident Management (ITSM)	User ID and business partners	Used in CRM-related incidents, service requests, and problems reported by the customer or the user.
License Management	User ID	Personal data is stored as part of log entries where they indicate the person who changed the state of automatic distribution of licenses or triggered the license distribution process.
Quality Gate Management (QGM)	Business partner and user ID	Compliance of software change for QGM processes: all participants in the change process have to be tracked. The standard CRM authorization concept for all **CRM documents** applies.

Application	Object	Purpose, Comments, Safeguards
Requirement Management	Business partner and user ID	Compliance of software requirements management processes: all participants in the change process have to be tracked.
System Recommendation	SAP user names	SAP user names are used to log the decisions by a user, for instance, assignments, comments, creation of ChaRM requests, and so on. This log and the comments are relevant for auditing. For each user, a personalization such as filter settings, is stored. The respective authorization object is `SM_FUNCS`.
Custom Code Management (CCM)		
CCM and Custom Code Library	Owner data	*Owner Data*, if the owner is a person, *Owner Data* describes who is responsible for the custom code data. The purpose is to **assign an owner to one or more custom code objects**. The owner data is protected by authorization object `SM_CC_LIB.`
Data Volume Management (DVM)		
DVM	User ID	You can create **impact and reference projects** based on existing solutions.
Job Management		
Job Management	User ID, e-mail, business partner	Send the **notification** by e-mail if a job has failed or has not run due to any reason. Additionally, it is used to check the created by or last changed by user. According authorization objects are in place.
Process Management		
Custom Development Management Cockpit (CDMC)	User ID	User IDs are stored in Customizing tables for information purposes like who created a project, who executed the activity, and so on. Authorization object used is `S_CDMC`.
Customizing Distribution and Customizing Scout	User ID	To keep track of who has created the synchronization group and the setup.
JSON file (Process Document Viewer)	User name	The application needs to display the name of the user in the customer organisation responsible for the different processes extracted from SAP Solution Manager and display the creator of the processes in SAP Solution Manager.
SLO Analysis Services Tool		

Application	Object	Purpose, Comments, Safeguards
Solution Documentation	Business partner and user ID	The business partner and user IDs are needed to store responsible persons and/or owners of **elements** or persons who created the last change of **an element or an attribute** in the application. The user ID is used for digital signature of **KW documents**. The application dynamically reads basic information associated with the business partner ID or user ID and displays this information. This basic information is the name of the user, which can consist of a combination of first name, last name, academic title, and so on. **i Note** The application stores the IDs of business partners and users but not the person-related data associated with these IDs. The person-related data associated with these IDs is read on demand. Relevant authorization objects `SM_SDOC` and `SM_SDOCADM` are used to protect the application.
Solution Documentation Graphical Editor Diagram Entities	User ID	User IDs are mandatory for traceability and auditing on who performed what actions on the system, to display the users responsible for creation, and last changes of diagram objects and diagram entities. This allows you to keep track on changes in diagrams and different diagram entities. The *Graphical Editor* is managed by application *Solution Documentation*. The relevant authorization object used is `SM_GAL_GO`.
Quick Upgrade Analyser (QUA)	User ID	Range of HR personal numbers, vendor, and customer numbers
Project Management		
Project Management (ITPPM)	User ID	User ID is stored in log data for the copied Customizing table `SMCP_CUST_TABLOG`.
Root Cause Analysis		
Agent Administration	User ID	User IDs in the *Maintenance Mode History* are mandatory for **traceability and auditing** on who performed this action on the system. This information is only visible to users assigned to role `SAP_RCA_AGT_ADM`.
E2E TA Housekeeping: Trace Analysis	User ID	User IDs are integral parts of **logs and traces** which are collected from the managed systems and are displayed in the application. Authorized users are allowed to display traces.
Exception Management	Reference to a user ID	Exception management may include a reference to a user ID as part of the **data payload that is retrieved**.
SAP Engagement and Service Delivery		

Application	Object	Purpose, Comments, Safeguards
Customer Service Administration (CSA)	E-mail address	When a CSA session task is changed to being *Overdue* or having received a *Warning*, a **notification E-mail** is sent to the related person, whose e-mail address is maintained as a recipient.
DSA / Web DSA	User ID	User IDs are mandatory for traceability and auditing on who performed what actions on the system. The **session data** can be accessed if the user has authorization object `D_SVAS_SES` assigned.
EarlyWatch Alert Settings (EWA Settings)	Business partner ID and user ID	User IDs are mandatory for traceability and auditing on who performed what actions on the system. Business partner IDs are stored as **contacts for EWA Sessions**.
Issue Management	Business partner ID and user ID	**Issues, top issues, task issues** are objects based on CRM. The assigned business partner reflects the role (processor, reporter) and is used to inform any relevant persons via e-mail in case of status changes. The user ID which is stored displays who created and/or changed an object. Corresponding authorization objects are in place.
Service Delivery	Business partner ID and user ID	**Service sessions** are executed by SAP employees or the user itself. The User ID which is stored, displays who created and/or changed the service session. A business partner can be assigned optionally. **Engagement Cycles and Support Requests** are based on CRM. The User ID which is stored, displays who created and/or changed an Engagement Cycle or Support Request. According authorization objects are in place.
Service Content Update	User ID	The **Service Content** is used when executing services such as SAP EarlyWatch Alert, SAP CQC for implementation or others within the service session workbench (DSA). **i Note** Software component version ST-SER 720 contains the service content. Transaction `AGS_UPDATE` offers an option to **receive updates from the support backbone**. The user ID which is stored displays who executed updates from the support backbone. According authorization object is: `SM_CNT_UPD`.
Service Data Collection (SDCCN)	User ID	Service data download (SDCC) is storing user IDs for auditing and traceability in regards to the tasks created. See SAP Note 2643956.
Value Based Delivery Dashboard	User ID	Used for *Engagement Cycles*.
SAP Solution Manager Administration		

Application	Object	Purpose, Comments, Safeguards
UOCShell Personalization	User ID	**Ownership** ("what is my personalization configuration") and traceability ("who last changed a personalization configuration")
Scope and Effort Analyser (SEA)		
Scope and Effort Analyzer (SEA)	User ID	User IDs are mandatory for traceability and auditing on who performed what actions on the system. The application is protected by authorization object `SM_SEA`.
Technical Administration		
Central Notification Management (`CNM`)	External recipients and user ID	Responsible persons are maintained with name, phone number(s), or e-mail. An e-mail ID or a phone number is used to send **e-mails or SMS to the recipients**. User IDs are used to keep track of who created or changed the **CNM resources**.
IT Calendar and Work Mode Management/ IT Events	User ID	User IDs are stored to keep track of who created and changed the calendar events like work modes and IT events. Authorization objects: • `SM_WMM_AUT` Authorization object for workmode management • `SM_ITE_ACT` Authorization object for IT event
IT Task Management	User names and business partner ID	Tasks are assigned to business partners and users. Authorization object `SM_TP_AUTH`: Authorization object for IT task planning
Service Availability Management (SAM)	User IDs	Used in **Service Definition, Service Outage** Service availability data is audit relevant. This data is protected by the following authorizations: • `SM_SAM_DEF` Service Availability Management - Service Definition • `SM_SAM_OUT` Service Availability Management - Service Outage
Technical Monitoring		
BI Monitoring	User ID	Administration purpose (for instance to check the created by or last changed by user)
BW Reporting: System Monitoring (also: System Reporting)	User ID	The user ID is part of the statistical record created by SAP basis. The ABAP statistical records are collected from the managed systems and stored for use in the SAP Solution Manager-related BW for RCA (see also the according scenario information) and system reporting. It is not explicitly used by system reporting but could be used by individual analysis.
Central Job Overview	User ID	Customizing (mails customizing and saving variants).

Application	Object	Purpose, Comments, Safeguards
Data Readiness Monitoring (DRM)	User ID, e-mail ID	Customizing (mails customizing and saving variants) and administration purpose (for instance to check the created by or last changed by user).
Interface - and Connection Monitoring	User ID	The user ID is stored in a table but not displayed in the UI.
Job Monitoring	User ID	Administrative purpose to check *Created by* or *Last Changed by* information.
Monitoring and Alerting Infrastructure including Alert Inbox (MAI and Alert Inbox)	User ID	Alert inbox keeps an action log for each alert that was processed. Some of these actions include sending notifications (e-mails, SMS), postponing an alert, creating an incident out of an alert, confirming an alert, adding a comment to an alert, and so on. Authorization object `SM_MOAL_TC`
Message Flow Monitoring (MFM)	User ID	**Configuration**: The application maintains the person responsible for each **message flow type** by manually entering the name of the user. This can be replaced manually by the administrator at any time. **Monitoring**: The application maintains the **filter variants** for a user ID. **Application Part**: The **payload information** collected from the managed systems, including the SAP PI system, can contain personal information. The application is protected by the `SM_MOAL_TC` authorization object, with the corresponding values for message flow monitoring. Additionally, the message flow for a group or an instance is protected by the `SM_MFM_FG` authorization object and the payload is protected by the `SM_MFM_PYL` authorization object.
PI Monitoring	User ID	In the message search application, users can save **filter variants** for their user IDs. The application is protected by authorization object `SM_MOAL_TC`, with the corresponding values for PI Monitoring.
Self Diagnosis	User ID	User IDs are mandatory for traceability and auditing on who performed what actions in the system. In the *Self-Diagnosis* application, the user ID is saved when *Self-Diagnosis* settings are changed and saved. The application is protected by authorization object `D_SM_S_DIA`.
System Monitoring (Mobile Optimized SAP Fiori App)	User ID	User IDs are used to store **favourite systems** that a user would like to display when the application loads.
User Experience Monitoring	User ID	**Personalization** for the monitoring application such as organization of views, preferences, filters, and so on. User IDs are mandatory for traceability and auditing on who performed what actions on the system. User ID stored in configuration logs by the Guided Procedure framework. Any personal data within a recorded script.
Test Suite		

Application	Object	Purpose, Comments, Safeguards
Test Suite BW Report	Text of the business partner and business partner IDs	The text and the ID of business partners is essential information in the reports, like the processor of a ticket or the tester of a test case. End users can do filter, drill down, and aggregation on business partners. All reports in the *Dashboard Builder* (see also function *Dashboard Builder* in scenario *Additional Functions*) are protected by authorization objects `SM_DSHCAT` and `SM_DSHO`. Data in the SAP Solution Manager-related BW is protected by authorization objects in the `RS` object class. For **Test suite BW report**, the BW info object `0SMTBP` contains the text of a business partner.
Partner Test Management	User ID	Used for: • Administration of data for connectivity to third-party system and association information • Retaining the status of different asynchronous activity triggered by SAP Solution Manager system to synchronize with HP ALM • Retaining the test results synchronised from HP ALM and logs for association Authorization object `SM_TS_PTM` is used to protect the application.
Test Suite including Test Automation and Management, SUT Management (CBTA and TAO)	Business partners and user ID	Business partners are used to store **test plan, test package, and test sequence** responsibles. They are also used to stored the tester assigned to a given test package and/or test cases. They are also used in filter definition for test cases hierarchy and analytics reports. A user ID is used to store the *Created by* and *Changed by* data for major objects. It is also used to store *Executed by* data for batch job execution as well as user preferences in *Personalization*. As test plans reflect the information from *Solution Documentation* (see also scenario *Process Management*) hierarchy, all node attributes from Solution Documentation which refer to personal data are also stored in the model for both business partners and user IDs. User IDs are stored in case of **digital signature**, both for **test plan** and **test documents** (for instance test plan attachments and test package attachments, test note and test results). User IDs are stored in SUT management.
Infrastructure		
Extractor Framework (EFWK)		
Guided Procedure Authoring (GPA)	Users ID	User IDs are mandatory for traceability and auditing on who performed what actions on the system. They are also mandatory for the business to identify who created guided procedures, steps, and activities.

Application	Object	Purpose, Comments, Safeguards
Guided Self Services (GSS)	User ID	User IDs are mandatory for traceability and auditing on who performed what actions on the system. The log can only be accessed if the user has authorization object `SM_SETUP` with the value **Display** to be able to navigate in the setup scenarios.
Landscape Management Database (LMDB)	User ID	Change log entries because they contain the information about which user executed changes in low level format. It is used to broadcast landscape changes to applications via the *LMDB Notification Framework* and to analyse changes during SAP delivered support. The `AI_LMDB_AD` authorization object protects generic access to the CIM objects stored in the LMDB.
	User ID	**Landscape Data Entities** User IDs are mandatory for traceability and auditing on who performed which actions on the entity. The `AI_LMDB_OB` authorization object protects access to technical systems and hosts in transaction LMDB. The `AI_LMDB_AD` authorization object protects generic access to the CIM objects stored in the LMDB. If accessed through transaction `LMDB_ADM`, only the generic CIM-based access is possible. If you access the CIM objects generically by using the *Details* button, the authorization object `AI_LMDB_AD` is needed as well.
	User ID	**Customizing of additional attributes** contains the information on which user created and executed changes. Additional LMDB attributes are used for Customizing. Users can create their own custom attributes and assign them to a technical system type and host.
	Business partner ID	Business partners contain information about a person, a group of persons, or organizations. Business partners can be assigned to a technical system. LMDB only displays the information of business partners assigned to a technical system. The relationship between business partners and technical systems are persisted in the CRM IBase.
	User ID	User IDs are used for **support** reasons; they allow the **identification of entries needed for special analysis**.
`SOLMAN_SETUP` (Configuration Transaction)	Picture upload	To allow for upload possibility of additional information. **i Note** It is in your responsibility what information the picture contains. The function is protected by authorization object `SM_UPLOAD`.

Application	Object	Purpose, Comments, Safeguards
SOLMAN_SETUP (Configuration Transaction)and managed system configuration	Users ID	User IDs are mandatory for traceability and auditing on who performed what actions on the system. Users IDs are stored in log table AGSSISE_LOG and are stored in the generic storage for configuration purposes.

Background job REFRESH_ADMIN_DATA_FROM_SUPPORT
 	
Service Connection Application
	Contact person	Details of contact persons, instance name, gender, telephone number, e-mail, country, language, and so on are synchronized from SAP Support Portal.
		
		The data in the relevant table AICONTACTS is used in the following scenarios:
		
		• *Incident Management*: Report AI_SDK_SP_GENERATE_BP_V2 generates business partners and users based on this table. This report can be run when SAP Solution Manager is run by *Value Added Resellers (VAR)*, so that the customer of the VAR is able to create incidents in the SAP Solution Manager system of the VAR.
		• *Service Connection Application*: The S-User is selected as a contact person when setting up or opening a service connection.
		• *SAP Communication*: This table is used as a value help of S-User selection in transaction AISUSER.
		
		Table Information:
		
		• Table AISUSER stores the mapping between SAP Solution Manager users and contact persons. The data in table AISUSER is used to determine the requester for SAP communication.
		• Table AICONTACTS stores the details of contact persons, for example, name, gender, telephone number, e-mail, country, language, and so on, which is synchronized from SAP Support Portal.
		• The data in table AIINSTACCESS is used to perform pre-checks before the data is sent to SAP communication.
		Table AIINSTACCESS stores the authorization of each contact person, including the following authorizations:
		  • Create customer messages ANLEG
		  • Open service connections SVER
		  • Maintain system data INSTPROD
		• Table AICONNSTATUS stores the contact person for opening a remote connection at SAP. Before SP07, this table stored telephone number, e-mail address, and fax of this contact person. As of SP07, the contact person ID is stored instead of these fields.
		
		→ Recommendation
		
		Run the background job for report AI_SC_MIGRATION to refresh this table.
		
		The Order Software function in the SWCATALOG software catalog is no longer used in SAP Solution Manager 7.2. The job deletes all entries in this table for SWCATALOG after you have implemented SAP Note 2641326.

Additional Applications		

Application	Object	Purpose, Comments, Safeguards
Dashboard Builder	User ID	The user ID in the Dashboard Builder is stored in order to know which user created or modified a **dashboard**.
Dashboard Framework	User ID	The user ID is used to identify the user's **personal configuration**, or, in case of **custom developed objects**, identify the creator of such objects. Relevant authorization objects are `SM_APPTYPE`, `SM_DSBFWK`, and `SM_DSBINST`.
KPI Catalog API	User ID	The user IDs are used for **support reasons**. They allow the identification of entries that are needed for special analysis.
Rapid Content Delivery	User ID	User IDs are used to update the content delivered via software component `ST-CONT`. Authorization object: • `CSU_UNPACK` to unpack content
Social Application Integration `(SAI)`	User ID	The user ID is used to link the SAP Solution Manager user with the Social Application Platform user. The function is protected by the authorization object `SM_SAI`.
URL Framework	User ID	The user ID is stored to keep track of who has customized or created an application URL in the URL framework. You require access permissions for the URL framework UI.
Functions relating to SAP Solution Manager Release 7.1		
Application Specific Upgrade Toolbox (ASU Toolbox)	User ID, technical user ID (RFC scenario)	User IDs are used to store who has created or changed **ASU Content/ASU task list** and who has executed and confirmed an ASU task list step. In the RFC scenario (ASU step is executed on a separate system), the technical user ID stored is used for the RFC connection. Authorization object is `B_ASU_ADMI`.
ESR/PSLE Self Service Reporting (ESR/PSLE)	Business partner ID and user ID	Business partner IDs are essential information in engagement self-service reports. They are stored in SAP Solution Manager-related BW for **reporting** purposes. User IDs are used for **configuration** purposes. Data in the SAP Solution Manager related BW is protected by the authorization objects in the `RS` object class.
Roadmap	User ID	User IDs are stored to display who created the Roadmap and who changed it last.
Solar Project, Learning Map, Solutions (SOLAR)	Business partner and user ID	User IDs are stored to keep track of who has created or changed Project, Learning Map, Solution Elements. Business Partners can be assigned as customer attributes to project and solution elements.
Solution Documentation Assistant (SDA)	User ID	To keep track of who has created and changed **analysis projects, analysis, and check steps**.

Application	Object	Purpose, Comments, Safeguards
Switch Framework (Business Function Scoping)	User ID	
System Monitoring based on CCMS	User ID	These tables are used to store user personalization in the system monitoring scenario if the CCMS infrastructure is being used. As of SAP Solution Manager 7.1, the system monitoring scenario is part of a new infrastructure base. If an SAP Solution Manager system is upgraded from release 7.0 to release 7.2, tables referencing data for System Monitoring based on CCMS may still contain old data, which could contain personal information such as user names.
Testworkbench BW Reporting	User ID	The following types of user ID are part of the testworkbench data: • Tester • User responsible for creating test plans or test cases • Message processor The structures were used in SAP Solution Manager 7.1 and are obsolete in SAP Solution Manager 7.2. They may, however, still contain data if an upgrade took place. There is a standard BW access mechanism in place for accessing data.
Test Management	User ID, business partner ID,	See the *Test Suite* scenario and section for *Test Automation*. The data refers to tests that have been planned and performed before the upgrade to the current release. The data is available for reference purposes only.
Transaction SMSY	User ID	

Additional Information Sources

- Specific **application security**, see the respective sections in the *Application Specific Security Guide*.
- Specific **configuration security**, see *Secure Configuration Security Guide*.
- Authentication and authorization features are described in more detail in sections **Managing Authentication** and **Managing Authorization** of this guide. See also the *Authorization Concept in SAP Solution Manager* security guide.
-

10.4 Reporting on Existing Data to Identified Data Subject

SAP Solution Manager and Managed Systems: Automated Option - Transaction SM_PD_INFO

Using Transaction SM_PD_INFO

You can report on existing data subjects in SAP Solution Manager using transaction SM_PD_INFO. Here, you find:

- The option to run the report over all scenarios using *All Scenarios*. This information retrieval is run using a background job. The *Job Log* for the background job lists all relevant scenarios and functions and their specific user information.
- A number of reports separated per scenario and function to report on individual data subjects. If a function has the option for automatic information retrieval, it is listed underneath in column *Report* with symbol X.

> **i** Note
>
> To run information retrieval reports which connect to the managed systems, the READ RFC connection is used.

> **→** Tip
>
> To ease using the information retrieval for your currently used functions, you can maintain table AIDPP_REPORTS(_T) accordingly. In the table, set the flag for your own functions. In addition, you can also maintain your own authorizations in fields AUTH_OBJECT und AUTH_VALUE, which allows you to restrict access to specified functions in the transaction for individual users only.

Authorization Protection

The transaction as well as each report is protected by authorization object S_TCODE value SM_PD_INFO, which you have to assign to the user running the reports.

> **i** Note
>
> SAP strongly recommnds you to only assign this authorization to individual users and remove it after usage.

Read Access Log

The transaction is protected by a read access log. The *Read Access Log* for the reports in transaction SM_PD_INFO can be called in transaction SLG1 using object SM_PD_INFO.

SAP Solution Manager and Managed Systems: Manual Procedure Option

For some functions, both the automatic and manualoptions exist. And, for specific functions, explicit manual procedures are available. Manual procedures are described in column *Manual Procedures*. Authorization protection is mentioned if required.

BW System-Related Retrieval Function

For information retrieval in software component ST-BCO, you can use transaction `SMBCO_PD_INFO` for the following functions:

- BW Reporting for System Monitoring (System Reporting)
- SAP Solution Manager 7.1 TWB Reporting

The transaction is protected by authorization object `S_TCODE` value `SMBCO_PD_INFO`.

> **i Note**
>
> SAP strongly recommends you to only assign this authorization to individual users and remove it after usage.

Read Access Log

The transaction is protected by a read access log. The *Read Access Log* for the reports in transaction `SM_PD_INFO` can be called in transaction `SLG1` using object `SMBCO_PD_INFO`.

Check SAP Note 2640144.

Overview Information Retrieval Options for Individual Functions

The table below gives an overview over information retrieval options.

Functions

Application	Report	Manual Procedure
BPCA		
BPCA	X	When you run the report in SAP Solution Manager, the managed system report can be started from here. **i Note** See SAP Note 2640865
BPO		

Application	Report	Manual Procedure
BPO	X	
Interface Documentation	X	
Change Control Management		
BW Reporting for ITSM and Change Request Management	X	In SAP Solution Manager, run the report in transaction `SM_PD_INFO`. In SAP BW, to view all usages of a business partner ID for BW objects, proceed as follows: 1. In the BW system, call transaction `RSA1`. 2. Choose *Modeling -> InfoObjects* and search for the relevant InfoObjects (`0SPRBPNO, 0SPRCUBP1, 0SPRCUBP2, 0SPRCUBP3, 0SPRCUBP4, 0SPRCUBP5, 0SPRCUBP6, 0SPRCUBP7, 0SPRCUBP8, 0SPRCUBP9, 0SPRCUBP10`). 3. In the context menu for each relevant InfoObject, choose *Maintain Master Data*. If the system displays the *No master data maintenance possible* message, this business partner ID is not used in this InfoObject. If the system displays the *<System ID>: Change Master Data of Info Object Name 0SMTBP* screen, search for the relevant business partner ID. If the business partner ID is not displayed on the master data screen, this business partner ID is not used in this InfoObject. 4. If you find the business partner ID and want to delete it, proceed as follows: • Select the business partner ID and then choose *Delete Keys -> Save*. • Select *Delete SIDs, Delete Texts and Simulation Mode*. • For the search mode, select one usage per value per object. • Choose *Start*. • In the *Confirm Deletion of SID* dialog box, choose *Yes*. • On the *Master Data used* screen, choose *Details*. The system displays the where-used list for this business partner ID. • If the simulation finished successfully, the business partner ID in the master data of this InfoObject is not used in any other BW objects and can be deleted from the master data of this InfoObject. See section *Simplification of Deletion* for more details. If your SAP Solution Manager 7.2 system has been upgraded from SAP Solution Manager 7.1, look for user information in the obsolete `SPR_MDIDX` database table in SAP Solution Manager BW.
Change Request Management	X	

Application	Report	Manual Procedure
Configuration Validation / CCDB Administration	X	**i Note** You can display personal data for CCDB using transaction `SM_PD_INFO`. CCDB offers a selection of data using a variety of filters. As the user ID is stored in element keys or values, user-dependent data is displayed when a selection is done using the user ID as element pattern. Within the application, on tab *Status*, select *Cross Selection*, enter the user ID in the *Element Pattern* field, and press either *Display* or *Display Elements*. *Display Elements* displays the element keys and values having the user ID and the context like configuration store. *Display* offers a list of configuration stores that have the requested user ID stored. This information is needed if the configuration stores that contain the user ID should be deleted. **→ Recommendation** Because of performance reasons, it is recommended to do the selection per configuration store type. In the *Store Filters* area, select the *Type* to restrict a configuration store type. For the selection related to the *XML Store* type or *Text Store* use the element pattern of the user ID starting and ending with an asterisk *. **Example** For instance `*DDIC*` to find elements which have the user ID `DDIC` stored. Text and xml type stores might have the user ID as part of a string, for instance, in the comments of the configuration store `ABAP_INSTANCE_PROFILE`. **→ Recommendation** As the selection using **User ID** is time consuming and not needed for all other store types, just the user ID should be entered as element pattern. For these store types, the user ID is stored in a field, if at all.
ITSM	X	
License Management		This scenario stores user IDs as part of the configuration data and logs that are handled by the scenario SAP Solution Manager Configuration and Guided Procedure Authoring. Refer to the instructions for reporting on existing data to an identified data subject for the scenario *SAP Solution Manager Configuration (SOLMAN_SETUP)* and *Guided Procedure Authoring (GPA)* in scenario *Infrastructure*.
Quality Gate Management	X	
Requirements Management	X	

Application	Report	Manual Procedure
System Recommendation	X	
CCM		
CCM	X	
DVM		
DVM		Run report `DVM_GDPR_INFO`.
Job Management		
Job Management	X	
Process Management		
CDMC	X	When you run the report in SAP Solution Manager, the managed system report can be started from here. **i Note** To run the report in the managed system from SAP Solution Manager, you need to add the following function module authorization to the READ user in your respective managed system for authorization object `S_RFC`: `CNV_CDMC_GDPR_UNAME_INFO, CNVCDMC_GDPR_INFO`. See also SAP Note 2257213.
Customizing Distribution and Scout	X	
JSON file (Process Document Viewer)		1. Export the offline application content. 2. Navigate to the *Data* folder under the application folder. 3. Open the *FastFact JSON* file. 4. Check the value of the relevant fields such as *Changed by* or *Responsible*. 5. Open the *MasterPage JSON* file. 6. Check the relevant field. 7. Open the *UserRole JSON* file. 8. Check the value of the following fields: • Description • Name
SLO Analysis Services Tool	X	
Solution Documentation	X	For further analysis, you can use the advanced search function. All attributes are indexed in the embedded search. You can use this search function to search for specific information in the attribute values as well as in the document content.

Application	Report	Manual Procedure
Solution Documentation - Diagram Entities	X	
QUA		Run report `/SLOAS/GDPR_INFO` in your managed system.
Project Management		
Project Management Customizing	X	
RCA		
Agent Administration - Maintenance Mode		Open the *Agent Administration* UI, select the *Agents* tab and then choose *History* (next to *Maintenance Mode*). Search the history table for the relevant user ID. The data persisted in the *Maintenance Mode History* view of the *Agent Administration* is only visible to users with the `SAP_RCA_AGT_ADM` or the `SAP_J2EE_ADMIN` role.
E2E TA Housekeeping: Trace Analysis		In the E2E Trace Analysis application, use the filter function and press the filter icon in the business transaction table. Specify the data in the *Text* field.
Exception Management	X	
SAP Engagement and Service Delivery		
CSA		Report `RDSVASACSA_PERS_DATA` is provided to retrieve all personal data stored in the CSA database tables. An authority check is taken into account when the report is executed and `SLG1` logs are provided after execution.
DSA / Web DSA	X	
EWA Settings	X	
Issue Management	X	
Service Delivery	X	
Service Content Update	X	

Application	Report	Manual Procedure
SDCCN	X	When you run the report in SAP Solution Manager, the managed system report can be started from here. **i Note** To run the report in the managed system from the SAP Solution Manager, you need to add the following function module authorization to the Read user in your respective managed system for authorization object `S_RFC`: `/BDL/CHECK_GDPR_INFO`. See also SAP Note 2257213.
Value Based Delivery Dashboard	X	
SAP Solution Manager Administration		
UOCShell	X	
SEA		
SEA	X	
Technical Administration		
Technical Administration	X	
Technical Monitoring		
BI Monitoring	X	
BW Reporting for System Monitoring (System Reporting)	X	To check for existing data in the BW system, use transaction `SMBCO_PD_INFO` In addition, you can display existing data by using transaction `RSA1` to report on existing data. The information providers used for system reporting on ABAP statistical data are contained in information area `0CCMS_STAT`.
Central Job Monitoring	X	
DRM	X	
Interface and Connection Monitoring	X	
Job Monitoring	X	
MAI and Alert INbox	X	
MFM	X	

Application	Report	Manual Procedure
PI Monitoring	X	
Self Diagnosis	X	
System Monitoring	X	
User Experience Monitoring	X	
Test Suite		
BW Reporting for Test Suite	X	In SAP BW, to view all usages of a businesspPartner ID for BW objects, proceed as follows: 1. In the BW System, call transaction `RSA1`. 2. Choose *Modeling -> InfoObjects* and search for the relevant InfoObject (`0SMTB`). 3. In the context menu for each relevant InfoObject, choose *Maintain Master Data*. If the system displays the *No master data maintenance possible* message, this business partner ID is not used in this InfoObject. If the system displays the *<system ID>: Change Master Data of InfoObject 0SMTBP* screen, search for the relevant business partner ID. If the business partner ID is not displayed on the master data screen, this business partner ID is not used in this InfoObject. 4. If you find the business partner ID and want to delete it, proceed as follows: • Select the business partner ID and then choose *Delete Keys -> Save*. • Select *Delete SIDs, Delete Texts and Simulation Mode*. • For the search mode, select one usage per value per object. • Choose *Start*. • In the *Confirm Deletion of SID* dialog box, choose *Yes*. • On the *Master Data used* screen, choose *Details*. The system displays the where-used list for this business partner ID. • If the simulation finished successfully, the business partner ID in the master data of this InfoObject is not used in any other BW objects and can be deleted from the master data of this InfoObject. See section *Simplification of Deletion* for more details.
Partner Test Management	X	
SUT Management	X	
Test Management (Automation)	X	
Test Suite	X	
Infrastructure		

Application	Report	Manual Procedure
Extractor Framework	X	
GPA	X	Data for all scenarios that are part of SAP Solution Manager Configuration are checked, as well as logs and statuses for *Guided Self-Services (GSS)* and *Guided Procedure Authoring (GPA)*.
GSS	X	Data for all scenarios that are part of SAP Solution Manager Configuration are checked, as well as logs and statuses for *Guided Self-Services (GSS)* and *Guided Procedure Authoring (GPA)*.
LMDB	X	
Service Application Connection / S-User Master Data	X	
`SOLMAN_SETUP`	X	Data for all scenarios that are part of SAP Solution Manager Configuration are checked, as well as logs and statuses for *Guided Self-Services (GSS)* and *Guided Procedure Authoring (GPA)*.
Managed System Configuration as part of `SOLMAN_SETUP` transaction		This scenario stores user IDs as part of the configuration data and logs that are handled by the scenario SAP Solution Manager Configuration and Guided Procedure Authoring. Refer to the instructions for reporting on existing data to an identified data subject for the scenario SAP Solution Manager Configuration and Guided Procedure Authoring.
Additional Functions		
Dashboard Builder	X	
Dashboard Framework	X	In addition, use program `DSH_DASHBOARD_ANALYSER` to check content of personal dashboard instances.
KPI Catalog API	X	
Rapid Content Delivery	X	
SAI	X	The `SAI_ADMIN_TOOL` application displays all users who use SAI services. This application can also be used to remove users from SAI services. For more information on deletion, see section *Simplification of Deletion* in this chapter.
URL Generation Framework	X	
Functions relating to Release 7.1		

Application	Report	Manual Procedure
ASU Toolbox	X	Run report `/ASU/SMT_GDPR_INFO_ASU_TOOLBOX` in your managed systems.
ESR / PSLE Self - Service Reporting	X	
Roadmap	X	
SAP Engagement and Service Delivery	X	
SOLAR	X	
Switch Framework	X	
System Monitoring	X	
System Monitoring based on CCMS	X	
Test Management	X	
Transaction SMSY	X	

10.5 Simplifying Deletion of Personal Data

Personal Data Deletion Options

The deletion of personal data might be required and may include a certain retention period of these data in the system before deletion. If retention periods are required and how to specify them is described per function.

In addition, personal data required for customizing/configuration purposes may also be subject to remaining in the system until the end of the business purpose is reached. Specific information is given in the individual chapters per function.

Authorization Mechanims

Deletion is protected by either table protection or application protection. The protection mechanisms in place are mentioned in column *Authorization Mechanism* in the table below.

- *Table Protection using Authorization Groups*: Authorization object `S_TABU_DIS` with the according authorization group is used to protect a groupo of tables. For authorization groups used in SAP Solution Manager, see section *Tighten Table Read and Write Access* in this guide or check transaction `SE54`.
- *Table Protection for Individual Tables*: Authorization object `S_TABU_NAM` is used to protect individual tables.
- *Application Authorizations*: Application authorizations are used to protect the specific function.

Interdependency SAP's Backbone and SAP Solution Manager

SAP's backbone is the leading system in regards to S-user assignments and usage. S-users, which are created, edited, and deleted or expired in the backbone are replicated into the SAP Solution Manager system accordingly.

> → Remember
>
> Update your S-User regularly in the support backbone system.

Business Partner Blocking/Deletion

Business partners can be centrally blocked and deleted. The functionality is used in SAP Solution Manager scenarios. Any specific deviations are described separately per function. For more information, see SAP Note 1825608 Simplified Blocking and Deletion of Central Business Partner.

Deletion with SAP ILM Tool Support

Some SAP Solution Manager scenarios use SAP ILM toolsSupport. For more information, see the following SAP Notes:

- 2354273 Data protection for CRM transaction data
- 2039738 Simplified Data Deletion based on SAP ILM in CRM.

Overview of Functions with Deletion Possibilies with SAP Solution Manager

Below, you find an overview of deletion possibilities for various functions.

Functions

Application	Provided Deletion Functionality	Authorization Mechansim
BPCA		

Application	Provided Deletion Functionality	Authorization Mechansim
BPCA	Manual deletion is in place for all objects storing personal data. Data can be deleted in the following ways for the individual objects: 1. 3PTM Registry: View cluster `AGS_BPCA_3PTM_TOOL_REGISTRY` 2. BPCA Analysis As of Support Package 08, ILM support is available, see also section *SAP ILM Tool Support* ILM Object `SM_BPCA_ANALYSIS` Destruction object `SM_BPCA_ANALYSIS_DESTRUCTION` Manual Deletion *Solution Manager Launchpad -> Test Suite -> Business Process Change Analyzer* 3. Optimization Approach *Solution Manager Launchpad -> Test Suite -> Business Process Change Analyzer -> Details Optimization Approach -> Edit* As of Support Package 08, ILM Support is available, see also section *SAP ILM Tool Support* ILM Object: `SM_BPCA_OA` Destruction object: `SM_BPCA_OA_DESTRUCTION` 4. TBOM *Solution Manager Launchpad -> Project and Process Management -> Solution Documentation -> List View -> Restrict to object type TBOM* 5. TBOM History As of Support Package 08, ILM support is available, see also section *SAP ILM Tool Support* ILM Object: `SM_BPCA_TBOM_HISTORY` Destruction object: `SM_BPCA_TBOM_HIST_DESTRUCTION` Manual Deletion: TBOM history logs are deleted when the corresponding executables are deleted in *Solution Documentation*. 6. TBOM Classification View maintenance for table `AGS_TBOM_CLASS_C`. 7. TBOM Criticality *Solution Manager Launchpad -> Test Suite -> Administration Change Impact Analysis -> Administration Change Impact Analysis -> Maintain TBOM Criticality Table* 8. TBOM Filter *Solution Manager Launchpad -> Test Suite -> Administration Change Impact Analysis -> Administration Change Impact Analysis -> Maintain TBOM Filter Table* 9. TBOM Options View maintenance for view `AGS_BPCA_ACTVFCT`	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_SM_BPCA_*_ALL.`

Application	Provided Deletion Functionality	Authorization Mechansim
	10. TBOM Work Item As of Support Package 08, ILM support is available. See also section *SAP ILM Tool Support* ILM Object: `SM_BPCA_WORK_ITEM` Destruction object: `SM_BPCA_WI_DESTRUCTION` Manual deletion: *Solution Manager Launchpad -> Test Suite -> My Tasks TBOM Work List -> All Work Items* 11. TBOM Work Item Configuration View maintenance for view `V_AGS_TBWI_CRM_C` The following objects exist in the managed systems where BPCA functions are used: 1. TBOM options in managed system View maintenance for the `VTBOM_FCT_SWITCH` 2. BPCA object and key mapping in managed systems View cluster `BPCA_TR_RT_MAPP` 3. Exceptions for table key recording view maintenance for view `VBPCA_TABK_EXC`	
BPO		
BPCC	Run report `E2EEM_HOUSEKEEPING_REPORT`. You can use the BPCC configuration tab *Housekeeping*. Here, you can see the status of the housekeeping job and define for each category and subcategory when the data stored should be deleted. Separately, the IPA store can be configured to be deleted after a specified number of days. Here are the detailed steps to delete process instances: 1. Open the SAP Solution Manager launchpad. 2. Open tile *Configuration – Business Process Completeness Check* in area *Data Consistency Management*. 3. Change to tab *Housekeeping*. 4. For the category and sub-category you would like to delete, set the *No of Days* to keep data to 1. 5. Check that processing status is not enabled. 6. Save your changes.	The deletion is protected by authorization object `S_TABU_NAM` in role `SAP_OP_DSWP_BPM`.

Application	Provided Deletion Functionality	Authorization Mechansim
BP Improvement	Run report `GDPR_BPIMP_CLEAR_ALL`. Historical key figure data containing personal data in BPA TwinCubes (BW) is handled by an automatic housekeeping process. The data retention period for this information provider can be maintained as follows for the business process improvement Administration scenario: 1. Open the SAP Solution Manager launchpad. 2. Navigate to the *Business Process Improvement* launchpad group. 3. Choose *Business Process Improvement: Administration*. 4. Select the *BW Setup* tab. 5. Maintain the data retention period. You can delete data from individual BPA TwinCubes at any time by executing the `AGS_BPA_RI_DATA_DELETE`. In addition, you can delete personal data for the following functions: **Business process analytics** To delete key figures, proceed as follows: 1. Open the SAP Solution Manager launchpad. 2. Navigate to the *Business Process Improvement* launchpad group. 3. Choose *Solution Documentation: Monitoring Configuration*. 4. Select the appropriate solution. 5. Select *Analytics Library* and look for the key figure. 6. Select the key figure and delete it. To delete key figure variants or categories, proceed as follows: 1. Open the SAP Solution Manager launchpad. 2. Navigate to the *Business Process Improvement* launchpad group. 3. Choose *Business Process Analytics: Classic*. 4. Select the *Key Figure Variants* tab. 5. Choose *Manage Variant Categories and Variants*. 6. Choose *Category Maintenance or Variant Maintenance*. 7. Select the relevant variant category or variant and delete it. **Business process operations dashboards** If you want to delete objects that are no longer needed due to business reasons, proceed as follows: 1. Open the SAP Solution Manager launchpad. 2. Navigate to the *Business Process Improvement* launchpad group.	The deletion is protected by authorization object `SM_BPM_ACF` for activity `ACTVT 06` delete in role `SAP_SM_BPOIMP_ALL`.

Application	Provided Deletion Functionality	Authorization Mechansim
	3. Choose *Configuration: Dashboards Business Process Operations*. 4. Select the relevant tab *Analytical Key Figure Instance, Panel, Dashboard*. 5. Delete the objects that are no longer needed. **Progress management boards and maintenance tool persistence browser** To delete user information, logs, and objects, execute the `AGS_BPA_PERSISTENCE_REORG` report. **Dependency diagrams (including setup application)** To delete user information, logs, and objects, execute the `AGS_BPM_RI_PERSISTENCE_REORG` report. **BPO reporting infrastructure maintenance (especially Usage Analysis)** The usage analysis function has a data retention period after which all logged personal data is reorganized. To set the data retention period, proceed as follows: 1. Open the SAP Solution Manager launchpad. 2. Navigate to the *Business Process Improvement* launchpad group. 3. Choose *Business Process Improvement: Administration*. 4. Select the *Usage Analysis* tab. 5. Choose *Display Settings*. 6. Set the data retention period as required.	

Application	Provided Deletion Functionality	Authorization Mechansim
Business Process Monitoring (BP Mon) and Alert Inbox	**Business Process Monitoring application** Up to and including SAP Solution Manager 7.2 SP04, the Business Process Monitoring application and Business Process Operations Alert Inbox logged the last solution context used by a user accessing these applications. As of SAP Solution Manager 7.2 SP05, a different logging mechanism is used. You can delete the context that was persisted up to SAP Solution Manager 7.2 SP04 by upgrading to SAP Solution Manager 7.2 SP05 or higher and by executing the `AGS_BPM_ALREP_RESET_DEFAULTS` report. For the user name, enter asterisk * and select all three deletion options. As of SAP Solution Manager 7.2 SP05, Business Process Monitoring app logs the last *Solution Context* that an end user used to access the Business Process Monitoring application, the Business Process Operations Alert Inbox, the Job Monitoring application, and OCC Alert Reporting. To delete the *Persisted Solution Context* for a user for each application, execute the `E2E_BPM_VARIANT_CLEANUP` report. Mass deletion is possible. To delete *Notification Groups*, access the *Business Process Operations Object Administration*. Access the configuration of any Business Process Monitoring object. Select the *Notifications* tab. On the righthand side of the screen, open the *Notification Groups* maintenance. Choose *Delete all*. **Business Process Monitoring configuration** In the Business Process Monitoring configuration, the creation user and change user of Business Process Monitoring objects is persisted. This user information is deleted when you delete the relevant Business Process Monitoring object. You can do this in the *Business Process Operations Object Administration*. Select the *Overview* tab and filter for Business Process Monitoring objects where the monitoring ID is not empty. Select the Business Process Monitoring objects that you want to delete and then choose *Deletion*.	• The deletion is protected by authorization object `SM_MOAL_OC` activity `ACTVT 06` delete for *Monitoring Object Type* `BP_MON` in role `SAP_OP_DSWP_BPM`. **i Note** Since deleting a BPMon object also means deleting the object in the solution documentation, the respective authorization for deleting objects in the solution documentation also needs to be assigned to the user executing the deletion. • The deletion of the persistence of personalization data in Business Process Monitoring via report `E2E_BPM_VARIANT_CLEANUP` is governed via authorization object `SM_MOAL_TC` with activity `ACTVT 02` change for Monitoring Object Types in role `SAP_OP_DSWP_BPM`: • `BP_MON` to delete personalization for the BPMon application • `INBOX` to delete personalization for the BPO Alert Inbox • `JOB_MON` to delete personalization for the Job Monitoring application

Application	Provided Deletion Functionality	Authorization Mechansim
CDC	Run report `DSWP_CDC_DELETE_PERS_DATA. It deletes data which is not anymore needed for the group type definitions.` **! Restriction** Relevant as of SP08. You also have manual deletion options: • Comparison results Delete comparison results by executing the `DSWP_CDC_COMPARE_REORG` program. **i Note** SAP recommends that you execute this program on a regular basis to delete outdated results. • Comparison groups 1. Start CDC. 2. In the comparison group dropdown list, select *Comparison Groups Only*. 3. • To delete individual comparison groups: Select the relevant rows, choose *Delete*, and then confirm your selection. • To delete all comparison groups: Select all rows, choose *Delete*, and then confirm your selection. • Comparison Group Types Comparison group types can only be deleted individually. 1. To delete a comparison group type, start *CDC*. 2. Select the *Comparison Group* tab. 3. Select the group type that you want to delete and then choose *Delete Group Type*. • Comparisons 1. To delete comparisons, start *CDC*. 2. In the *Comparison Group* dropdown list, select *Comparisons Only*. 3. • To delete individual comparisons: Select the relevant rows, choose *Delete*, and then confirm your selection. • To delete all comparisons: Select all rows, choose *Delete*, and then confirm your selection. • Data Models A deletion of a comparison does not automatically result in the deletion of the underlying data model as the data model might be relevant for other or future comparisons. 1. To delete data models, start *CDC*.	• In role `SAP_CDC_INSTANCE_CREATOR` • `SM_CDC_OBJ` with `ACTVT 06` (delete) protects *Data Model* and *Data Model Change Documents*. • `SM_CDC_INS` with `ACTVT 06` (delete) protects *Comparison* and *Comparison Change Documents*. • `SM_CDC_INS` with `ACTVT 65` (reorganize) protects *Comparison Results*. • `SM_CDC_GRP` with `ACTVT 06` (delete) to protect *Comparsion Groups*.

Application	Provided Deletion Functionality	Authorization Mechansim
	2. Choose *Mass processing*. 3. On the next screen, choose *Delete Data Models* and then choose *Continue*. 4. In the first step of the guided procedure, select the data models that you want to delete and then choose *Next*. 5. If the correct data models are shown on the next screen, choose *Delete Data Models*. 6. A popup informs you if deletion was successful. • Change Documents To delete change documents, execute the `DSWP_CDC_SHOW_CHANGEDOCS` program.	
Interface Documentation	A manual deletion of interfaces and interface details is possible. You can search all interfaces for the person responsible in the *Solution Documentation* application and delete them. Follow the steps to delete process instances: 1. Open the *Solution Documentation* using transaction `SOLDOC`. 2. Navigate to the *Interface Details* element. 3. Select the element and select *Delete*.	
Job Health Check	To delete data for a specific user from the `0SM_JSM*` info cubes, proceed as follows: 1. In the BW system, call transaction `RSA1`. 2. Select the cube. 3. In the context menu, choose *Planning-Specific Properties -> Change Real-Time Load Behaviour ...* . 4. Switch to Real-Time Data Target Can Be Loaded with Data; Planning not allowed. 5. Do not select a transport. 6. Choose *Manage -> Contents -> Delete Selection -> Deletion Selection*s. 7. Select the ID of the JSM job scheduling user whose data you want to remove from the system. 8. Choose *Execute*. 9. Switch the cube back to *Planning Mode*.	The deletion is protected by authorization object `S_TABU_DIS` with table authorization group `SMJM` in role `SAP_OP_DSWP_BPM`.

Application	Provided Deletion Functionality	Authorization Mechansim
OCC Alert Reporting	Up to and including SAP Solution Manager 7.2 SP04, the OCC Alert Reporting function logged the last solution context used by a user accessing OCC Alert Reporting. As of SAP Solution Manager 7.2 SP05, a different logging mechanism is used. You can delete the context persisted up to SAP Solution Manager 7.2 SP04 by upgrading to SAP Solution Manager 7.2 SP05 or higher, and by executing the `AGS_BPM_ALREP_RESET_DEFAULTS` report. For the user name, enter asterisk * and select all three deletion options. As of SAP Solution Manager 7.2 SP05 Business Process Monitoring logs the last *Solution Context* that an end user used to access the Business Process Monitoring application, the Business Process Operations Alert Inbox, the Job Monitoring application, and OCC Alert Reporting. To delete the persisted solution context for a user for each application, execute the `E2E_BPM_VARIANT_CLEANUP` report. Mass deletion is possible.	The deletion of the persistence of personalization data in OCC Alert Reporting via report `AGS_BPM_ALREP_RESET_DEFAULTS` and via report `E2E_BPM_VARIANT_CLEANUP` (both reports are necessary) is governed via authorization object `SM_MOAL_TC` with activity `ACTVT 02` change for Monitoring Object Type `REPORTING` (role: `SAP_OP_DSWP_BPM`).
Change Control Management		

Application	Provided Deletion Functionality	Authorization Mechansim
BW Reporting: ITSM and Change Request Management	To delete information concerning business partners that are not only blocked but are also no longer relevant for reporting, proceed as follows: Provided Deletion Functionality: 1. Run program report `ITSM_REP_GDPR_STOP_WLI` in SAP Solution Manager. 2. Wait for 10 minutes. 3. Run program report `ESR_GDPR_DELETE_USER_INFO` in SAP Solution Manager. 4. Run program report `ITSM_REP_DELETE_BW_DATA_710` in SAP Solution Manager BW. 5. Run program report `SMT_REP_DELETE_BW_DATA` in SAP Solution Manager BW. 6. Run program report `ITSM_REP_DELETE_BW_DATA` in SAP Solution Manager BW. 7. Perform re-initialization for ITSM BW report via transaction `SOLMAN_SETUP` -> *IT Service Management -> 4.1 Define Extraction Settings*. Make sure the *Initialize* check box is selected. 8. Perform re-initialization for ChaRM BW report via transaction `SOLMAN_SETUP` -> *Change Control Management -> Change Request Management -> 6.1 BW Reporting: Define Extraction Settings*. Make sure the check box *Initialize* is selected. 9. Perform re-initialization for test suite BW report via transaction `SOLMAN_SETUP` -> *Test Suite -> Test Suite Preparation -> Step 2.5 Analytics*. Make sure the *Initialize* check box is selected.	
ChaRM	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. Destruction objects: - `AI_CRM_CM_DESTRUCT_OLD_DATA`: For deletion of obsolete table data which must be performed only once. - `AI_CRM_CM_DESTRUCT_REP_TRACK`: For deletion of reporting and transport tracking data. In addition, ILM processes for blocking and deletion of business partners are used: - Business partners `CA_BUPA`	*SAP ILM Tool Support*

Application	Provided Deletion Functionality	Authorization Mechansim
Configuration Validation	The CCDB deletes by default configuration data including those data that hold user IDs after 36 months. This setting is changeable and can be adjusted in CCDB itself. The cross selection using the *Display* button generates a list of configuration stores. It is possible to mark one configuration store, several, or all configuration stores of the list and choose *Delete Selected Stores*. This function can run online or in background mode, which is preferred if many configuration stores are marked. The deletion of the data is done by a daily job. The information whether this job is running successfully is displayed on tab *Status*, subtab *General*. In *CCDB Infrastructure*, the status of administration tasks should have a green *Successful* rating. Detail logs for the housekeeping task are displayed in tab *Exception* using the Log Type filter *Admin*. Task: Housekeeping. The deletion removes the configuration store and its data. **i Note** The next extractor run loads the configuration data and recreates the configuration store. This means that, as long as the user ID in question is stored in the managed system, the user ID is stored again. To avoid this, delete the user ID in question in the managed system before the deletion in the CCDB is performed. Another approach is to remove the managed system from CCDB completely with the effect that no data is available in the CCDB. If you want to delete all data which is available in CCDB related to a technical system and avoid that it is loaded again, the first step is to delete the extractors. To delete a technical system in CCDB select tab *Status* and then *Technical Systems*. Mark the system and click the *Delete all Stores* button. This operation is performed online or in background depending on the selected option. In most cases, the background deletion is the recommended option because it may take several minutes. Subsequently, delete the technical system and its stores in the CCDB administration. The CCDB administration can be started via *Solution Manager Launchpad → Solution Manager Administration → Configuration Change Database Store Administration* tile. **i Note** If you want to start a new history, do not delete the extractors. As a result, the technical system appears again in the CCDB administration after the next extractor run. On tab *Configuration*, the *Information* button opens a dialog that gives you some background information about the CCDB data retention. The configuration stores of type *Event* are handled	The deletion is protected by authorization objects SM_CCDB* in role SAP_CV_ALL.

Application	Provided Deletion Functionality	Authorization Mechansim
	separately as these can have a high number of records, because new items (events) are extracted and stored. **Example** A prominent example of an event store is the store for the transport requests `ABAP_TRANSPORTS`. For any other stores, the first snapshot is stored and afterwards only information about changes are stored. Thus, these stores are not supposed to hold lots of records. For more information on deletion, see section *Simplified Deletion*.	
ITSM	The SAP ILM tool is used. See also section *SAP ILM Tool Support*. Destruction objects • Incident: `CRM_INCDNT` • Problem: `CRM_PROBLM` • Service Request: `CRM_INCDNT` In addition, ILM processes for blocking and deletion of business partners are typically used in conjunction with ITSM scenarios: • Business partners `CA_BUPA`	*SAP ILM Tool Support*
License Management	Run report `AGSSISE_DEL_LOGS_GP_SETUP` to delete log entries which are older than a given date.	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_SM_LICMAN_ALL.`
QGM	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. Destruction objects: • `AI_CRM_CM_DESTRUCT_OLD_DATA`: For deletion of obsolete table data which must be performed only once. • `AI_CRM_CM_DESTRUCT_REP_TRACK`: For deletion of reporting and transport tracking data. In addition, ILM processes for blocking and deletion of business partners are used: • Business partners: `CA_BUPA`	*SAP ILM Tool Support*
Requirements Management	See section *Archiving of Objects*	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_ITPPM_ALL`.

Application	Provided Deletion Functionality	Authorization Mechansim
System Recommendation	As soon as a technical system is not managed by SAP Solution Manager anymore and does not send data to SAP Solution Manager via LMDB SAP recommends to decommission the system in transaction `SOLMAN_SETUP` *Managed System Configuration*. In addition to the activities proposed by this procedure, you can delete any remaining data about such a system using report `AGSNO_RPT_CLEANUP_SYSTEMS`. **i Note** After a defined number of years depending on your specific retention period, the data of the tables which contain personal data is anonymized or deleted, or the data sets are archived.	The deletion is protected by authorization object `SM_FUNCS` with `ACTVT 06` (delete) in role `SAP_SYSREC_ALL`. **i Note** Any data in configuration of transaction `SOLMAN_SETUP` is protected by authorization object `SM_SETUP` accordingly.
CCM		
CCM	In the application, you can use the *Delete Owner* button to allow a user to delete selected owners together with all assignments to a custom code object.	The deletion is protected by authorization object `SM_TABU_DIS` in role `SAP_CCLM_ALL`.
DVM		
DVM	Once a solution is deleted, DVM-related data gets deleted as well. For more information, see SAP Note 264781.	The deletion is protected by authorization objects `SM_DVM` with `ACTVT 06` and `SM_DVM_APP` with `ACTVT 06`.
Job Management		
Job Management	Run report `AI_JOB_MANAGEMENT`. Tables are protected by authorization group `SMAL` and the application specific authorization objects. For more information on the authorizations, see the corresponding section for *Job Management* in the *Application - Specific Security Guide*.	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_SM_SCHEDULER_ADMIN`.
Process Management		
CDMC	Run report `CNVCDMC_GDPR_DELETE`. Deletion is protected by authorization object `S_CDMC`.	The deletion is protected by authorization object `S_CDMC`.
Customizing Distribution and Scout	Customizing group or setup can be deleted from within the applications.	The deletion is protected by `S_TABU_DIS`.
JSON file (Process Document Viewer)	Personal data exists in the *Process Portal* application. To delete the user IDs, delete the extracted ZIP file.	

Application	Provided Deletion Functionality	Authorization Mechansim
Solution Documentation	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. Destruction objects: • Destruction of SAP Solution Documentation documents: Delete unused documents depending on a retention period `SMD_DOC_HISTORY_DESTRUCTION` • Destruction of Content Activation Data: `SMMIG_CONT_ACT_DESTRUCTION` • Destruction of solution history data for deleted nodes: `SMUD_HISTORY_DESTRUCTION` • Destruction of Solution Documentation layouts: `SMUD_LAYOUT_DESTRUCTION` • Destruction of Solution Documentation reports: `SMUD_REPORT_DESTRUCTION` In addition, ILM processes for blocking and deletion of business partners are used: • Business partners: `CA_BUPA` Business partners are used in various parts of Solution Documentation. For blocked business partners, only the ID is displayed but no other personal data. The deletion of all data including personal data related to Solution Documentation is supported by manual deletion functionality. **KW documents** Personal data that is stored in KW documents which can be found using the embedded search. Such documents can then be deleted manually. See also SAP Note 2625551 Delete Unused Documents. **Personalization** If a user is deleted, all corresponding personalization data related to Solution Documentation is deleted. This includes private entities such as scopes, reports, and layouts. **Transaction** `SM_CLEANUP` The following programs are provided in this transaction: • Delete documents for deleted solutions and documents without solution assignment • Solution Documentation: Clean up library generation data • Solution Documentation: Delete personalization data for all deleted users Check the application log in transaction `SLG1` for object `SM_CLEANUP`.	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_SM_SL_ADMIN` and authorization object `SM_SDOCADM` with `ACTVT 06`.

Application	Provided Deletion Functionality	Authorization Mechansim
	Solutions In the *Solution Administration* application, an entire solution can be deleted. If a solution is deleted, all personal data in all versions of the solution is deleted too. The deletion of a solution includes also the deletion of all Knowledge Warehouse (KW) documents (see above) with all versions in the solution-specific folder. In addition, instead of deleting an entire solution, all unused documents that are no longer assigned to the solution can be deleted by executing the `SOLMAN_UNUSED_DOCUMENTS` report. This report is available with SAP Note 2625551. **Cross-solution entities** Most data in Solution Documentation is organized by solutions. In addition, there are some cross-solution entities: reports, layouts, and document types. For all these entities, there is a manual deletion function available. **Data related to content activation** All data related to Solution Documentation content activation can be deleted by executing the `RSMMIG_GP1_GP2_DATA_DELETE` report.	
Solution Documentation Graphical Editor Diagram Entities	Since graphical editor objects are solution specific, deletion of these objects is related to the deletion of *Solution Documentation* as explained in the Solution Documentation section.	
Project Management		
ITPPM	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. The Customizing log can be deleted at the end of purpose using the ILM object. Destruction object • Customizing Log: `SMCP_CUSTLOG_DESTRUCT` In addition, ILM processes for blocking and deletion of business partners are used: • Business partners `CA_BUPA`	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_ITPPM_ALL` and *SAP ILM Tool Support*.
RCA		

Application	Provided Deletion Functionality	Authorization Mechansim
Agent Administration	Run transaction `SM_CLEANUP` to delete user data. Check the application log in transaction `SLG1` for object `SM_CLEANUP`. Manually, data can be deleted by using the function *Clear History* in the *Agent Administration – Maintenance Mode History - Clear History*.	not applicable
E2E TA Housekeeping: Trace Analysis	Once a trace has been recorded and uploaded it can be either deleted manually, or it will be deleted automatically by a housekeeping job after a configurable retention time.	not applicable
Exception Management	Housekeeping settings are available in the regular *Exception Management* configuration area, which is available in *Solution Manager Configuration* using transaction `SOLMAN_SETUP` under section *Application Operations*.	The deletion is protected by authorization object `SM_SETUP` with `ACTVT 02` (change) in role `SAP_EM_COCKPIT`.
SAP Engagement and Service Delivery		
CSA	Report `RDSVASACSA_PERS_DATA` is provided to delete all personal data stored.	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_OP_DSWP_CSA`.
DSA / Web DSA	To delete data from service sessions, execute the `RDSMOPREDUCEDATA` report. This report has various selection criteria such as system IDs, dates, and session packages, and can be used for mass deletion.	
EWA Settings	To delete **configuration data** for SAP EarlyWatch Alert Management, you can use the following reports: • `AGSSISE_DEL_LOGS_GP_SETUP` for log and status • `PD_EWA_OLD_DATA_CLEANUP` for old EWA settings data Additionally, you have to manually delete the **settings and recipents**. To **manage favorites** in the report viewer, run report `PD_EWA_VIEWER_FAV_CLEANUP`.	The deletion is protected by authorization object `SM_SETUP` with `ACTVT 02` (change) in role `SAP_SETUP_BASIC`.
Issue Management	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. Destruction objects • Issue or top issue: `CRM_SERORD` • Task: `CRM_ACT_ON` In addition, ILM processes for blocking and deletion of business partners are used: • Business partners `CA_BUPA`	*SAP ILM Tool Support*

Application	Provided Deletion Functionality	Authorization Mechansim
Service Delivery	Use report `RDSMOPREDUCEDATA` to delete data with complex selection criterias. **Personalization** Use report `RESD_PERSONAL_DATA_DELETION` to delete personalization data for a user ID. **Service Request** The SAP ILM tool is used, see also section *SAP ILM Tool Support*. Destruction object • Support request `CRM_SERORD` In addition, ILM processes for blocking and deletion of business partners are used: • Business partners `CA_BUPA`	*SAP ILM Tool Support* The deletion of user IDs is protected by authorization object `S_TABU_DIS`.
Service Content Update	Use report `RAGS_SCU_DELETE_DELTA_LOGS` to delete all entries in the delta log.	The deletion is protected by authorization object `SM_CNT_UPD`, with activity `ACTVT 30` for content update `CONT_UPD` in role `SAP_SETUP_BASIC`.
SDCCN	In each managed system where you want to remove the data related to the service data download, execute the `/BDL/HANDLE_OLD_RECORDS` report. The deletion is protected by authorization objects `S_SDCC` and `S_SDCCN` with `ADMIN` and `WRITE` permissions. See SAP Note 2643825 - Deletion of personal data stored by service data download (transaction SDCCN)	The deletion is protected by authorization objects `S_SDCC` and `S_SDCCN` with `ADMIN` and `WRITE` permissions in role `SAP_SDCCN_ALL`.
Value Based Delivery Dashboard	The SAP ILM support tool is used. See section on *Archiving of Objects* for more information.	*SAP ILM Tool Support*
SAP Solution Manager Administration		
UOCShell Personalization	A background job `SM:TECHMON_UI5_CONFIG_CLEANUP` with report `TECHMON_UI5_CONFIG_CLEANUP` is scheduled in transaction `SOLMAN_SETUP` *Configuration > Basic Configuration > Step 2 : Scheduled Jobs*. Periodicity: weekly. The job removes all system and application monitoring configuration entries of non-existing users.	The deletion is protected by authorization object `S_TABU_NAM` in role `SAP_SM_BATCH`.
SEA		

Application	Provided Deletion Functionality	Authorization Mechansim
SEA	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. ILM Object: `SM_SEA_DESTRUCTION` Destruction Object: `SM_SEA_DESTRUCTION` Manual deletion is in place for all objects storing personal data. To access the application, choose *Solution Manager Launchpad → Test Suite → Scope and Effort Analyzer*. See SAP Note 2421158 - SEA - Deletion of personal data stored by ST.	Manual deletion is protected by authorization object `S_TABU_DIS` in role `SAP_SEA_ALL`.
Technical Administration		
CNM	To delete user IDs, execute the `CNM_USER_INFO_DEL` report. To delete all recipients created before a specific date and time, execute the `CNM_USER_INFO_DEL_F_DATE` report. The LDAP user (used for connection to LDAP server to fetch DL details) is maintained in the central notification management application. This can be accessed via the *Configuration* tile (SMS and LDAP Servers) under the *TechnicalAdministration* catalog. If needed, you can remove the user from the LDAP server configuration.	The deletion is protected by authorization object `SM_NOTI_TA` with `ACTVT 06` (delete) in role `SAP_NOTIF_ADMIN`.
IT Calendar and Work Mode Management /IT Events	To delete personal data, execute the `ITC_USER_INFO_HANDLING` report.	The deletion is protected by authorization object `SM_WMM_AUT` with `ACTVT 06` (delete) in role `SAP_SM_WMM_ALL`.
IT Task Management and Planning	IT task management uses standard CRM functionality. A CRM task is created and assigned to business partners. Apart from the detection and deletion functionality supported by CRM, the user information in the IT task plan can be taken care of by using report `TPA_USER_INFO_HANDLING`.	The deletion is protected by authorization object `SM_TP_AUTH` with `ACTVT 06` (delete) in role `SAP_TASK_PLANNING_ALL`.
SAM	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. Destruction object is `SAM_DESTRUCTION` with the following selection fields: • Entity ID • Service ID **Note** The retention period uses the valid to timestamp of service definitions. All service availability management data that is equal to the valid to timestamp + 1 day is deleted. In addition, ILM processes for blocking and deletion of business partners are used: • Business partners `CA_BUPA`	*SAP ILM Tool Support*

Application	Provided Deletion Functionality	Authorization Mechansim
Technical Monitoring		
BI Monitoring	Run report `AC_BIMON_DELETE_PERSONAL_DATA`.	The deletion is protected by authorization object `SM_MOAL_TC` with `ACTVT 02` (change) in role `SAP_SM_BIM_LEVEL02`.
BW Reporting for System Monitoring (System Reporting)	Run report `CCMSBI_DELETE`. For more information, see SAP Note 2640144 - Identifying and deletion of personal data stored by ST-BCO. Data in information cubes is subject to automatic reorganization after lifetime is reached. Lifetime is configured in the SAP Solution Manager Configuration. All other data can be deleted when reporting for system monitoring is no longer used.	The deletion is protected by authorization object `S_TABU_NAM` in role `SAP_SETUP_BASIC`.
Central Job Overview	Run report `AC_CJO_DELETE_PERSONAL_DATA`.	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_SM_CENTRAL_JOB_OVERVIEW`.
Data Readiness Monitoring	Execute the `AC_DRM_DELETE_PERSONAL_DATA` report.	The deletion is protected by authorization object `SM_MOAL_TC` with `ACTVT 02` (change) in role `SAP_SM_BIM_LEVEL02`.
Interface and Connection Monitoring	The user ID associated to an interface channel can be deleted together with the interface channel itself. The delete function is available in *SAP Solution Manager Configuration* launchpad (transaction `SOLMAN_SETUP`) under *Application Operations → Integration Monitoring → Interfaces and Connections → Step 5.2 Configuration* of the guided procedure.	
Job Monitoring	`Run report AC_JOBMON_DELETE_PERSONAL_DATA`.	The deletion is protected by authorization object `SM_MOAL_TC` with `ACTVT 02` (change) in role `SAP_SM_JMON_LEVEL02`.

Application	Provided Deletion Functionality	Authorization Mechansim
MAI and Alert Inbox	**Configuration** MAI stores configuration which is used by the business. Configurations can be retained until they serve the business purpose. After the configuration is no longer used, the possibility to delete the configuration is provided in the MAI application. The template created can be deleted from the template maintenance tool from where it is created. Run reports: • `ACR_DELETE_UNUSED_CUSTOM_TMPL` - Delete unassigned custom templates • `ACR_DELETE_UNUSED_ALERT_CONSUM` - Delete unassigned alert consumer variants • `ACC_DELETE_OBSOLETE_USERS` - Delete obsolete user data from Alert Personalization Settings **Monitoring** Monitoring for a system can be deactivated by decommission monitoring. **Alerts** Housekeeping program `E2EA_HOUSEKEEPING` scheduled as `SAP_ALERT_HOUSEKEEPING` job deletes as per configured intervals. It can be used to delete alerts that are no longer relevant for business. With the alert deletion, the information of users who was or were assigned as processors or took any action on those alerts are also deleted.	The deletion is protected by authorization object `S_TABU_DIS` in role `SAP_SETUP_BASIC`.
MFM	**Payload and EDI attributes** are deleted by the following housekeeping jobs: • `E2EEM_HOUSE_KEEPING` • `E2EEM_HOUSE_KEEPING_PP` The **payload information** collected from the managed systems can contain personal information. The data is deleted as part of the housekeeping process within the application. **Contact persons** maintained in the message flow configuration and filter variants for user IDs can be deleted by executing the `E2EE_MFMON_DELETE_PD` report.	The deletion is protected by authorization object `SM_MOAL_TC` with `ACTVT 02` (change) and `S_TABU_NAM` in role `SAP_SM_MFM_LEVEL02` .
PI Monitoring	Filter criteria can be deleted manually in the application by the user who created the filter. Additionally, you can delete the filters related to personal data (user ID) by executing the `AC_PIMON_DELETE_PD` report.	The deletion is protected by authorization object `SM_MOAL_TC` with `ACTVT 02` (change) in role `SAP_SM_PIM_LEVEL02`.

Application	Provided Deletion Functionality	Authorization Mechansim
Self Diagnosis	Run report `SD_DELETE_PD`.	The deletion is protected by authorization object `D_SM_S_DIA` with `ACTVT 06` (delete) in role `SAP_SETUP_BASIC`.
System Monitoring (Mobile Optimized SAP Fiori App)	While a user is still active, they can remove systems from their favorites, so that their personal data is deleted from the application. In addition, to delete data for a specific user, execute the `TECH_SYSMON_APP_USER_DATA_DEL` report. **i Note** Application System Monitoring (Mobile App based on Android, discontinued): To delete data for a specific user, execute the `TECH_SYSMON_OLD_USER_DATA_DEL` report.	The deletion is protected by authorization object `S_TABU_NAM` in role `SAP_SM_SYM_LEVEL02.`

Application	Provided Deletion Functionality	Authorization Mechansim
User Experience Monitoring	**Scenario Definition (Scripts)** You can delete scripts in transaction `SOLMAN_SETUP`. If a script is no more required, it can be manually deleted. Proceed as follows: *Solution Manager Launchpad → Configuration All Scenarios tile → Application Operations → User Experience Monitoring → Step 3.3 Assign Script*. Choose the script to delete and press the *Delete* button. **Any personal data within a recorded script** Since the content of a recorded script depends on what has been recorded by a user, any personal data can be recorded. To make sure that personal data in such scripts is correctly removed, SAP recommends you to do this when you parameter the scripts and before you upload them to the *User Experience Monitoring* repository. 1. In the *Script Editor*, go to *EEM Navigator* panel and select the script you like to verify. 2. In the context menu, choose *Explore in File System*. The system opens the script folder in the editor workspace. 3. In the content of the files and sub-folders, you can search for data which you do not want to keep in clear text. 4. Replace the content as follows: • If you find such data in the recordings.meta folders or in the replaying.meta folders, replace the text with a dummy value directly in the file. • If you find such data in the root folder of the script such as in script.http.xml, ConfigScript.xml, and so on, edit the script in the *Editor* and replace the text with an UXMon variable of type *secure*. See the SCN Wiki on how to declare UXMon variable in the Editor • If there is a text which you do not want to keep in clear text in your script data, you can store this text in a UXMon secure variable, or you can replace it with a dummy value. **Configuration settings** Execute the `UXMON_GDPR_DELETE` report to delete user configuration settings (extra customization configuration).	The deletion is protected by authorization object `S_TABU_NAM` in role `SAP_SM_EEM_CONF`.
Test Suite		

Application	Provided Deletion Functionality	Authorization Mechansim
BW Reporting Test Suite	Proceed as follows: Provided Deletion Functionality: 1. Run program report `ITSM_REP_GDPR_STOP_WLI` in Solution Manager. 2. Wait for 10 minutes. 3. Run program report `ESR_GDPR_DELETE_USER_INFO` in Solution Manager. 4. Run program report `ITSM_REP_DELETE_BW_DATA_710` in Solution Manager BW. 5. Run program report `SMT_REP_DELETE_BW_DATA` in Solution Manager BW. 6. Run program report `ITSM_REP_DELETE_BW_DATA` in Solution Manager BW. 7. Perform re-initialization for ITSM BW Report via transaction `SOLMAN_SETUP` *-> IT Service Management -> 4.1 Define Extraction Settings*. Make sure, the check box *Initialize* is selected. 8. Perform re-initialization for ChaRM BW Report via transaction `SOLMAN_SETUP` *-> Change Control Management -> Change Request Management -> 6.1 BW Reporting: Define Extraction Settings*. Make sure, the check box *Initialize* is selected. 9. Perform re-initialization for Test Suite BW Report via transaction `SOLMAN_SETUP` *-> Test Suite -> Test Suite Preparation -> Step 2.5 Analytics*. Make sure, the check box *Initialize* is selected.	
Partner Test Management	Execute the `AGS_ADAPTER_PD_DELETE` report.	The deletion is protected by authorization object `SM_TS_PTM` with `ACTVT 01` (create/generate) in role `SAP_TMT_ADMIN`.
Test Automation	The SAP ILM tool is used, see also section *SAP ILM Tool Support*. The objects for the ILM destruction report are: • Object: `SM_CBTA` • The destruction object is `SM_CBTA_DESTRUCTION`. • The Data Destination Program is `SM_CBTA_DESTRUCTION` Minimum retention time of one year is lowest limit and can be individually extended.	*SAP ILM Tool Support* In addition, the deletion of user IDs is protected by auhorization object `SM_SUTMNGT` with `ACTVT 23` (maintain) in role `SAP_SM_CBTA_ADMIN`.

Application	Provided Deletion Functionality	Authorization Mechansim
Test Suite	The SAP ILM tool is used, see section *Archiving of Objects*. The destruction of objects is optional. Run transaction `SM_CLEANUP` to delete: • Personalization data for all deleted users • Control table for deleted test scripts Check the application log in transaction `SLG1` for object `SM_CLEANUP`. Manual deletion is in place for all objects that store personal data. In the Test Management application, data can be deleted in the following ways for individual objects via *SAP Solution Manager Launchpad → Test Suite → Test Plan Management*: • Test plan: In the Test Plan Management view, select the test plans that you want to delete, and then choose *Test Plan → Delete*. This also deletes all related data (test packages, test sequences, test status, test notes, and test results). • Test sequence: In the Test Plan Management view, select the test plan with test sequences that you want to delete and then choose *Test Plan → Edit*. In the Test Plan Maintenance application, select the *Test Sequences* tab. Select the test sequences that you want to delete and then choose *Test Sequence → Delete*. Save your changes. This also deletes all data related to the deleted test sequences (test packages which reference to the test sequence, test status, test notes, and test results). • Test package: In the Test Plan Management view, select the test plan with test packages that you want to delete, and choose *Test Plan → Edit*. In the Test Plan Maintenance application, select the *Test Packages* tab. Select the test packages that you want to delete, and then choose *Test Package → Delete*. Save your changes. This also deletes all data related to the deleted test packages (test status, test notes, and test results). In addition, run transaction `SM_CLEANUP` to delete old `SSIMG` for test plan hierarchy. Check the application log in transaction `SLG1` for object `SM_CLEANUP`.	*SAP ILM Tool Support* The deletion of user ID is protected by authorization objects `SM_TPLN` and `SM_TPCK` with activity `ACTVT 06` (delete) in role `SAP_STWB_2_ALL`. Authorization for the deletion of user preferences is managed by `S_USR*` authorizations for user deletion.

Application	Provided Deletion Functionality	Authorization Mechansim
SUT Management	User IDs are used. You can remove them manually within the application. Proceed as follows: 1. In the SAP Solution Manager system, go to tile *Test Suite Administration*. 2. Choose the *Test Automation Framework* tab and choose *Maintain SUT Systems*. The system opens the SUT Management application. 3. Go to tab *System Data Container Hierarchy* and open the filter criteria to enter the relevant user ID in the *Business User* field. 4. Select *Filter*. The system removes all entries in the *Business Destination Enhancement Details*, which do not match the specified business user. 5. Expand the hierarchy and navigate to each entry where the user may have been registered. 6. Select the corresponding *Test Profile* from the *Business Destination Enhancement Details* and click *Remove*. 7. Save your changes. 8. Repeat step 6 within tab *SAP ABAP Backend*, for tab *CBTA* and tab *URI Based SUT*.	
Infrastructure		

Application	Provided Deletion Functionality	Authorization Mechansim
EFWK	Extractors in EFWK for each scenario run periodically to delete the text of business partners, which are set to be blocked in the business partner application. Remaining potential risks are: • If these extractors are stopped manually, the extractor does not update the text of the business partner. • Because the extractors are scheduled periodically, there is a time frame between the time when a business partner is blocked in a business partner function and the time when the text of this business partner is updated in the BW infoobject. Within this time frame, a user can see the text of the business partner which has been blocked in the business partner function. The delivered value of this time frame is 1440 minutes (24 hours). The text of a blocked business partner can be deleted manually via the *Master Data Maintenance* tool in BW. There are various ways provided in SAP BW to delete the text of a particular record in one InfoObject. You can use report `RSDMDD_DELETE_BATCH`. In the BW system, choose transaction `RSA1`, go to `Modeling` → `InfoObjects`. Select the infoObject and select it to open the context manual for *Maintain Master Data*.	not applicable

Application	Provided Deletion Functionality	Authorization Mechansim
GPA	Using GPA you can delete *Guided Procedures* and their execution logs, including user data. Guided procedures can be filtered per users, creation date, change date, and so on. **⚠ Caution** Delete GPA data only for custom guided procedures or plugins. No personal data is stored in SAP-delivered guided procedures or plugins. Guided procedure authoring data can be deleted manually by using the user interface. Only the customer namespace data should be deleted. The following data can be deleted directly by using the guided procedure catalog via *SAP Solution Manager launchpad → Guided Procedures launchpad group → Guided Procedure Catalog*: • Delete logs by selecting a guided procedure and choosing *Execution Logs → Delete Execution Logs* (With Job). • Delete statuses by selecting a guided procedure and choosing *Execution Logs → Delete Execution Instances* (With Job). • Delete guided procedure plans by choosing *Display All Plans* for each guided procedure and then choosing *Delete* for each plan. • Delete a complete guided procedure by choosing *Delete*. **ℹ Note** • Guided procedures used as references are only deleted if the guided procedures that reference them are deleted first. • Only delete a guided procedure once you have removed its logs and statuses as mentioned above. • Delete plug-ins by editing an existing guided procedure, adding a plug-in step, and then choosing *New* to open the plug-in maintenance screen. On this screen, choose *Delete*. You can also directly call the Web Dynpro for plug-in maintenance by calling transaction `SICF` starting the Web Dynpro `AGS_GPA_PLUGIN_MNGT`. Once the data mentioned above has been manually deleted, execute the `PR_UNUSED_DATA_CLEANUP` report to clean up unused or obsolete data. This cleans up orphaned steps, activities, and documentation help texts. To delete old data, execute the `PR_OLD_DATA_CLEANUP` report.	The deletion is protected by authorization object `S_TABU_DIS` with table authorization group `SMGP` in role `SAP_SM_GP_ADMIN`.

Application	Provided Deletion Functionality	Authorization Mechansim
	To delete all logs and statuses for guided procedures, execute the `AGSSISE_DEL_LOGS_GP_SETUP` report. The following steps are relevant for a full clean-up: 1. Go to transaction `SOLMAN_SETUP_ADMIN`. 2. Open the *Generic Storage Admin* menu. 3. Filter on configuration ID: `GP_*`. 4. Remove all entries This removes the remaining data from Guided Procedures executions.	
GSS	**Log and Status** Logs and statuses that are stored for Guided Self Services can be deleted together with all SAP Solution Manager Configuration logs and statuses. To do so, execute the `AGSSISE_DEL_LOGS_GP_SETUP` report by entering the number of days for which you need to keep the logs and then selecting SAP Solution Manager and Guided Self Services. **i Note** To delete **old data**, execute the `PR_OLD_DATA_CLEANUP` report, and select *SAP Solution Manager*. **i Note** If technical users or configuration users are deleted in transaction `SU01`, the `SM:AGSSISE_USER_CLEANUP` batch job will automatically clean up the data stored in the generic storage. **! Restriction** Using this report impacts the auditing and traceability of all SAP Solution Manager Configuration scenarios. **GSS session data** To delete Guided Self Services session data, execute the `RDSMOPREDUCEDATA` report. Use this report to filter according to session package (`GSS*`) and remove the relevant session data for Guided Self Services.	The deletion is protected by auhorization object `SM_SETUP` with `ACTVT 02` (change).
LMDB	Report `RLMDB_CLEAR_CHANGELOG` can be used to delete LMDB Change Log Entries which are older than a given date. A detailed report documentation exists, which explains how to execute the report and schedule a periodical job.	The deletion is protected by authorization objects `AI_LMDB_OB` and `AI_LMDB_AD` in role `SAP_SYSTEM_REPOSITORY_ALL`.

Application	Provided Deletion Functionality	Authorization Mechansim
	To delete LMDB Change Log Entries that are older than a given date, execute the `RLMDB_CLEAR_CHANGELOG` report. A detailed report documentation which explains how to execute the report and schedule a periodic job exists. This cleans up the `LMDB_P_CHANGELOG` table. A job log is written.	
	To delete LMDB Landscape Entries whose end-of-purpose has been reached, follow the *Decommissioning* guided procedure of the *Technical Administration* application. Alternatively, there are dedicated delete functions on the LMDB UI. This cleans up the `LMDB_P_INSTANCE` and `DIAGLS_STAT_MAIN` tables. An LMDB change log is written.	
	To delete custom *LMDB additional attributes* in the `VC_LMDB_ADD_ATTR` view cluster whose end-of-purpose have been reached, use transaction `SM34`. This cleans up the `SMSY_ATTRIB` table.	
	To delete *LMDB log configuration* of the `V_LMDB_LOG_CONF` view and the `DIAG_UNIF_CONFIG` table for a specific user, execute the `RLMDB_USER_DATA_CLEANUP` report. This cleans up the tables mentioned here. These tables are cleaned up during user deletion too. An application log is written.	
	To remove *business partner assignments* from technical systems, use the LMDB user interface. Standard functions, such as blocking a business partner for data protection reasons, can be performed by using the standard business partner functionality.	
	For tables `DIAG_LOG_MAIN` and `DIAG_LOG_MESS`, housekeeping is done by means of the `PR_DIAGLS_CLEANUP` report.	
	Run transaction `SM_CLEANUP` to: • Delete entries from the obsolete file path repository • Delete entries from the obsolete data stores Check the application log in transaction `SLG1` for object `SM_CLEANUP`.	

Application	Provided Deletion Functionality	Authorization Mechansim
Managed System Configuration	Run report `AGSSISE_DEL_LOGS_GP_SETUP` to delete log and status entries which are older than a given date. Then, run report `PR_UNUSED_DATA_CLEANUP`. Persisted user data can be deleted by using transaction `SOLMAN_SETUP_ADMIN`: 1. Start transaction *SOLMAN_SETUP_ADMIN* 2. Select *Generic Storage Admin* 3. Switch to edit mode 4. Delete appropriate Generic Storage Entries of the following configuration IDs: • `AGS_INSE_USER` • `AGS_USER_MNGD_ADMIN` • `AGS_USER_MS_SM_COLLJ` • `AGS_USER_MS_SUPPORT` • `AGS_USER_MS_SUPPORTJ` • `AGS_USER_MS_WILYAGT` • `AGS_USER_RFC_BACK` • `AGS_USER_RFC_READ` • `AGS_USER_RFC_TMW` • `DIR_SCOPE_MIGRATION` • `RCA_SETUP`	The deletion is protected by authorization object `SM_SETUP` with `ACTVT 02` (change) in role `SAP_SETUP_BASIC`.

Application	Provided Deletion Functionality	Authorization Mechansim
Transaction `SOLMAN_SETUP`	**⚠ Caution** If you delete logs and statuses, the traceability of the current SAP Solution Manager Configuration is deleted, too. If you delete generic storage data from the SAP Solution Manager Configuration, the current configuration of the system is deleted too, and has a high impact on functionality. To delete **SAP Solution Manager Configuration statuses and logs for all scenarios**, execute the `AGSSISE_DEL_LOGS_GP_SETUP` report and select *SAP Solution Manager* and *Guided Self Services*. To delete **data stored for configuration in the SAP Solution Manager Configuration Generic Storage**, call transaction `SOLMAN_SETUP_ADMIN`, select *Generic Storage Admin*, and remove the relevant configuration ID. To delete **mass configuration data**, run report `PR_OLD_DATA_MASS_CONF_CLEANUP`. To delete **old data**, execute the `PR_OLD_DATA_CLEANUP` report and select *SAP Solution Manager*. **i Note** If technical users or configuration users are deleted in transaction `SU01`, the `SM:AGSSISE_USER_CLEANUP` batch job automatically cleans up the data stored in the generic storage. To delete obsolete data, execute the `PR_UNUSED_DATA_CLEANUP` report and select both SAP Solution Manager and Guided Procedure Authoring. See also SAP Note 2647547.	The deletion is protected by authorization object `SM_SETUP` with `ACTVT 02` (change) in role `SAP_SETUP_BASIC`.

Application	Provided Deletion Functionality	Authorization Mechansim
Service Connection Application	**Router Permission Table** If you maintain your router permission table by means of the SOLMAN_SAPROUTER transaction, you have to manually delete the related FTP user and FTP passwords in this transaction. In addition, make sure your router permission table does not contain personal data. **Clean up report** AI_SC_CLEANUP_DATA The AI_SC_CLEANUP_DATA report provides a way to delete obsolete personal data if you are planning to shut down functions. This report provides the following functions: • Service Connection Application buffer Select this if you are planning to shut down the service connection application using transaction SOLMAN_CONNECT. This function deletes all service connection data including contact persons. If you decide at a later stage to re-open the service connection application, execute the AI_SC_MIGRATION report to download the buffer data from SAP. • Line Opener log This deletes the log for the AI_SC_LINE_OPENER report and records the user who runs this report. • SAP Router data This deletes data for the SOLMAN_SAPROUTER transaction. • System Upload Data buffer This deletes the buffered hash data, which contain the data that is sent to SAP via job SM:UPLOAD SYSTEM DATA for system upload purposes. **i Note** The upload in job SM:UPLOAD SYSTEM DATA has been deactivated. For more information, see SAP Note 2863831. • S-user Master Data (see tables AICONTACTS, AIINSTACCESS) This deletes personal data and authorizations for S-users, including the AICONTACTS and AIINSTACCESS tables. After the report is finished, you then have to execute the report SOLMAN_DELETE_CUSTOMER_DATA Cleanup S-users, or AI_SDK_SP_GENERATE_BP_V2 to check and lock the relevant Business Partners that are generated by the AI_SDK_SP_GENERATE_BP_V2 report.	**Router Permission Table** The clean up of all sap router data is protected by authorization object SM_RTR_PRM with ACTVT 06 (delete). **Clean Up Report AI_SC_CLEANUP_DATA** Deletion is protected by authorization object S_TABU_DIS: • Clean up all data for setting up / opening service connection and LOP Check is based on authorization group SMSC. • Clean up all S-Users is based on authorization group AISU.

Application	Provided Deletion Functionality	Authorization Mechansim
	> **i Note** > You are not allowed to delete S-users in this report if you manage customer numbers in the `V_AISAPCUSTNOS` view • Transaction `AISUSER` This deletes all data in the `AISUSER` transaction. Only select this option if you are sure that you do not want the SAP Solution Manager system to communicate with SAP. > **i Note** > You are not allowed to delete the entries in this report if you manage customer numbers in the `V_AISAPCUSTNOS` view. • **Data in obsolete tables** This deletes all obsolete tables that are no longer used in SAP Solution Manager 7.2.	
Additional Functions		
Dashboard Builder	You can delete the dashboard or category in the dashboard builder in the configuration mode. If you delete a dashboard via the configuration UI, then the related information is removed from the according tables. To delete a dashboard, open the dashboard in the configuration mode and choose the *delete* button at the bottom of the page. To delete a **dashboard category**, choose *Edit Dashboard Category* and then select the category and choose the *Delete* button.	Authorization object `S_TABU_DIS` is used with table authorization group `CSA0` is used to safeguard the content of the tables in role `SAP_SM_DSH_CONF`.
Dashboard Framework	**Individual dashboard configurations** can be deleted from within the dashboard or by using the `DSH_DELETE` program. **General dashboard configurations** can be deleted only by deleting the corresponding dashboard alias by means of the specific tool: Web Dynpro application `DASHBOARD_MANAGEMENT`. **Dashboard framework objects** (apps and data suppliers) can be deleted only in the specific tool: Web Dynpro application `DASHBOARD_APPLOADER`. **Namespaces** can be deleted by using `DSH_DELETE` program if no apps are assigned to them.	The deletion is protected by authorization object `S_TABU_NAM` for tables `DSH_APP_INSTANCE, DSH_CONTEXT, DSH_NAMESPACES`.

Application	Provided Deletion Functionality	Authorization Mechansim
KPI Catalogue API	Logs and traces are automatically deleted after 30 or 90 days. Downloaded definitions can be deleted by using the `SMKPI_DELETE` program.	Authorization object `S_TABU_DIS` is used with table authorization group `SMTA` is used to safeguard the content of the tables.
Rapid Content Delivery	User IDs of the users who have downloaded and imported `ST-CONT 200` content into an SAP Solution Manager 7.2 system are stored. Run the `RCD_DELETE_PERSONAL_DATA` report.	The application is protected by authorization object `CSU_UNPACK` with `ACTVT 02` (change) in role `SAP_SETU_BASIC`.
SAI	The `SAI_ADMIN_TOOL` BSP application displays all users who use SAI services. This application can also be used to remove users from SAI services.	The deletion is protected by `S_TABU_NAM` in role `SAP_SM_SAI_ADMIN`.
URL Framework	1. Open the SAP Solution Manager launchpad. 2. Navigate to the *SAP Solution Manager Administration* launchpad group. 3. Open the URL framework application → Templates → Root Cause Analysis tile. 4. In the applications table, search for the user ID whose URL customization you would like to delete. 5. For each search result, either choose *Delete* (for application IDs/URLs that were created), or, if the selected application was simply customized, choose *Restore*.	Not applicable
Functions related to Release 7.1		
ASU Toolbox	Run report `/ASU/ASUDEL` to delete ASU content for a given ASU scenario or version. See SAP Note 2646822 - Deletion of personal data stored by ST-PI (ASU Toolbox)	The deletion is protected by authorization object `S_ADMI_FCD` with value `RSET`.
ESR/PSLE	Run report `ESR_GDPR_DELETE_USER_INFO`.	
BW Reporting Testworkbench	All data can be deleted by using the `CCMSBI_TWB_REORGANIZATION` program. See SAP Note 2640144 - Identifying and deletion of personal data stored by ST-BCO	To delete TWB data, the `S_RZL_ADM` authorization object with the `ACTVT ID` and the `01` (create) field is required. See also SAP Note 2645383.
Roadmap	Run report `RSOLAR_DELETE_ROADMAP`. This report deletes roadmaps which were created in the SAP Solution Manager Release 7.1.	The deletion is protected by authorization object `S_AIRMAUTH` with `ACTVT 06` (delete)

Application	Provided Deletion Functionality	Authorization Mechansim
Solar Project, Learning Map, Solutions	**Scenario: Solution Directory** Run report `RSOLAR_DELETE_SOLUTIONS_71` This report deletes old solutions which were created and edited in the SAP Solution Manager ST 7.1. Their sessions, documents, download data, and reporting documents which are contained in the solutions are also deleted. You can select solutions from the F4 help, or a creation date range for deletion. **Scenario: Solar Learning Map** Run report `RSOLAR_DELETE_LEARNING_MAP` This report deletes learning maps which were created in the SAP Solution Manager ST 7.1. You can select learning maps from the F4 help.	The deletion is protected by authorization objects `S_PROJECT` with `ACTVT 06` (delete) for SOLAR projects, and `D_MD_DATA` with `ACTVT 10, 00`.
Solution Directory	Run report `RSOLAR_DELETE_SOLUTIONS_71`. This report deletes old solutions which were created and edited in the SAP Solution Manager Release 7.1, their sessions, documents, download data, and reporting documents.	The deletion is protected by authorization object `S_TABU_DIS` with table authorization group `SMAN` in role `SAP_SOL_***`.
SDA	SDA can be activated by implementing the SAP Note 2283635 on SAP Solution Manager Release 7.2, then you can choose which analysis projects and analysis should be deleted.	The deletion is protected by authorization object `D_SOL_RBE` with `ACTVT 70` for `AGS_RBE`.
SAP Engagement and Service Delivery	Use report `RAGS_SERVPLAN_MIGRATION` to delete obsolete data. The data remained in the system after the migration from SAP Solution Manager 7.1 to SAP Solution Manager 7.2. It deletes service sessions, issues, top issue, and data from service session access keys.	
Switch Framework	Run report `RSOLAR_DELETE_PROJECT`. This report deletes personal data stored in application Switch Framework.	
System Monitoring based on CCMS	Run report `RS_WBA_SYSMON_DELETE`.	The deletion is protected by authorization object `DSWP_ACTIO` with `ACTVT 02` (change), and authorization object `S_MI_CCMS` with `ACTVT 06` (delete).
Test Management	Run report `SMT_PRVD_DELE_TWB71` During the update, test plans and test packages from SAP Solution Manager Release 7.1 were not removed in order to keep them for reference purpose. These are available inSAP Solution Manager release 7.2 in display mode only and can be removed as soon as the data is no longer needed.	The deletion is protected by authorization object `S_TWB` with `ACTVT 06` (delete), and `TREE_TYPE TWB2` for test plans respectively `TWB3` for test packages.

Application	Provided Deletion Functionality	Authorization Mechansim
SMSY	Run report SMSY_CLEANUP.	The deletion is protected by authorization object AI_LMDB_AD with activity ACTVT 06 (delete) in role SAP_SYSTEM_REPOSITORY_ALL.

10.6 Tighten Table Read and Write Access/Table Protection

In many scenarios for SAP Solution Manager, the system needs to read table entries. The direct access to tables is limited wherever possible because a huge number of changes can be executed this way. In some cases, users need to look at data directly. To look at data in a table, users use these transaction codes most frequently: SE16, SE16N, or SE17, SM30, SM34, SM31 or "proxy" transactions.

Authorization Object S_TABU_DIS

Authorization object S_TABU_DIS is used to control table access. It determines what group of tables using authorization groups someone can look at when they use any of the transaction codes above. The authorization object S_TABU_DIS controls complete access during standard table maintenance (transaction SM31), advanced table maintenance (transaction SM30), or the Data Browser (transaction SE16). If you need to control access to individual tables instead to groups of tables, you can use authorization object S_TABU_NAM (see section underneath).

You can assign a table to a specified group. Group assignments are defined in table TDDAT (transaction SE54). For SAP Solution Manager, SAP delivers dedicated authorization groups for specific functions.

The following authorization groups are used in SAP Solution Manager:

Authorization Group	Remarks
AISU	All S-User-related tables
/ASU	ASU Tool
BCSV	CRM: Status profile maintenance
BI* (Remodeling, Repartitioning, Warehouse)	All BI-related tables
BPCA	Business Process Change Analyzer-related tables
CHRM	Other than CRM-related tables for Change Request Management

Authorization Group	Remarks
CRMC	All CRM-related Customizing views as CRM-based scenarios can refer to the same tables and ICC
DFWK	Dashboard Framework-related tables
DIAGST	All RCA-related tables
DNO	CRM: Basis message
DSA	SAP Solution Manager DSA
IVIS	Integration visibility
LMDB	All LMDB and SMSY-related tables
SARC, BCTA	Data volume management
SBPO	SAP Solution Manager: Business Process Operations (Monitoring)
SDCO	All other than CRM-related tables for incident management
SEA	SAP Solution Manager: Scope and Effort Analyzer
SGEN	Tables related to ES-Reporting and SUGEN
SISE	Tables related to SAP Solution Manager Configuration (transaction SOLMAN_SETUP), *Basic Configuration*
SMAL	Tables related to Monitoring and Alerting (Technical Monitoring)
SMAN	Tables related to Implementation and Upgrade
SMCB	SAP Solution Manager: CBTA
SMCM	SAP Solution Manager: Customer Life-Cycle Management
SMCP	Project Management
SMDC	SAP Solution Manager: Data Consistency Management (general)
SMDS	SAP Solution Manager: Data Consistency Management (sensitive)
SMGP	SAP Solution Manager: GPA
SMJM	SAP Solution Manager: Job Management
SMLIC	SAP Solution Manager: License Management
SMRC	SAP Solution Manager: Root Cause Analysis
SMRS	SAP Solution Manager: System Recommendation

Authorization Group	Remarks
SMSD	SAP Solution Manager: Service Delivery
SMTA	Technical Administration
SMUA	Process Documentation: Administration Data
SMUD	Process Documentation: Instance Data
SMUG	Process Documentation: Authorization Groups
SMUL	Process Documentation: Library
SMUM	Process Documentation: Model Data
SRCD	Rapid Content Delivery
SS	RS: SAP Control
STAO	SAP Solution Manager: TAO
TSTM	Tables related to Test Management
USAG	Process Documentation: SMUD Usage

Managed Systems

Authorization Group	Remarks
ST-PI	ST-PI-related table authorization group **! Restriction** This authorization group is relevant for all tables for ST-PI in managed systems.

⚠ Caution

Authorization object S_TABU_DIS is delivered with value asterisk (*) for roles assigned to prominent users in SOLMAN_SETUP such as SOLMAN_ADMIN and SOLMAN_BTC.

The majority of users in a production environment do not need direct access to tables. They view data through transaction codes. However, a few users might need access. When providing direct access to tables, you should use transaction SM30. Extra precautions should be taken for the selected users who require access to transaction SE16 because powerful access to a variety of data might be incorporated. You can make SE16 safer by creating a custom transaction code. With a custom transaction code, the user executes SE16 with a view of the table they require. This means they do not enter the table name instead, the custom transaction code takes them into transaction SE16 and directly into the table.

The combination of the object S_TABU_DIS with other objects can be critical:

- With ACTVT value 02 and S_TABU_CLI (see underneath) for S_TCODE SM30, SM31 allows maintenance of cross-client tables

- With `ACTVT` value `02` for `S_TCODE SM30, SE16` allows unrestricted table maintenance (for example `SAP_SUPPDESK_CONFIG`, see *Application - Specific Guide* section on *Incident Management*)

Authorization Object S_TABU_NAM

The existing SAP table authorization concept is mainly based on the group assignment of tables and the authorization object `S_TABU_DIS`. But, authorization object `S_TABU_DIS` can not always be sufficient.

This authorization object contains the fields:

- `ACTVT:` Display and change access similar to `S_TABU_DIS`
- `TABLE`: Table name

With this object, the system checks the view names or table names directly, so that an exact authorization check is possible. In the function module `VIEW_AUTHORITY_CHECK`, the system checks `S_TABU_NAM` only if the authorization check on `S_TABU_DIS` was unsuccessful.

> **i** Note
>
> Run report `SUSR_TABLES_WITH_AUTH` (see SAP Note 1500054) for analyzing table authorizations for a user or a single role. You can use this program to selectively determine the authorizations for the object `S_TABU_DIS` or `S_TABU_NAM` with regard to the tables that can be accessed using it. Transaction `SU24_S_TABU_NAM` reduces the effort required for maintaining authorization default values during the introduction of an authorization concept with `S_TABU_NAM`.
>
> See also the following SAP Notes:
>
> - 1481950 Information on the new authorization check for generic table access
> - 1541577 Impact of `S_TABU_NAM` in Risk Analysis and Remediation

S_TABU_NAM in Function Retrofit (Change Request Management)

For the retrofit function in Change Request Management, role `SAP_CM_MANAGED_DEVELOPER_RETRO` is delivered. This role contains authorization object `S_TABU_NAM` in an inactive state. To be able to use this function and role, you need to set the object active and add either full authorization for tables or add only those table names which are relevant for you.

Authorization Object S_TABU_CLI

Authorization object `S_TABU_CLI` grants authorization to maintain cross-client tables with the standard table maintenance transaction `SM31`, extended table maintenance transaction `SM30`, the *Data Browser*. It acts as an additional security measure for cross-client tables and enhances the general table maintenance authorization `S_TABU_DIS`.

> **⚠** Caution
>
> A combination of `S_TABU_DIS` value `X`, `S_TABU_DIS` value `02` for field `ACTVT`, and `S_TCODE` values `SM30, SM31, SCC5` is critical.

10.7 Change Log Information per Function

→ Recommendation

We strongly advice to get familiar with the Auditing and Logging possibilities of SAP NetWeaver: https://help.sap.com/saphelp_nw70ehp2/helpdata/en/c7/69bcb7f36611d3a6510000e835363f/frameset.htm. In addition, to find out how to use transactions `SM19` and `SM20`, check https://blogs.sap.com/2014/12/11/analysis-and-recommended-settings-of-the-security-audit-log-sm19-sm20/

Application Logs

Deletion of personal data is logged. Logs can be accessed either in transaction `SLG1` or transaction `SOLMAN_SETUP`, which is based on transaction `SLG1`.

In Transaction `SLG1`

Most log files for SAP Solution Manager can be accessed by using transaction `SLG1` which requires authorization object `S_APPL_LOG`, therefore object and available subobject are listed per function underneath. You need to assign the authorization object with the according values to your user.

In Transaction SOLMAN_SETUP

Authorization object `SM_SETUP` with `ACTVT 61` is checked by the frame of the transaction `SOLMAN_SETUP`. It allows you 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_APPLOG`.

Logging of Customizing Tables

Changes to Customizing tables can be logged via the *Table Change Logging* function provided by SAP NetWeaver.

See the SAP Help Portal for details on Table Change Logging.

Application Log Overview

The table below provides you with information on the transaction for the logging files access. In the *Comments* column, you can find additional information, for instance, if separate logging applications are used, if Customizing table logging applies, and so on.

Application Log Overview

Application	Transaction	Object	Subobject	Comment
BPCA				
BPCA	SLG1	BPCA_DELETE		For Customizing table logging, check the information above. For deletion logs, see transaction SLG1. The logging for the objects is realized as follows: 1. 3PTM Registry: Table logging for Customizing tables. 2. BPCA Analysis: Access via *Solution Manager Launchpad → Test Suite → Business Process Change Analyzer*. Log via SLG1. 3. Optimization Approach: Access via *Solution Manager Launchpad -> Test Suite -> Business Process Change Analyzer -> Details Optimization Approach -> Edit*. Creator and last change user are logged. Protected via authorization object SM_BPCA. 4. TBOM: Access via *Solution Manager Launchpad -> Project and Process Management -> Solution Documentation -> List View -> Restrict to object type TBOM -> Open TBOM -> Action Log*. Protected via authorization object SM_BPCA. 5. TBOM History: Displays change history. 6. TBOM Classification: Table logging for Customizing tables. 7. TBOM Criticality: Table logging for Customizing tables. 8. TBOM Filter: Table logging for Customizing tables. 9. TBOM Options: Table logging for Customizing tables. 10. TBOM Work Item: Access via *Solution Manager Launchpad → Test Suite → My Tasks TBOM Work List → All Work Items → Open Work Item → Action Log*. Protected via authorization object SM_BPCA. Deletion is logged via transaction SLG1. 11. TBOM Work Item Configuration: Table logging for Customizing tables. 12. TBOM Options in managed system: Table logging for Customizing tables 13. BPCA Object and Key mapping: Table logging for Customizing tables
BPO				
BPCC		E2E_EXCMGT	HOUSEKEEP	For the housekeeping job, you can use the job log in transaction SM37.

Application	Transaction	Object	Subobject	Comment
BPI	SLG1	AGS_BPA		See section *Overview of Relevant Applications in SAP Solution Manager* for additional information on log information access. For handling configurable business objects in dependency diagrams and progress management boards, you can access a change log in the persistency browser by executing the AGS_BPA_PERSISTENCE_BROWSER report in SAP Solution Manager. Change log information can be deleted with the report AGS_BPA_PERSISTENCE_REORG. Deletion operations on business objects are logged in the application log (transaction SLG1). The relevant object is AGS_BPA and the subobject is PSM (Persistence Manager) or DIR (Business Process Operations Dashboards).
BP Monitoring	SLG1	E2E_ALERT and SOLAR	BPMO	External ID starting with DELE is used to log deletion activities.
		in the managed system /SDF/E2E	/SOMO/BPMON	Report name E2E_BPM_VARIANT_CLEANUP used as external ID to log deletion activities for persisted solution context.
CDC	SLG1	SM_DCM	In the same order: • CDC_DELETE_CHDOC_COM • CDC_DELETE_CHDOC_MOD • CDC_DELETE_COMP_DEF • CDC_DELETE_DATAMODEL • CDC_DELETE_GROUP • CDC_DELETE_RESULTS	In the same order: • Deletion of change docs for comparisons • Deletion of change documents for data models • Deletion of comparisons • Deletion of data models • Deletion of groups and comparison group types • Deletion of comparison results

Application	Transaction	Object	Subobject	Comment
Job Health Check				The job health check does not change personal data, but collects the user ID of the job execution user. Therefore, there is no change log. If you have deleted selective data from the JSM cubes in the job log you find who deleted whom and when. Note that the job logs are reorganized. Thus, download them if you need to persist this information.
Interface Documentation	SLG1	AGS_DCM	IFDOCU	
OCC Alert Reporting	SLG1	SOLAR	BPMON	Report names AGS_BPM_ALREP_RESET_DEFAULTS and E2E_BPM_VARIANT_CLEANUP are used as external IDs to log deletion activities.
Change Control Management				
BW Reporting for ITSM and ChaRM	SLG1	ITSM	ITSM_SETUP	Logs the re-initialization in transaction SOLMAN_SETUP
		RSD	CUBE_DEL, ODSO_DEL	Logs the deletion of cube data and DSO in transaction RSA1.
		RSDMD	MD_DEL	
Requirements Management ChaRM QGM	SLG1	ARCHIVING, CRM_DATAARCHIVING		**Note** For Change Request Management, also authorization object S_APPL_LOG in transaction SLG1 is checked. These logs are only relevant for technical data such as objects inside transport requests. This data can also be obtained in the managed systems directly in the transport organizer.
Configuration Validation (CCDB)	SLG1	CCDB	STORE-DELETION	

Application	Transaction	Object	Subobject	Comment
ITSM	SLG1	AISDK	• AISDK_HIER • AISDK_SP (Service Provider) • AISDK_SP_BG (Master Data Comparison Background)	Numerous SLG1 objects are used, in particular by the CRM framework.
		PPF	PROCESSING	Processing log
License Management	SLG1	SOLAR		Additional AGS_SISE logs are available.
System Recommendation	SLG1	AGS_SR	CHECK	The change log functionality within the application itself is protected by authorization object S_APPL_LOG with the same object and subobject information.
CCM				
CCM	SLG1	CCLM	CCLM	
			LIB	Logs concerning changes in the library, including the creation and deletion of CCLM owners and contracts.
			DECOM	Logs concerning analyses in the decommissioning cockpit.
			QUAL	Logs concerning analysis in the quality cockpit.
DVM				
DVM	SLG1	DVM	DVMICI	Improvement project
			DECISONMAKER	Prioritized object list
Job Management				
Job Management	SLG1	SOLAR, AI_JOB_MANAGEMENT	AGS_EXTJOB, JOBMANAGEMENT	
Project Management				

Application	Transaction	Object	Subobject	Comment
IT PPM				Copy of Customizing is similar to the customizing copy of ChaRM transaction types, which use logging in separate specific tables. ITPPM logs the original source and the copied target data of every copy process including data and user (see table `SMCP_CUST_TABLOG`).
Process Management				
CDMC				Own logs, it stores basic information of the repository objects.
Customizing Distribution and Scout	`SLG1`	`SOLAR`	`DEFAULT`	Logs deleted setup or configuration information. Check also in transactions `SCDT_LOG` and `SCDR_LOG_DELETE`.
		`CUST_SYNC`	`DISTRIB`	
Solution Documentation and Solution Documentation Graphical Entities	`SLG1`	`SMUD`	`BPD`	Changes on attributes and elements are stored in own history tables of the application. Changes on KW documents trigger separate physical IDs (PHIOs) for every version. The corresponding history information can be viewed using the function that is provided in the application. In addition to this, specific important actions are written into the `SLG1` log.
Solution Documentation - Content Activation	`SLG1`	`SMMIG_GP, SOLAR`	`MIGRATION`	
RCA				
Agent Administration				This scenario is storing user IDs as part of the logging data in the *Maintenance History* view of the agent administration. Open the *Agent Administration UI*, navigate to the *Agents* tab and select the *History* link next to the *Maintenance Mode* button. Scroll through the history table for the user ID in question.
E2E TA Housekeeping				See Java Logging.
Exception Management	`SLG1`	`EXM`	• `COLLECTOR` • `COMMON` • `EXM LOADER` • `SETUP`	Configuration steps are logged in the *Guided Procedure Framework*.
SAP Enagement and Service Delivery				

Application	Transaction	Object	Subobject	Comment
CSA	SLG1	SOLAR	CSA	
DSA/Web DSA	SLG1	SOLAR	JOB	Job RDSMOPREDUCEDATA is logged. The following tables are relevant: DSVASSESSADMIN (change/creation user) DSMOPSERSESSN (change/creation user) DSWPDOWNLOADADM (change/creation user) DSVASSESSIONHEAD (change/creation user) DSVASDOCHEAD (change/creation user) DSVASRESULTSERR (creation user)
EWA Settings	SLG1	SOLAR	SAP_BACKEND	Log for old data cleaned up by report PD_EWA_OLD_DATA_CLEANUP
		SM_SETUP	SM_DEL_LOG_GP	Log and statuses of the EarlyWatch Alert Management scenario
Issue Management				Top issue, issue, and task use CRM framework.
Service Delivery	SLG1	SOLAR	SAP_BACKEND	Service session exchange with SAP uses SLG1 to log changes including changes to personal data. (External ID: GET_SERV_PLAN*).
SDCCN	SLG1	/BDL/LOG	DELETE	Deletion of SDCCN data is logged in SLG1 in every managed system.
SAP Solution Manager Administration				
UOCShell Personalization				Logs for names of deleted users and number of deleted entries are written in the job pool.
SEA				
SEA Analysis	SLG1	AGSSEA		Protected via authorization object SM_SEA. Deletions of SEA analysis are logged in SLG1 (External key *ADMIN_DELETE_ANALYSES).
Technical Administration				
CNM	SLG1	CNM	USER_INFO	

Application	Transaction	Object	Subobject	Comment
IT Calendar and Work Mode Management	SLG1	IT_CALENDAR	USER_INFO, USER_INFO_OBSOLETE, HOUSE_KEEPING	
IT Task Management	SLG1	TASK_PLANNING	USER_INFO	
Technical Monitoring				
BI Monitoring	SLG1	AI_JOB_MANAGEMENT	BIMON	
BW Reporting for System Monitoring (System Reporting)	SLG1	ASR_EXTRACT	• EXTRACTOR Data extractor • SETUP Setup of ASR extractors • TEST Test Mode Extractor	
		GENDL_TASK	GENDL_TASK_SUB Step in post processing of BW data	
Central Job Overview	SLG1	AI_JOB_MANAGEMENT	CJO	
DRM	SLG1	AI_JOB_MANAGEMENT	DRM	
Interface and Connection Monitoring	SOLMAN_SETUP			Change logs are generated and displayed in the context of transaction SOLMAN_SETUP for the scenario.
Job Monitoring	SLG1	AI_JOB_MANAGEMENT	JOBMON	

Application	Transaction	Object	Subobject	Comment
MAI	SLG1	E2E_ALERTING	AUTOCONFIG, DIRECTORY, DPC_RUNTIME, DPC_SETUP, ENGINE, REPOSITORY, SELF_MON, MEA_DIRECTORY_API	
Message Flow Monitoring	SLG1	E2E_EXCMGT	SETUP, ME_ASSEMBLER, MSG_ACTION	
MFM	SLG1	COMPMON_DEL	MFMON	
PI Monitoring	SLG1	COMPMON_DELETE	PIMON	
Self Diagnosis	SLG1	COMPMON_DELETE	SELFDIAG	
System Monitoring	SLG1	SYSMON	USER_INFO	
User Experience Monitoring	SLG1	EEM	RUN	Configuration steps are also logged in transaction SOLMAN_SETUP.
Test Suite				
BW Reporting for Test Suite	SLG1	SMT_ST	SMT_SETUP	Logs the re-initialization in transaction SOLMAN_SETUP.
		RSD	CUBE_DEL	Logs the deletion of transactional data in cubes.
			ODSO_DEL	Logs the deletion of transactional data in DSOs.
		RSDMD	MD_DEL	Logs the deletion of master data in infoobjects.
Partner Test Management	SLG1	E2E_PI_DOMAIN	EXTRACTOR, DOMAIN	Configuration: Using logs which are exposed through the APIs by SAP Solution Manager setup.
		E2E_PI_MESSAGE	EXTRACTION	

Application	Transaction	Object	Subobject	Comment
		E2E_PI_MONITORING	CHANNELMON, CHANNEL_EXTRACTOR, INITIALIZATION, RESET	
SUT Management	SLG1	SOLAR	TST	
Test Suite	SLG1	SMT_TWB	DEFAULT	Objects (test plans, test packages, and test sequences) that are deleted in the application itself via the *Delete* button are also logged there. The log is mainly used to log what is happening in the backend (method access and error messages). **i Note** No deletion information is logged as the main object (test configuration, for example) is an eCATT object. Therefore, logging should be handled by the eCATT application. Logging for users is done by the main application.
Test Automation (CBTA)	SLG1	SOLAR	TST	
Infrastructure				
GPA	SLG1	SM_GPA	SM_GPA_PLAN_MAN	The log can only be accessed if the user has authorization object SM_GPACUST value display to be able to navigate in the configuration scenarios. Guided procedures plans
		SM_SETUP	SM_DEL_LOG_GP	Cleanup logs and statuses for guided procedures
		SM_GPA	SM_DEL_GPA	Other guided procedures objects
GSS	SLG1	SM_SETUP	SM_DEL_LOG_GP	
Job RDSMOPREDUCEDATA	SLG1	SOLAR	JOB	
LMDB	SLG1	AI_LMDB		Customizing tables: LMDB_LOG_CONF (via V_LMDB_LOG_CONF) SMSY_ATTRIB (via VC_LMDB_ADD_ATTR)

Application	Transaction	Object	Subobject	Comment
SOLMAN_SETUP	SLG1	SM_SETUP	SM_DEL_LOG_GP	The deletion of logs is logged. The log can only be accessed if the user has authorization object SM_SETUP value display to be able to navigate in the setup scenarios Logs and statuses
			SM_DEL_GP	Log for mass configuration data as well as the log and statuses reports
			SM_GENST_DEL_USER	Log for user data cleaned up by SM:AGSSISE_USER_CLEANUP job
			SM_GENSTORE	Log for generic storage
Managed System Configuration				AGS_SISE_LOG
Service Connection Application	SLG1	SOLAR	SC	The change log indicators are active in the tables AICONTACTS, AIINSTACCESS, AISUSER. When the REFRESH_ADMIN_DATA_FROM_SUPPORT job runs, application log is written.
Additional Functions				
Dashboard Builder	SLG1	DSH_BUILDER	BADI, BPA, BPM, DATA_FEEDER, FM_CON, GATEWAY	
Dashboard Framework	SLG1	ASR_EXTRACT	SETUP	The deletion of objects via standard tools DASHBOARD_MANAGEMENT and DASHBOARD_APPLOADER is not logged. The deletion of individual configurations is logged via SLG1.
KPI Catalog API	SLG1	SMKPI_LOG		
Rapid Content Delivery	SLG1	SOLAR	CSU_DWLD_IMPORT and CSU_PACK	
SAI	SLG1	SAI_LOG		External ID: SAI_EXT_NO
URL Framework	SLG1	DIAGURL	MANAGER; API	URL Maintenance and URL runtime
Functions relating to SAP Solution Manager release 7.1				

Application	Transaction	Object	Subobject	Comment
ASU Toolbox				ASU toolbox creates a new content and task list versions if something is changed by end user.
ESR / PSLE Self - Service Report	SLG1	AGSESR	EXTRACTOR	
Roadmap	SLG1	ROADMAP		
SDA	SLG1	RBE40	DEFAULT	
Service Content Update	SLG1	SOLAR	DEFAULT	In addition, check the change log protocol in transaction AGS_UPDATE.
Service Delivery	SLG1	AGS_ESD	WKC	External ID: DATA_MIGRATION_710TO720
SOLAR, Switch Framework	SLG1	SOLAR	DEFAULT	Learning Map
			DOCU	Solar Project
System Monitoring based on CCMS	SLG1	APPL_LOG	OTHERS	External ID SYSMON
TWB Reporting	SLG1	TWB	TWB_DATA_LOADER_CUBE	Data Loader Call
			TWB_DATA_LOADER_V1	Data Loader Version 1
		TWB_ST	TWB_ATT_EXTR	TWB Attribute Extractor
			TWB_BI_SETUP	TWB BI Reporting Setup
			TWB_EXTRACTOR	TWB Main Extractor
			TWB_MDA_EXTR	TWB Master Data Extractor
Test Management	SLG1	SMT_TWB	DEFAULT	SAP Solution Manager Testing: Test workbench
SMSY	SLG1	SMSY_LOG_OBJ	SECURITY	

Additional information

For more information on logging or tracing, see the *Application Operations Guide* ILM https://wiki.wdf.sap.corp/wiki/pages/viewpage.action?pageId=1577448349 .

10.8 Archiving of Objects

Methods of Archiving

Within SAP Solution Manager, the following methods are used:

- SAP ILM tool support and transaction SARA: For more information, see section *SAP ILM Tool Support*.
- Transaction SARA (respectively transaction SARI for display purposes)
- Guided procedures framework. For more information, see section *Guided Procedure Framework* in the guide.

SAP ILM Tool Support

Once a document has reached the end of its purpose, you can use the ILM object for archiving and thus blocking the document in the system.

Authorization object S_ARCHIVE is used. For SAP Solution Manager-related ILM archiving objects, assign application area CRM (Customer Relationship Management) and your archiving ILM object.

Archiving Business Partners

ILM object CA_BUPA with archiving object CA_BUPA enables:

- Residence rules in relation to consuming applications to control blocking of the central business partner can be maintained.
- Deletion of a central business partner considering retention rules in relation to consuming application is possible.

Transaction SARA

In general, a system adminsitrator would be executing destruction or archiving of objects. Authorization object S_ARCHIVE is used in SAP archiving programs called by transaction SARA to protect the access to archive files. It is also contained in role SAP_SETUP_BASIC_ARCHIVE.

→ Recommendation

- SAP strongly recommends you to remove all instances of `ACTVT 01` or `06` in combination with authorization object `S_PROGRAM: ACTVT SUBMIT`, as this allows deletion of archive files.
- For additional detailed information on ILM related authorizations and roles, see documentation for ILM.

SAP Solution Manager Configuration

To allow any user to use the archiving in SAP Solution Manager Configuration (`SOLMAN_SETUP`), you must assign authorization object `SM_SETUP` with activity `ACTVT 24` (archive). You can archive logs using the SAP Solution Manager Administration in transaction `SOLMAN_SETUP_ADMIN`. Then, logs are no longer visible in the `SAP Solution Manager Configuration`. If you assign the delete permissions, you can delete archived logs.

Overview

The following table gives you an overview of functions using archiving methods. In the *Comment* column, specific details are mentioned.

Application	Method of Archiving	Comment
Change Control Management		
Change Request Management	SAP ILM Tool Support	The SAP ILM tool is used. The archiving object for Change Request Management is `CRM_SERORD`. Archiving needs to be performed for the Change Request Management transaction types. For more information on the relevant **transaction types**, see the section for *ChaRM* in the *Application - Specific Security Guide*. i Note The task list data and reporting data is not archived, but it is deleted. After archiving, the data can no longer be displayed in the WebClient UI, but only in a technical view.
ITSM	SAP ILM Tool Support	Full instructions are provided in SAP Note 1758090. SAP ILM tool is used. ILM objects are: • Incident: `CRM_INCDNT` • Problem: `CRM_PROBLM` • Service Request: `CRM_INCDNT`

Application	Method of Archiving	Comment
QGM	SAP ILM Tool Support	The SAP ILM tool is used. The archiving object for Quality Gate Management (QGM) is `CRM_SERORD`. Archiving needs to be performed for the QGM transaction types. For more information on the relevant **transaction types**, see section *QGM* in the *Application - Specific Security Guide*. **i Note** The task list data and reporting data is not archived, but it is deleted. After archiving, the data can no longer be displayed in the CRM WebClient UI, but only in a technical view.
Requirements Management	SAP ILM Tool Support	The SAP ILM tool is used. The archiving object for requirements management is `CRM_SERORD`. Archiving needs to be performed for the requirements management **transaction types**. For more information on the relevant transaction types, see section *Requirements Management* in the *Application - Specific Security Guide*. **i Note** The task list data and reporting data is not archived, but it is deleted. After archiving, the data can no longer be displayed in the CRM WebClient UI, but only in a technical view.
Test Suite	SAP ILM Tool Support	The SAP ILM tool is used. The archiving objects for test suite are `SM_TPLN, SMT_TPCK, SMT_TFLW`. For more information on how to archive, see the application help for test suite.
Infrastructure		
License Management	Transaction `SARA`	For `AGS_SISE_LOG` message archiving.
Transaction `SOLMAN_SETUP`: *Managed System Configuration*	Transaction `SARA`	For `AGS_SISE_LOG` message archiving
Transaction `SOLMAN_SETUP`: Solution Manager Configuration	Transaction `SARA`	For more information, choose text `AGS_SISE_ARCH_DISPLAY` in transaction `SE61`. SARA object ID is `SISELOG`.

Application	Method of Archiving	Comment
Service Connection Application		When an individual S-user is expired, inactive or deleted at SAP, the job `REFRESH_ADMIN_DATA_FROM_SUPPORT` removes the corresponding entry in `AICONTACTS` as well as its authority data in table `AIINSTACCESS`. Then, it adds the record for its S-User ID and customer number in table `AICONTACTS_DEL` for further processing. After that, you have two ways to archive the corresponding business partner and lock the user (Any added entries in table `AICONTACTS_DEL` are deleted as well): 1. Run report `AI_SDK_SP_GENERATE_BP_V2`. 2. Run report `SOLMAN_DELETE_CUSTOMER_DATA`, select the *Cleanup S-Users* option. The business partner for contact persons is archived when the contact person becomes obsolete. See *Simplification of Deletion*.
SAP Engagement and Service Delivery		
Issue Management	SAP ILM Tool Support	The archiving objects are `CRM_SERORD` and `CRM_ACT_ON`.
Service Delivery	SAP ILM Tool Support	Use archiving object `CRM_SERORD`.
Value Based Delivery Dashboard	SAP ILM Tool Support	The archiving object is `CRM_SERORD`.
Technical Monitoring		
Exception Management	Guided procedure framework	The archiving and deletion of log entries are handled by the guided procedure framework. The content entries are deleted based on the housekeeping settings (retention time). The job runs every day.
User Experience Monitoring	Guided procedure framework	The archiving and deletion of log entries are handled by the guided procedure framework. The content entries are deleted based on the housekeeping settings (retention time). The job runs every day.
Additional Applications		
Rapid Content Delivery	Transaction SARA	Archiving object is `CSU`. Archived data belongs to content deliveries downloaded or imported. Per default, the job is scheduled to run once in every three months in SAP Solution Manager Configuration → *Basic Configuration Procedure*. This time interval can be adapted.

10.9 SAP ILM Tool Support

Transactional data (documents) is blocked using SAP Information Lifecycle Management, master data is blocked using a central blocking indicator. An authorization concept controls both types of blocking. This means that only authorized users, for example an auditor, can access blocked data.

SAP ILM Tool Support

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data.

For more information on ILM, see SAP Note 1825544 Simplified Deletion and Blocking of Personal Data in SAP Business Suite and SAP Information Lifecycle Management.

Business Partner Blocking

Transactional data related to a central business partner (business partner data that is managed centrally) exist in several applications. Some data relates to closed business, other data to open or new business. As long as business activities are in progress, most data will neither be blocked nor be deleted. As soon as business activities related to the central business partner are completed, you need to block the data. After the data reaches the longest retention period, you need to delete the data.

The central business partner needs to be blocked in the leading system and the connected systems after considering the application`s consumption of the central business partner. The relevant applications, including the central business partner application itself, needs to provide permission for blocking the central business partner based on the residence rule calculation defined in the ILM framework. After the central business partner is blocked, business users must no longer be able to display or process this data. Only authorized users such as an auditor should view the central business partner.

PFCG role `SAP_CA_BP_DP_ADMIN` and authorization object `B_BUP_PCPT` are available to maintain the authorization for the following activity types:

- `ACTVT 03` Display (blocked data for a central Business Partner)
- `ACTVT 05` Lock (execute the blocking/end of purpose check for a central Business Partner)
- `ACTVT 95` Unlock (execute the unblocking check for a central Business Partner)

> → Tip
>
> If you do not assign the authorization object and your business partner is blocked, you are not able to see any business partner data anymore. If you need to display blocked business partners for audit reasons, assign the object with `ACTVT 03` display. The object is not contained in any of the SAP Solution Manager standard roles.

For more information, refer to 1825608 Simplified Blocking and Deletion of Central Business Partner.

CRM-Related Additional Information

- 2044428 FAQ End of Purpose Check of central business partner data in CRM
- 2354273 Data protection for CRM transaction data
- 2039738 Simplified Data Deletion based on SAP ILM in CRM.

11 Useful Tools to Help Your Running Operation Stay Secure

11.1 Run a Security Optimization Service

1. Start the *SAP Engagement and Service Delivery* launchpad group in transaction `SM_WORKCENTER`.
2. Go to *Service* and choose the *Service View* subview.
3. *Create* a new *Security Optimization Service*.
4. A guided procedure lets you create the new service for the required systems.

For the *Security Optimization Service*, you have to assign additional authorizations. For more information, see SAP Note 696478.

11.2 SAP EarlyWatch Alert Management

The SAP EarlyWatch Alert (EWA) service monitors the most critical areas of an SAP component, focusing on performance and stability. EWA data is based on weekly performance and system statistics, as well as of system configuration and error analysis data. The data is collected by unmodifiable data collectors using transaction `SDCCN` in the target system and stored in SAP Solution Manager cluster tables `BDLDTOC` and `BDLDATCOL` for persistence. The report displays aggregates of this data as analysis results, trend graphs, and so on.

Configuration

You can configure SAP EarlyWatch Alert reporting in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`). Since the setup for EWA is mandatory for all systems in your system landscape, the procedure for setting up SAP EarlyWatch Alert Management can be run by user `SOLMAN_ADMIN`.

Data Protection

The report does not contain any user-specific data. Although the statistical data can contain user names, they are not related to app data, but only to technical data, such as response times or information for technical error analysis. If the user who collects the data in the source system is authorized to run transaction `ST03` (Workload Monitor) and display application-related data, the EWA report also displays technical transaction codes with user names. This can be avoided by removing value `S_TOOLS_EX_A` from the authorization object `S_TOOLS_EX` for the user in question.

Data Archiving

For more information, see SAP Note 546685.

11.3 Using Configuration Validation for Regular Checks of Compliance

11.3.1 Introduction

> → Tip
>
> For an introduction, see also https://wiki.scn.sap.com/wiki/display/TechOps/ConfVal_Reporting

The following document is intended to give you a minimum recommendation on how to use and implement the Configuration Validation (CV) function for your SAP Solution Manager, especially for the topic of authorizations and users. This includes the customizing of ConfigStores, and subsequent definition of the compliance reporting. All recommendations are based on SAP Solution Manager best practices only.

For more information, see the online documentation for this topic and the information. See the *Root Cause Analysis* launchpad group in the SAP Solution Manager system.

CV can be used for many other topics related to security compliance and optimization, as well as other configuration-related settings in your system. In addition, due to the nature of the Solution Manager system as a single source of truth and the subsequent connection to all required managed systems, this function can also be applied from within Solution Manager to all of your managed systems as well.

The following general description is not based on a specific SAP Solution Manager Support Package.

In this document, we cover the following topics by way of example, which can be evaluated on a regular basis once implemented:

Topic	According ConfigStore and According Section in the Guide	Remarks
Which of your predefined critical standard users still have their default passwords assigned and are not compliant?	`STANDARD_USERS`	This CS is shipped by SAP by default. It cannot be adapted or changed. If you are not compliant with this ConfigStore, we highly recommended to check the specific users.
Which users are assigned the `SAP_ALL` profile and are not compliant?	`AUTH_PROFILE_USER`	The profile definition `SAP_ALL` is predefined by default from SAP. This ConfigStore can be extended by defining additional ConfigStore values. For example, you can also check for profile `SAP_NEW`, or any other profile you have defined.

Topic	According ConfigStore and According Section in the Guide	Remarks
Which users have what roles?	AUTH_ROLE_USER	
Which roles exist with a specific pattern in a role name?	AUTH_PATTERN_ROLE	
For example, which display roles have change or edit authorizations?	AUTH_DISPLAY_ROLE	
Which roles have specific authorizations or authorization combinations?	AUTH_COMB_CHECK_ROLE	
Which users have specific authorizations or authorization combinations?	AUTH_COMB_CHECK_USER	
Which users can run which transactions?	AUTH_TRANSACTION_USER	
Are there any users in the system with the wrong user type?	AUTH_USER_TYPES	

11.3.2 Prerequisites

System Configuration

The following prerequisites have to be met before you can use Configuration Validation:

- Configured SAP Solution Manager system/client
- Configured BW system/client
- Extractor Framework is running and extractors are collecting data
- RFC connections READ and BW-related are working
- A dialog user with the required authorizations in your SAP Solution Manager system and BW system

More Information

For more information about configuring SAP Solution Manager, see the corresponding *Secure Configuration (SOLMAN_SETUP) Guide* for SAP Solution Manager 7.2.

11.3.3 Users and Roles in the SAP Solution Manager

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

Template End User

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

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

Administrator User CV_ADM_XXX (Help Text ID: TP_CV_ADM)

Single Roles	Help Text ID
SAP_CV_ALL	AUTH_SAP_CV_ALL Full authorization for Configuration Validation, especially Report Directory **i Note** Authorization object AI_CCDB_SC is set to inactive in the role. The authorization restricts access to the User ConfigStores, and therefore security-relevant data. If you allow your administration user to read this data, set the authorization object to active in this role.
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
BW-Related Single Roles	Help Text ID
SAP_BI_E2E SAP_SM_BI_ADMIN	• AUTH_SAP_BI_E2E • AUTH_SAP_SM_BI_ADMIN **⚠ Caution** If the BI scenario is remote, these roles have to be assigned to the BI user in the remote system in addition to authorization object S_RFCACL.

Display User CV_DIS_XXX (Help Text ID: TP_CV_DIS)

Single Roles	Help Text ID
SAP_CV_DIS	AUTH_SAP_CV_DIS
SAP_SYSTEM_REPOSITORY_DIS	AUTH_SAP_SYSTEM_REP_DIS
SAP_SMWORK_DIAG	AUTH_SAP_SMWORK_CHANGE_MAN
SAP_SM_FIORI_LP_EMBEDDED	AUTH_SAP_SM_FIORI_LP_EMBED
SAP_BI_E2E SAP_SM_BI_DISP	• AUTH_SAP_SM_BI_E2E • AUTH_SAP_SM_BI_DISP ⚠ Caution If the BI scenario is remote, these roles have to be assigned to the BI user in the remote system in addition to authorization object S_RFCACL.

Main Authorization Objects

AI_CCDB_SC

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

→ Recommendation

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

11.3.4 Defining Configuration Stores

Get an Overview of Configuration Stores

ℹ Note

For an overview of defining Configuration Stores, see SDN https://wiki.scn.sap.com/wiki/display/TechOps/ConfVal_Reporting.

What data does each ConfigStore contain?

The content of a CS (or in other words, what data the extractors collect) is always defined by the specific definition of it. The data you see here, is all the information collected by the extractors according to the

definition for the specific CS. Initially, some CS already have a definition delivered by SAP, for instance CS AUTH_PROFILE_USER. But not all CS contain initial content and are empty.

What happens if the definition of the ConfigStore changes?

When you start changing the definition of the CS to your individual needs, the extractors collect content according to this new definition, and it is displayed by the system.

Define the Concept

Before you implement anything in your system, it is vital that you have a concept for security compliance that you want to implement. To do this, we recommend some preparatory steps and explanations that help you easily deploy your requirements later. We therefore recommend that you develop your concept and plan how to translate it into the system by preparing a table that includes questions and answers as well as some technical information:

- What is the requirement?
- When is the system compliant?
- How should the reports be named? Do you have any naming conventions that are required and support your work?

Know the Procedure of Implementing ConfVal

Each CS is unique in that, according to the focus of the compliance task, a specific statement needs to be added. In addition, each CS allows you to maintain it specifically to your needs. Therefore, the recommendations we give in the individual sections of this document can only be taken as an example or template with which you can start. For each implementation for a CS, we recommend the following steps after your concept is finished and you know what you want to implement. All these steps are followed in the recommendations for the CS that are described in this document.

Define the CS in transaction CCDB

By default. most CS are delivered by SAP without any content, except for STANDARD_USERS or AUTH_PROFILE_USER. Therefore, you need to define the content of the CS according to your concept of what you want to check later on. You can define almost any CS, except for STANDARD_USERS. Depending on what you want to check, the extractors collect data. This collected data provides the background against which you can later run compliance definitions.

Generally, all CS are defined using a specific transaction: CCDB. In this transaction, you can also check for errors if, for example, extractors are not working. To define CS content, proceed as follows (how to define each specific CS is explained in the individual sections per CS):

1. Choose transaction CCDB.
2. Choose the *Technical System* tab and filter for your system ID (in this case the SAP Solution Manager system ID).
   The system should not display any error messages for extractors.
3. Mark the line for the ABAP stack, as in this example we want to define a CS for ABAP.
   The system displays a number of filter buttons for the Stores underneath.

4. Choose the *Correct* button.
   The system display all correctly running CS for your system and clients.
5. Mark the line for the CS you want to define and choose *Store Details*.
6. Open the tray to display the detail list underneath.
7. Go to the *Customizing* tab.
8. Define your own *Store Customizing* for this particular CS (see following sections per CS).

   > → Recommendation
   >
   > Make sure, you are not overwriting the default customizing *000 SAP (Default)*, but create your own.

9. After you have defined it, you need to set it as relevant for the system, otherwise the extractors will not collect the data that you defined.

11.3.5 STANDARD_USERS: Which Standard Users Retain Their Default Password?

Use

With this CS you can answer questions, such as "Which of the passwords of standard users have not been changed?". Changing passwords that are generally known is one of the first things you should do to secure your system. In addition, we strongly recommend to regularly check the compliance with this requirement. This CS is a standard CS delivered by SAP, so you do not need to configure it specifically. Users checked are:

SAP Users Checked

- `DDIC`
- `EARLYWATCH`
- `SAP*`
- `SAPCPC`
- `TMSADM`

11.3.6 AUTH_PROFILE_USER: Which Users Have Profile SAP_ALL / SAP_NEW Assigned?

Use

With this CS you can answer questions, such as "Which users have profiles SAP_ALL and SAP_NEW assigned?". Assigning these two profiles is generally a security risk and should be handled carefully. If possible, try to minimize authorizations for users instead of extending them.

11.3.7 AUTH_ROLE_USER: Which User Is Assigned Critical Roles

Use

With this CS you can answer questions, such as "Which users have roles assigned that are critical in your system landscape?". The pattern of roles can vary. You can, for example, use this function to find out which roles can be deleted from the system.

In this case, we want to find out and check which users have critical roles `SAP_J2EE_ADMIN` or `SAP_SM_USER_ADMIN` assigned.

Customzing CS

1. Define the CS and assign the pattern `SAP_J2EE_ADMIN` in column *Role Pattern* and an asterisks * in column *User Pattern* to see all users. You can also specify users here.

   > **i** Note
   >
   > The column *Check ID* defines an ID for the value in question.

2. Wait for the next extractor run.

Result

To perform a quick check of users, you can check directly in transaction `CCDB` for this CS. Simply choose the *Content* button for the latest extractor results.

11.3.8 AUTH_PATTERN_ROLE: Which Roles Exist for a Specific Pattern in the Role Name?

Use

With this CS you can answer questions, such as "Which roles with a specific pattern do exist in the system?". The pattern can vary, such as the name space of a role. You can, for example, use this function to find out which roles can be deleted from the system.

In this case, we want to check which navigation roles from SAP have been copied, as navigation roles should not be copied.

Procedure

1. Define the CS and assign the pattern.
   The following conditions apply:
   - Copied roles do not start with name space *SAP*.
   - Navigation roles all contain the pattern *SMWORK*.

   The pattern/value is therefore: `*SMWORK*`.
   Wildcards indicate, that we check for all possible characters before and after the pattern *SMWORK*.

   > **i** Note
   >
   > The *Parameter* column defines an ID for the value in question.

2. Wait for the next extractor run.
   The selection of roles is read from table `AGR_1251`.

Result

The system displays all navigation roles that have been copied and can therefore be removed from the system.

11.3.9 AUTH_DISPLAY_ROLE: Which Display Roles Have Change/Edit Authorizations?

Use

With this CS you can answer questions, such as "Which display only roles contain change authorizations?". You can, for example, use this function to check whether your defined display roles contain only display authorizations. The system checks if other activities than 03 (display) are present in an authorization object in the roles defined.

In this case, we want to check which SAP display roles contain authorizations that do not follow the default activity for display `ACTVT 03`.

11.3.10 AUTH_COMB_CHECK_ROLE: Which Roles Have Specific Authorizations or Authorization Combinations?

Use

With this CS, you can answer questions, such as the following:

- Which roles have specific authorization objects with specified values?
- Which roles have specific authorization object combinations with specified values?

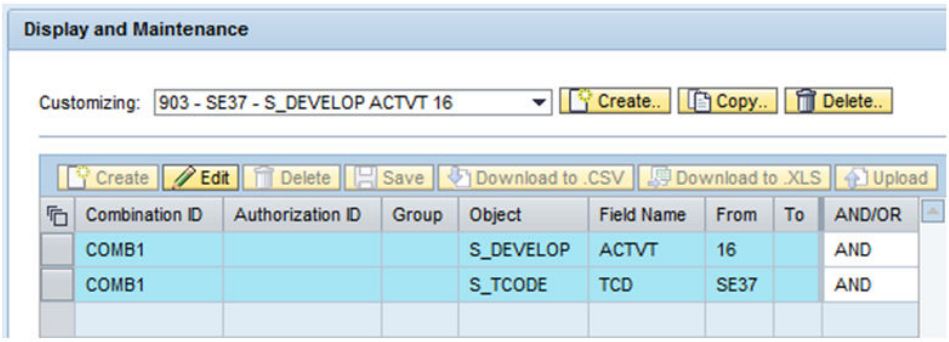
You can use this function to check whether specific critical authorization objects and authorization values are contained in roles in your system.

Procedure

> **Example**
>
> You want to display all roles in the system that contain transaction code `SE37` to run function modules and authorization object `S_DEVELOP` with activity `16` for execution.

The definition table requires at least a self-defined *Combination ID*, *Object*, *Field Name*, *Values* and `AND/OR` clause.

1. Define the CS.
   The following conditions apply:
   - Define a *Combination ID* for the combination you define. For example: `COMB1`.
   - Object names are `S_TCODE` and `S_DEVELOP`.
   - The field name for `S_TCODE` is `TCD  SE37`.
   - The field name for `S_DEVELOP` is `ACTVT` with value 16.
   - The clause value for both objects is `AND`.
2. Enter the values for the combination per line.



Tab: Customizing

3. Set the new definition to active by selecting it as *Store Customizing*.
4. Wait for the next extractor run or manually start an extractor run by checking the store (*Expert Functions* button) and using executing extractors (*Execute Extractors* button).
   The selection of roles is read from table `AGR_1251`.
5. You can check for any Upload information in the *Log* tab.

Result

The system displays all roles that contain the above combination of authorizations.

11.3.11 AUTH_COMB_CHECK_USER: Which Users Have Specific Authorizations or Combinations Assigned?

Use

With this CS, you can answer questions, such as "Which users have specific authorization objects with specified values assigned?". It is very similar to CS `AUTH_COMB_CHECK_ROLES`. We recommend to reuse your customizing from the `AUTH_COMB_CHECK_ROLES` store.

You can use this function to, for example, check whether specific critical transactions such as `SE80` are assigned to users in your system.

Procedure

> **Example**
>
> You want to display all users in the system that are assigned transaction code `SE37` or `SOLMAN_SETUP`.

The definition table requires at least a self-defined *Combination ID*, *Object*, *Field Name*, *Values* and `AND/OR` clause.

1. Define the CS.
   The following conditions apply:
   - Define a *Combination ID* for the combination you define. For example: `COMB1`.
   - The object names are `S_TCODE` and `S_DEVELOP`.
   - The field name for `S_TCODE` is `TCD  SE37`.
   - The field name for `S_DEVELOP` is `ACTVT` with value 16.
   - The clause value for both objects is `AND`.
2. Enter the values for the combination per line.
3. Set the new definition to active by selecting it as *Store Customizing*.
4. Wait for the next extractor run or manually start an extractor run by checking the store (*Expert Functions* button) and using executing extractors (*Execute Extractors* button).
   The selection of roles is read from table `AGR_1251`.
5. You can check for any upload information in the *Log* tab.

Result

The system displays all users that contain the above combination of authorizations.

11.3.12 AUTH_TRANSACTION_USER: Which Users Are Allowed to Run Critical Transactions?

Use

With this CS, you can answer questions, such as "Which users are allowed to run predefined critical transactions?".

Procedure

> ✤ Example
>
> You want to display all users in the system that are assigned transaction code `SU01` and `PFCG`.

1. Enter the values for the transaction in the *Transaction Code* field.
2. Set the new definition to active by selecting it as *Store Customizing*.
3. Wait for the next extractor run or manually start an extractor run by checking the store (*Expert Functions* button) and using executing extractors (*Execute Extractors* button).
4. You can check for any upload information in tab *Log*.

Result

The system displays all users that contain the above combination of authorizations.

11.3.13 AUTH_USER_TYPES: Are There Any Users in the System with Wrong User Type?

Use

With this CS you can answer questions, such as "Are all users in the correct user type group?".

Procedure

> ### Example
>
> We want to display all users in the system that are assigned to user type *Service*. For SAP Solution Manager, no users with type *Service* are supposed to be created.

1. Define the CS.
   The following conditions apply:
   - Define a *Check ID* for the combination you define. For example: `COMB1`.
   - The user names are all users, enter `*`.
   - The usser type is `Service`.
2. Enter the values for the combination per line.
3. Set the new definition to active by selecting it as *Store Customizing*.
4. Wait for the next extractor run or manually start an extractor run by checking the store (*Expert Functions* button) and using executing extractors (*Execute Extractors* button).
5. You can check for any upload information in the *Log* tab.

Result

The system displays all users that contain the above combination of authorizations.

Important Disclaimers and Legal Information

Hyperlinks

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

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

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

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

Example Code

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

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP