



PUBLIC

Document Version: 8.0 – 2023-11-02

Security Guide for SAP S/4HANA 2020

Content

- 1 Introduction. 7**
- 2 Before You Start. 8**
- 3 User Administration and Authentication. 10**
 - 3.1 User Management. 10
 - Non-SAP Fiori Technology. 10
 - SAP Fiori Technology. 12
 - 3.2 User Data Synchronization. 13
 - 3.3 Role Administration. 13
 - 3.4 Integration into Single Sign-On Environments. 13
- 4 System Hardening with SAP Security Notes. 15**
- 5 SAP S/4HANA System Landscape Information. 17**
- 6 Network and Communication Security. 19**
 - 6.1 Communication Channel Security. 19
 - 6.2 Network Security. 20
 - 6.3 Communication Destinations. 20
- 7 ICF and Session Security. 21**
- 8 File System Access Security. 23**
- 9 Virus Scanning. 24**
 - 9.1 Virus Scanning in File Uploads. 24
 - 9.2 General Recommendations for Virus Scan Profiles. 25
 - 9.3 Further Protection Against Active Content. 27
- 10 Additional System Hardening Activities. 29**
- 11 Data Protection and Privacy. 31**
 - 11.1 Read Access Logging. 33
 - 11.2 Deletion of Personal Data. 34
 - 11.3 Information Retrieval. 35
 - 11.4 Consent Administration. 36
- 12 SAP S/4HANA Cross Application Infrastructure. 37**
 - 12.1 Data Security in SAP ILM. 37
 - Data Security in SAP ILM System Connections. 37

	Users and Authorizations in SAP ILM.	38
	Security of Stored Data in SAP ILM.	39
	Logs in SAP ILM.	40
12.2	Payment Card Security.	41
	Before You Start.	41
	Authorizations	42
	Data Storage Security.	43
	Setting Up Encryption Software	44
	Making Settings for Payment Card Security	44
	Relevant SSF Applications	46
	Generating Keys	46
	Migration of Payment Card Data Stored in Unencrypted Form	47
	Migration of Payment Card Data on SAP Business Partner.	47
	Migration to SSF Application PAYCRV	48
	Migration to Current Key Version	48
	Deleting a Key Version	49
	Security-Relevant Logging and Tracing.	49
	Recommended Implementation Steps	49
12.3	Data Security in Behavioral Insights.	50
	Roles and Authorizations.	51
	Data Protection.	55
13	SAP S/4HANA Enterprise Business Applications.	59
13.1	Asset Management.	59
	Maintenance Operations.	59
	Resource Scheduling.	60
	Environment, Health and Safety.	60
	Management of Change.	72
13.2	Finance.	75
	Financial Accounting.	75
	Controlling.	93
	Governance, Risk and Compliance for Finance.	94
	Treasury Management.	107
	Financial Operations.	128
	Billing and Revenue Innovation Management.	141
	Real Estate Management.	149
	Receivables Management.	155
	SAP S/4HANA Financial Closing cockpit.	177
	Travel Management.	177
	Incentive and Sales Force Management.	181
13.3	Human Resources.	236
	User Management.	236

	Authorizations.	237
	Security-Relevant Logging and Tracing.	242
	Core HR and Payroll.	242
	Talent Management.	367
	Time and Attendance Management.	458
13.4	Manufacturing.	476
	Production Planning.	476
	Manufacturing Execution for Discrete Industries.	477
	Manufacturing Execution for Process Industries.	490
	Project Manufacturing Management and Optimization.	491
	Quality Management.	492
	Maintenance Operations.	499
13.5	R&D / Engineering.	499
	Product Compliance.	499
	Product Safety and Stewardship.	501
	Enterprise Portfolio and Project Management.	529
	Integrated Product Development for Discrete Industries.	560
	Product Lifecycle Management.	566
	Product Development for Discrete Industries.	581
13.6	Sales.	581
	Sales Force Support.	582
	Order and Contract Management.	589
13.7	Service.	593
	Master Data.	593
	Business Roles.	598
	Internet Communication Framework Security (ICF) in Service.	599
	Service Processes.	600
	Field Service Management Integration.	608
	In-House Repair.	609
	Interaction Center.	611
	Subscription Order Management.	621
	E-Mail Response Management System.	624
	UI Framework.	631
	Knowledge Management.	643
	Deletion of Personal Data in Service.	644
	Warranty Management.	645
13.8	Sourcing and Procurement.	647
	Authorizations.	647
	Data Storage Security.	654
	Other Security-Relevant Information.	657
	Deletion of Personal Data.	659

	Specific Read Access Log Configurations.	662
	Ariba Network Integration.	664
	Supplier Management.	664
	Integration.	670
13.9	Supply Chain.	672
	Inventory.	673
	Delivery and Transportation.	684
	Warehousing.	707
	Advanced Order Promising.	725
13.10	Cross-Line-of-Business.	726
	Commodity Management.	726
13.11	Analytics Technology.	736
	Process Performance Monitoring.	737
13.12	Enterprise Technology.	739
	Master Data Maintenance.	739
	Enterprise Contract Management.	749
	Geographical Enablement Framework.	753
	Master Data Governance.	755
	Agent Framework.	756
13.13	SAP S/4HANA Industries.	757
	Consumer.	757
	Discrete Industries.	777
	Energy & Natural Resources.	780
	Financial Services.	815
	Public Services.	863
	Services.	927
13.14	Country-Specifics.	936
	Deletion of Personal Data in Business Applications.	936
	Read Access Logging for Electronic Documents.	937
	Specific Read Access Log Configurations.	938
14	Business Network Integration.	940
14.1	Security Aspects for Connectivity Types.	940
14.2	Direct Connectivity: SAP S/4HANA as Client.	941
14.3	Direct Connectivity: SAP S/4HANA as Server.	943
14.4	Roles and Authorizations (Ariba Network).	943
14.5	Roles and Authorizations (SAP Fieldglass).	944

Document History

Version	Date	Description
1.0	October 7, 2020	First published version for SAP S/4HANA 2020
1.1	October 8, 2020	The chapters Environment, Health and Safety [page 60] , Utilities [page 797] and Defense & Security [page 863] were updated.
2.0	February 24, 2021	First published version for SAP S/4HANA 2020 FPS01
3.0	May 26, 2021	First published version for SAP S/4HANA 2020 FPS02
4.0	November 03, 2021	First published version for SAP S/4HANA 2020 SPS03
5.0	May 04, 2022	First published version for SAP S/4HANA 2020 SPS04
6.0	November 02, 2022	First published version for SAP S/4HANA 2020 SPS05
7.0	May 03, 2023	First published version for SAP S/4HANA 2020 SPS06
8.0	November 2, 2023	First published version for SAP S/4HANA 2020 SPS07

1 Introduction

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Migration Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP S/4HANA.

To assist you in securing SAP S/4HANA, we provide this Security Guide.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP S/4HANA in general. In particular it comprises general considerations regarding the system access via SAP Fiori Apps. In case there are specific aspects for the underlying scenarios or applications these are described in an area-specific chapter.

2 Before You Start

Fundamental Security Guides

SAP S/4HANA is based on ABAP Platform and the SAP HANA Platform. With respect to SAP Fiori apps, SAP Gateway plays a fundamental role as well. This means that the corresponding Security Guides are also applicable for SAP S/4HANA.

Whenever other guides are relevant, an appropriate reference is included in the documentation for the individual solution areas in the specific part of this guide.

Also consider the following fundamental security whitepapers found on <https://support.sap.com/en/security-whitepapers.html>:

- Secure Configuration of SAP NetWeaver Application Server Using ABAP
- SAP Security Recommendations: Securing Remote Function Calls (RFC)
- Protecting SAP Applications Against Common Attacks

Approach for "Secure By Default"

SAP applies "secure by default" settings during system installation, system copies and system conversion from SAP ERP. Depending on the SAP S/4HANA release, the "secure by default" scope might vary. Overall, settings affect the profile parameters, ABAP platform configurations and HANA auditing.

New Installations and System Copies

- You have the choice to skip the activation of the secure profile parameters.
- Due to the nature of the settings, ABAP platform configurations and HANA auditing will always be enabled for new installations and system copies.

System Conversions

- You have the choice to skip the activation of the secure profile parameters.
- ABAP platform configurations and HANA auditing will only be enabled in case the source system does not have a customer configuration for the respective topic. For example, SAP Security Audit Log configuration is only enabled with "secure by default" settings in case the source system does not have any SAP security audit log configuration.

For detailed information on "secure by default" settings, see SAP Note [2926224](#).

Important SAP Notes

- SAP Note [1956820](#) contains information about saving temporary files when using Adobe Acrobat Reader in SAP applications.

- SAP Note [138498](#) contains information on single sign-on solutions.
- SAP Notes relating to security for the subcomponents of SAP S/4HANA are referenced in the documentation for the individual components in this guide.
- For a list of additional security-relevant SAP Hot News and SAP Notes, see the SAP Support Portal at <http://support.sap.com/securitynotes>.

3 User Administration and Authentication

Overview

SAP S/4HANA generally relies on the user management and authentication mechanisms provided with ABAP Platform, in particular the Application Server ABAP and the SAP HANA Platform. Therefore, the security recommendations and guidelines for user administration and authentication as described in the Application Server ABAP Security Guide and SAP HANA Platform documentation apply.

For more information, see:

- Go to https://help.sap.com/s4hana_op_2020, enter *Application Server ABAP Security Guide* into the search bar, press `Enter`, and open the search result with that title.
- *SAP HANA Security Guide* at the SAP Help Portal under http://help.sap.com/hana_platform/ under **► Security ►**

In addition to these guidelines, you can find information about user administration and authentication that specifically applies to SAP S/4HANA in the following topics:

- [User Management \[page 10\]](#)
This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with SAP S/4HANA.
- [User Data Synchronization \[page 13\]](#)
SAP S/4HANA can share user data with other components. This topic describes how the user data is synchronized with these other sources.
- [Role Administration \[page 13\]](#)
- [Integration into Single Sign-On Environments \[page 13\]](#)

3.1 User Management

3.1.1 Non-SAP Fiori Technology

User management for SAP S/4HANA uses the mechanisms provided with the Application Server ABAP, such as tools, user types, and password concept. For an overview of how these mechanisms apply for SAP S/4HANA, see the sections below. In addition, we provide a list of the standard users required for operating SAP S/4HANA.

User Administration Tools

This table shows the tools available for user management and administration.

Tool	Description
User maintenance for ABAP-based systems (transaction SU01)	For more information about the authorization objects provided by the subcomponents of SAP S/4HANA, see the application-specific sections.
Role maintenance with the profile generator for ABAP-based systems (PFCG)	For more information about the roles provided by the subcomponents of SAP S/4HANA, see the application-specific sections. For general information, go to https://help.sap.com/s4hana_op_2020 , enter <i>User and Role Administration of Application Server ABAP</i> into the search bar, press <input type="text" value="Enter"/> , and open the search result with that title.
Central User Administration (CUA) for the maintenance of multiple ABAP-based systems	For central administrative tasks

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run. The user types that are required for SAP S/4HANA

- Individual users
 - Dialog users - used for SAP GUI for Windows
 - Internet users - used for Web Applications
- Technical users
- Service users are dialog users who are available for a large set of anonymous users
- Communication users are used for dialog-free communication between systems
- Background users are used for processing in the background

For more information about these user types, go to https://help.sap.com/s4hana_op_2020, enter *Application Server ABAP Security Guide* into the search bar, press , and open the search result with that title.

Standard Users

This section describes the standard users necessary for operating SAP S/4HANA

i Note

Ensure you change the passwords and IDs of users that were created automatically during the installation.

System	User ID	Type	Password	Additional Information
ABAP Platform	<sapsid>adm	SAP system administrator	Mandatory	Application Server ABAP Security Guide
ABAP Platform	SAP Service <sapsid>	SAP system administrator	Mandatory	Application Server ABAP Security Guide
ABAP Platform	TMSADM	SAP system administrator	Mandatory	Application Server ABAP Security Guide
ABAP Platform	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	See ABAP Platform Security Guide	Optional	ABAP Platform Security Guide Note that EARLYWATCH and SAPCPIC may not be needed in your system landscape. See note below this table for details.
SAP ECC	SAP Users	Dialog users	Mandatory	The number of users depends on the area of operation and the business data to be processed

i Note

In most cases, the user EARLYWATCH is not used anymore. We recommend checking if this is the case in your landscape. If the user is not needed, it should be deleted to minimize the attack surface. For more information, see [1749142](#).

The user SAPCPIC is sometimes used in legacy RFC scenarios or with EDI. We recommend checking if SAPCPIC is needed in your landscape. If the user is not needed, it should be deleted to minimize the attack surface.

3.1.2 SAP Fiori Technology

For details on the user management and authorization concepts used in SAP Fiori apps, go to https://help.sap.com/s4hana_op_2020, enter *SAP Fiori Overview* into the search bar, press **Enter**, and open the search result with that title.

3.2 User Data Synchronization

By synchronizing user data, you can reduce effort and expense in the user management of your system landscape. Since SAP S/4HANA is based on ABAP Platform, you can use all of the mechanisms for user synchronization in ABAP Platform here.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *ABAP Platform Security Guide* into the search bar, press , open the search result with that title, and navigate to [▶ User Administration and Authentication ▶ User Data Synchronization ▶](#).

3.3 Role Administration

Business roles in SAP S/4HANA represent the central object used to structure users' access on the frontend server.

For more information, go to https://help.sap.com/s4hana_op_2020 and proceed as follows:

- **General information on role maintenance in systems based on Application Server ABAP:**
Enter *Configuration of User and Authorization Administration* into the search bar, press , and open the search result with that title.
- **Role maintenance for access based on SAP Fiori launchpad:**
Enter *SAP Fiori Launchpad* into the search bar, press , open the search result with that title and then navigate to one of the following entries:
 - [▶ Administration Guide ▶ Initial Setup of the Launchpad ▶](#)
 - [Security Aspects](#)
- **Authorization concepts and role maintenance for custom development:**
Enter *From the Programmed Authorization Check to a Role* into the search bar, press , and open the search result with that title.
- **UI content and authorization concept for SAP Fiori apps:**
Enter *SAP Fiori Launchpad Content and Authorization Concept* into the search bar, press , and open the search result with that title.

3.4 Integration into Single Sign-On Environments

Non-Fiori Technology

SAP S/4HANA supports the single sign-on (SSO) mechanisms provided by Application Server ABAP technology. Therefore, the security recommendations and guidelines for user management and authentication that are described in the *ABAP Platform Security Guide* also apply to SAP S/4HANA.

For non-Fiori technology SAP S/4HANA supports the following mechanisms:

- Secure Network Communications (SNC)
SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.

- SAP Logon Tickets
SAP S/4HANA supports the use of logon tickets for SSO when using a Web browser as the front-end client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication, but can access the system directly once it has checked the logon ticket.
For more information, go to https://help.sap.com/s4hana_op_2020, enter *Application Server ABAP Security Guide* into the search bar, press , open the search result with that title, and navigate to [▶ User Administration and Authentication](#) [▶ Integration in Single Sign-On Environments](#) [▶ Logon Tickets](#) [▶](#).

- Client Certificates
As an alternative to user authentication using a user ID and passwords, users using a Web browser as a front-end client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer Protocol (SSL Protocol). No passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.
For more information, go to https://help.sap.com/s4hana_op_2020, enter *Application Server ABAP Security Guide* into the search bar, press , open the search result with that title, and navigate to [▶ User Administration and Authentication](#) [▶ Integration in Single Sign-On Environments](#) [▶ Client Certificates](#) [▶](#).

For more information about the available authentication mechanisms, go to https://help.sap.com/s4hana_op_2020, enter *User Authentication and Single Sign-On* into the search bar, press , and open the search result with that title.

Fiori Technology

For details on the User Authentication and Single Sign-On concepts used in SAP Fiori apps, go to https://help.sap.com/s4hana_op_2020, enter *SAP Fiori Overview* into the search bar, press , and open the search result with that title. In addition, manual actions are required.














4 System Hardening with SAP Security Notes






Backlog of Existing Security Notes

There is also a backlog of security notes that require your attention during early phases of your SAP S/4HANA system setup. The following is a list of important security notes which include manual configuration steps and which you need to implement in your SAP S/4HANA system. These implementations/configurations can only be carried out by you due to your specific landscape and specific application environment.

i Note

Some of these SAP Notes may not be applicable in your system landscape.

SAP Note	Topic
1322944 	ABAP: HTTP security session management
1531399 	Enabling SSL for Session Protection
1585767 	Enabling Virus Scanning in SAP Content Server
1616535 	Secure configuration of ICM for the ABAP application server
1693981 	Unauthorized modification of displayed content
1853140 	Managing SAProuter from external host
1973081 	XSRF vulnerability: External start of transactions with OK-Code
2086818 	Fixing POODLE SSLv3.0 (CVE-2014-3566) Vulnerability
2107562 	Fixing POODLE SSLv3.0 (CVE-2014-3566) Vulnerability in Money Mobiliser Platform
2142551 	Clickjacking Framing Protection in AS ABAP
2185122 	Switchable authorization checks for RFC in data extraction within CA-MDG-APP-FIN
2245332 	Clickjacking Framing Protection in SAPUI5 Apps
2260344 	OS command injection vulnerability in SCTC_* Function modules

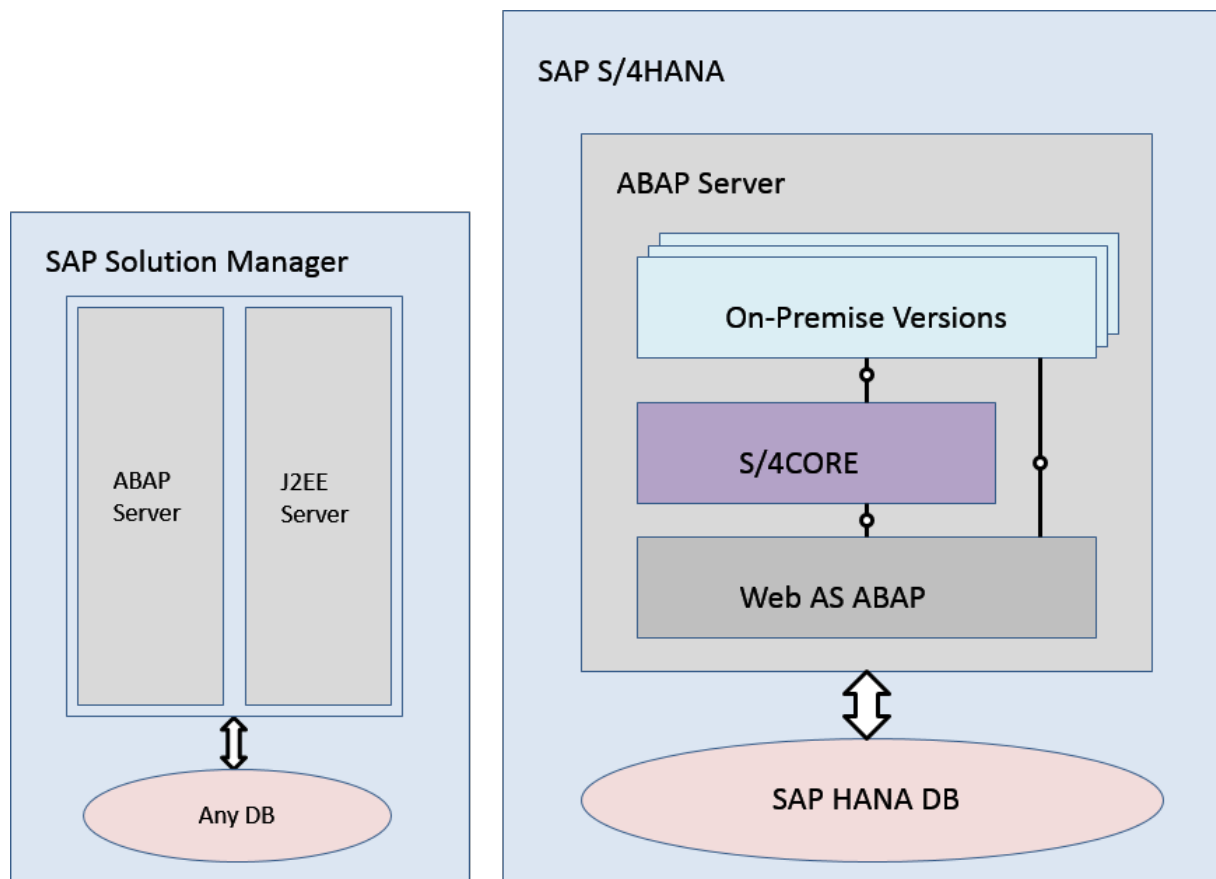
SAP Note	Topic
2319172 	Clickjacking Framing Protection in SAP GUI for HTML
2319192 	Clickjacking Framing Protection in BSP
2333957 	Clickjacking Framing Protection in SAP Fiori Launchpad for NW AS ABAP based on a list of allowed domains
2349128 	Clickjacking Framing Protection in UI theme designer on ABAP
2421287 	Front-end printing with SAP GUI 750

5 SAP S/4HANA System Landscape Information

There are various ways of deploying SAP S/4HANA in your new or already existing system landscape. This section describes some examples.

Example: SAP S/4HANA New Installation

A new installation of SAP S/4HANA needs to run on the SAP HANA database. It is recommended to use the SAP Solution Manager, which can run on any database. This very simple landscape can be enhanced with the SAP cloud solutions and SAP Business Suite products.



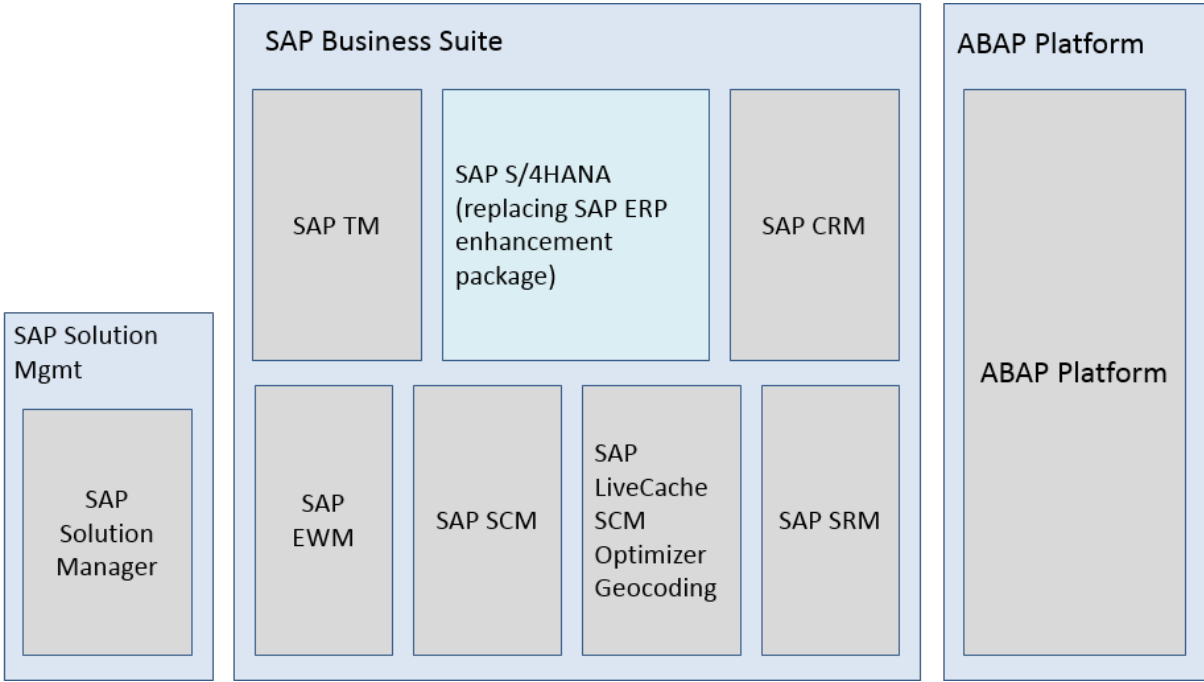
Simple SAP S/4HANA Deployment

Example: SAP S/4HANA in an SAP Business Suite Landscape

It is possible to integrate SAP S/4HANA into an existing SAP Business Suite landscape by replacing the SAP ERP enhancement package product with SAP S/4HANA. When performing this conversion in your system

landscape, you need to do some adaptations, for example you need to convert some of your existing business processes to the simplified SAP S/4HANA processes. Some of the SAP Business Suite processes are no longer supported, some have been changed, and there are also new processes. How to convert your existing processes to the SAP S/4HANA processes is described in the *Simplification Item Catalog*.

For more information about the *Simplification Item Catalog*, see the *Conversion Guide for SAP S/4HANA* at https://help.sap.com/s4hana_op_2020 ► *Implement* ► *Guides* ►.



Example SAP Business Suite landscape with an embedded SAP S/4HANA system

More Information

For more information about SAP Fiori for SAP S/4HANA see SAP Note [2590653](#).

6 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats. These threats can be based on software flaws, at both the operating system level and application level, or network attacks, such as eavesdropping.

If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system database or files.

Additionally, if users are not able to connect to the server local area network (LAN), they cannot exploit well-known bugs and security holes in network services on the server machines.

6.1 Communication Channel Security

SAP S/4 HANA uses several protocols for communication to internal and external applications. These can be SAP systems or third-party systems. The following protocols are supported:

- HTTPS
HTTP connections are protected by the Transport Layer Security (TLS) protocol. This protocol used to be known as Secure Sockets Layer (SSL).
- RFC
RFC connections can be protected using Secure Network Communications (SNC). For detailed recommendations on securing RFC connections, see SAP Note [2008727](#) and the SAP Whitepaper *Securing Remote Function Calls* attached to it.
- SOAP
SOAP connections are protected with Web services security.
- IDoc
- REST

i Note

We strongly recommend using secure protocols (TLS, SNC) whenever possible.

For more information on securing the protocols above, see the respective chapters in the ABAP Platform Security Guide.

For more information on configuring internet communication security, see SAP Note [1616535](#).

6.2 Network Security

Network

SAP S/4HANA is based on ABAP Platform technology. Therefore, for information about network security, see the respective sections in the ABAP Platform Security Guide. This includes information on using firewall systems for access control and using network segmentation.

Go to https://help.sap.com/s4hana_op_2020, enter *ABAP Platform Security Guide* into the search bar, press , and open the search result with that title.

If your system provides Internet services, you should ensure you protect your network infrastructure with a firewall at least. You can further increase the security of your system (or group of systems) by dividing the system into groups, placing the groups in different network segments, and then protecting each segment from unauthorized access by a firewall.

Bear in mind that unauthorized access is also possible internally if a malicious user has managed to gain control of one of your systems.

Ports

SAP S/4HANA is executed in ABAP Platform and uses the ports of AS ABAP. For more information, see the corresponding security guides under the topics for AS ABAP Ports.

6.3 Communication Destinations

The use of communication destination is application-specific. Therefore please check the application-specific chapters for details.

In this context please note that users and authorizations should be used with specific care, as the use of users and authorizations in an irresponsible manner can pose security risks. You should therefore follow the security rules below when communicating between application systems.

General Rules

- Employ the user types 'system' and 'communication'
- Grant a user only the minimum of authorizations
- Tell users to choose a secure password and to not divulge it to anyone else
- Only store user-specific logon data for users of type 'system' and 'communication'
- Wherever possible, use trusted system functions instead of user-specific logon data

7 ICF and Session Security

Internet Communication Framework (ICF) Services

You should handle Internet Communication Framework (ICF) services in a restrictive manner in order to minimize the attack surface on the web.

i Note

As a general rule you should only activate those ICF services that are needed for the applications running in your system.

For details on the required services, see the application-specific chapters of this guide. Use transaction `SICF` to activate or de-activate ICF services. For more information, see the SAP NetWeaver documentation.

Additional information on the required services can be found in the RFC/ICF Security Guide.

Go to https://help.sap.com/s4hana_op_2020, enter *RFC/ICF Security Guides* into the search bar, press `Enter`, and open the search result with that title.

i Note

If your firewall(s) use URL filtering, note the URLs used for the services, and adjust your firewall settings accordingly.

Session Security Protection

Secure Session Management

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management. We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

For SAP NetWeaver version 7.0 and higher, it is recommended to activate HTTP security session management using transaction `SICF_SESSIONS`. In particular it is recommended to activate extra protection of security-related cookies.

The `HttpOnly` flag instructs the browser to deny access to the cookie through client side script. As a result, even if a cross-site scripting (XSS) flaw exists, and a user accidentally accesses a link that exploits this flaw, the browser will not reveal the cookie to a third party.

The `Secure` flag tells the browser to send the cookie only if the request is being sent over a secure channel such as HTTPS. This helps protect the cookie from being passed over unencrypted requests.

These additional flags are configured through the following profile parameters:

Profile Parameter	Recommended Value	Description	Comment
icf/ set_HTTPOnly_flag_on_cookies	0	Add HttpOnly flag	Client-dependent
login/ticket_only_by_https	1	Add Secure flag	Not client-dependent

For more information, a list of the relevant profile parameters, and detailed instructions, see *Activating HTTP Security Session Management on AS ABAP* in the AS ABAP security documentation.

8 File System Access Security

More Information

For detailed information about data storage security, see the ABAP Platform Security Guide.

Using Logical Paths and File Names to Protect Access

Some applications in SAP S/4HANA save data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files - a security issue also known as directory traversal. This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime. If access is requested to a directory that does not match a stored mapping, then an error occurs.

In the application-specific part of this guide, there is a list of the logical file names and paths for each component. It also specifies for which programs these file names and paths apply.

Activating the Validation of Logical Paths and File Names

You enter the logical paths and file names in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation on path level at runtime, enter the physical path using the transactions `SFILE` (client-independent) and `SF01` (client-dependent). To determine which paths are used by your system, you can activate the appropriate settings in the Security Audit Log. The relevant SAL events are CUQ, CUR, CUS, CUT, DU5 and EU4.

For new installations it is recommended to enforce path validation as a default by setting `REJECT_EMPTY_PATH=ON` in table `FILECMCUST` (transaction `SM30`). For details see SAP Note [2251231](#) - *File validation enforcement switch for empty physical path*.

For more information, go to https://help.sap.com/s4hana_op_2020, enter one of the following titles into the search bar, press and open the search result with the relevant title.

- *Logical File Names*
- *Protecting Access to the File System Using Logical Path and File Names*
- *Security Audit Log*

9 Virus Scanning

Basic Concepts

We recommend installing and running a VSI 2.x-compliant virus scanner in your landscape. The SAP S/4HANA code calls this scanner using a dedicated interface during different stages of processing - during upload, download, and passage through the Gateway, and so on. You can customize the interface with the help of scan profiles.

We recommend running VSI scans for:

- Signature scans
All files should be checked against an up-to-date list of known virus signatures.
- Mime-type detection
Only trusted file types should be allowed.
- Active content detection
Files with active content should be blocked (for example, PDF files containing JavaScript).

For more information about virus scan profiles and customizing, go to https://help.sap.com/s4hana_op_2020, enter *Virus Scan Interface* into the search bar, press `Enter`, and open the search result with that title.

Additional information is available in SAP Notes [786179](#) and [1494278](#).

For virus scanning in SAP Content Server, see SAP Note [1585767](#).

9.1 Virus Scanning in File Uploads

Example

The system allows uploading of files. For example, users can add an attachment to business documents. Also, you can upload template files, such as e-mail HTML templates, which can be used to render data on a UI

Once uploaded into SAP S/4HANA, such documents may be displayed in SAP Fiori apps without further security-related checks. If a document contains malicious content, unintended actions could be triggered when the item is downloaded or displayed. This can lead to situations, such as cross-site scripting vulnerabilities. That is why proper virus scanning at upload time is an essential first line of defense against (stored) XSS attacks.

For a technical description of this problem see the *ABAP Platform Security Guide*.

Go to https://help.sap.com/s4hana_op_2020, enter *Preventing Cross-Site Scripting From Uploads* into the search bar, press `Enter`, and open the search result with that title.

It is clear that uploaded files need to be scanned for malware. Also, their type needs to be verified against a allowlist of MIME-types. You can meet both these requirements by installing and running a VSI 2.x-compliant virus scanner in your landscape.

SAP S/4HANA code calls the virus scanner (at upload time) through a dedicated interface, which you can customize. The pre-delivered scan profile, /SCMS/KPRO_CREATE, needs to be adapted according to your needs. At runtime the virus scanner rejects all upload documents that are not compliant with the rules specified in the scan profile.

i Note

Changes to the scan profile have a global effect. This means, for example, that all uploads ending up in KPro face the same virus scan settings at runtime.

9.2 General Recommendations for Virus Scan Profiles

Selecting Pre-Delivered Scan Profiles

As a first step, you should enable all the pre-delivered scan profiles. You should then consider performance issues when deciding which ones to disable.

Some scan profiles take effect at download time. One benefit of scanning at download time is that if a virus signature is updated since upload, it can be caught at download time. So if a compromised file is uploaded, it is discovered at download. However, download scanning can impact performance. That is because a file is uploaded only once, but it may be downloaded many times.

If you want to disable download time scanning, disable the following scan profiles:

- /SCET/GUI_DOWNLOAD
- /SIHTTP/HTTP_DOWNLOAD
- /SOAP_CORE/WS_SEND

Customer Profiles

You should set up the following customer profiles:

Name	Description
ZBASIC	Basic virus scanning profile
ZEXTENDED	Same as above with additional check for active content, and MIME-type detection

All active profiles should refer to ZEXTENDED, except the following, which should refer to ZBASIC.

- /SAPC_RUNTIME/APC_WS_MESSAGE_GET
- /SAPC_RUNTIME/APC_WS_MESSAGE_SET
- /SCET/GUI_UPLOAD

- /SIHTTP/HTTP_UPLOAD
- /SMIM_API/PUT
- /SOAP_CORE/WS_RECEIVE
- /UI5/UI5_INFRA_APP/REP_DT_PUT

For ZEXTENDED, the following settings are recommended:

- CUST_ACTIVE_CONTENT = 1
- CUST_CHECK_MIME_TYPE = 1
- CUST_MIME_TYPES_ARE_BLACKLIST = 0
This setting indicates 'allowlisting' - which indicates entities that are OK.

These settings tell the virus scanner to scan for active content and check MIME types according to the specified allowlist of file types.

Allowlist

Use the 'allowlisting' file type wherever possible.

Consider the following: the allowlist scanner should be as restrictive as possible. As a compromise, the list should also contain the complete set of file types required in all active customer scenarios. If you need to extend the allowlist, you should ensure that the list only contains MIME types from the [IANA List](#) .

Template List of File Types

i Note

Your allowlist should be as restrictive as possible. For example, you should delete non-needed types from the template list. A final allowlist is always a compromise between security and functionality.

Use the template list of file types for consideration.

- application/arj
- application/msword
- application/pdf
- application/postscript
- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
- application/vnd.openxmlformats-officedocument.presentationml.presentation
- application/vnd.openxmlformats-officedocument.wordprocessingml.document
- application/x-compressed
- application/x-dvi
- application/x-gzip

- application/x-zip-compressed
- application/xml
- application/zip
- image/bmp
- image/jpeg
- image/png
- image/vnd.dwg
- image/x-dwg
- text/plain
- text/richtext
- text/xml

9.3 Further Protection Against Active Content

Lines of Defense

There are at least two lines of defense against active content. The first is performing virus scanning in order to avoid uploading malicious content in the first place.

The second line of defense is SAP WebDispatcher. An alternative is the Internet Communication Manager (ICM). These protect against malicious active content being executed at the front end. This uses additional HTTP-response headers to instruct browsers to behave in a specific way. SAP WebDispatcher and ICM both offer the possibility to modify HTTP-response headers.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Administration of the ICM* into the search bar, press , open the search result with that title, and navigate to [Modification of HTTP Requests > Deleting, Adding, and Enhancing HTTP Header Fields](#).

SAP recommends adding the following headers:

- SetResponseHeader X-Content-Type-Options "nosniff"
This tells the browser not to try reading the attached file with the assumed MIME type.
- SetResponseHeader X-XSS-Protection "1; mode=block"
This prevents cross-site scripting.

Example: Secure Header Settings

Consider the following example of script code. It shows how to improve the security level. You need to adapt it to your own use case.

```
If %{RESPONSE_HEADER:Content-Disposition} regimatch ^inline [AND]
If %{RESPONSE_HEADER:Content-Type} regimatch html|xml|xsl
Begin
SetResponseHeader Content-Security-Policy "script-src 'none'; sandbox"
```

```
SetResponseHeader X-Content-Security-Policy "script-src 'none'; sandbox"  
End
```

If such a Content-Security-Policy header is added to HTTP responses containing previously uploaded files (when displayed inline and having content type containing html, xml or xsl), the execution of Javascript will be prevented at the frontend by all up-to-date browser versions.

10 Additional System Hardening Activities

Click-Jacking Protection

Click-jacking is an attack type where an attacker tries to hijack the clicks of an authenticated user in order to trigger malicious actions. This attack is based on framing the attacked page into an attacker-controlled enclosing page.

SAP S/4HANA uses an ABAP Platform protection to prevent click-jacking attacks. This is an allowlist-based solution that controls which pages are allowed to render your application within a frame. To enable the protection, you need to access and edit the allowlist.

A typical setup will contain host/port of the system (as seen from a browser) and host/port of any trusted system that hosts applications which are going to frame applications from the current system.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Using an Allowlist for Clickjacking Framing Protection* into the search bar, press and open the search result with that title.

SAP GUI for HTML transactions, Web Dynpro applications, and non-SAPUI5-based applications already use this flexible protection mechanism. SAP Fiori launchpad currently uses a slightly different, high security solution.

Unified Connectivity

If your SAP S/4HANA system can be accessed remotely using Remote Function Calls (RFCs), you can significantly increase protection by using the Unified Connectivity (UCON) administration framework.

Generally, external access to the function modules using RFCs is controlled by special authorization checks and the corresponding roles with purpose-specific assignments to users. UCON also provides a simple but comprehensive way of controlling which Remote Function Modules (RFM) can be called by other systems: an RFM can only be called externally if it is assigned to a Communication Assembly (CA).

External access is blocked for all RFMs not assigned to a CA. In this way, it is possible to control and restrict external access to RFMs independently from the user context.

For details, go to https://help.sap.com/s4hana_op_2020, enter *Unified Connectivity* into the search bar, press and open the search result with that title.

Switchable Authorizations Check Framework (SACF)

The Switchable Authorizations Check Framework (SACF) provides additional authorization checks for specific scenarios. These checks do not change the behavior of the application until you activate the respective scenario. A scenario definition comprises certain authorization objects and rules telling the system how to check them. An active scenario is a development object, which can be transferred through your landscape.


By default, most additional scenario-based authorizations checks are initially set to inactive in SAP S/4HANA (for compatibility reasons).

For more information, see the chapter *Activating Switchable Authorization Checks* in the SAP Whitepaper *Securing Remote Function Calls* which is attached to SAP Note [2008727](#) .

i Note

From a security perspective, SAP strongly recommends to activate all scenario-checks in SAP S/4HANA in order to maximize the resilience of systems.

Use the transaction `SACF` for the customizing and transaction `SACF_COMPARE` for comparison.

Please also read the important information contained in SAP Note [1922808](#) .

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Customizing Scenario-Based Authorizations* into the search bar, press and open the search result with that title.

Securing CALL TRANSACTION Statements

When a user manually launches an SAP transaction, the ABAP Kernel automatically checks the user's corresponding authorization (Authorization Object `S_TCODE`).

The system behaves differently if an SAP transaction is called by a program (ABAP statement `CALL TRANSACTION`). In this case, the authorization check (`S_TCODE-`) depends on the system configuration. This can be controlled using transaction `SE97` and profile parameter `auth/check/calltransaction`.

Two cases exist:

- **New installations**
We recommend setting the profile parameter `auth/check/calltransaction=3`. This switches on the authorization check for `CALL TRANSACTION` statements – as long as you have not explicitly switched it off using transaction `SE97`. This improves the security level because all roles need to contain appropriate authorizations.
- **Installations migrated from an SAP ERP enhancement package to SAP S/4HANA**
Roles formerly used in SAP ERP must be examined thoroughly and adopted with care into the new SAP S/4HANA environment. Only for the sake of a smooth transition you can avoid this temporarily by setting `auth/check/calltransaction=2`. This keeps the check behavior as it was before. However, as a permanent setting this is **not** recommended, as in the end you should adopt your roles to the new environment actively and with care.

For details, see the system documentation of transaction `SE97`.

11 Data Protection and Privacy

Use

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data protection acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data protection.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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 given system landscape and the applicable legal requirements.

i Note

In the majority of cases, compliance with data privacy laws is not a product feature.

SAP software supports data protection 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.

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	The information that specifies the reason and the goal for the processing of a specific set of personal data . As a rule, the purpose references the relevant legal basis for the processing of personal data.

Term	Definition
Blocking	A method of restricting access to data for which the primary purpose has ended.
Deletion	Deletion of personal data so that the data is no longer usable.
Retention period	The period of time between the end of the last business activity involving a specific object (for example, a business partner) and the deletion of the corresponding data, subject to applicable laws. The retention period is a combination of the residence period and the blocking period.
End of purpose (EoP)	The point in time when the processing of a set of personal data is no longer required for the primary business purpose, for example, when a contract is fulfilled. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorizations (for example, tax auditors).

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

Access control: Authentication features as described in section [User Administration and Authentication \[page 10\]](#).

Authorizations: Authorization concept as described in section [User Management \[page 10\]](#).

Read access logging: as described in section [Read Access Logging \[page 33\]](#).

Transmission control / Communication security: as described in section [Network and Communication Security \[page 19\]](#).

Input control / Change logging

Availability control as described in:

- Section [Data Storage Security \[page 23\]](#)
- Go to https://help.sap.com/s4hana_op_2020, enter *SAP Business Continuity* into the search bar, press , and open the search result with that title.

Separation by purpose: Is subject to the organizational model implemented and must be applied as part of the authorization concept.

⚠ Caution

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

You also need to make sure that no personal data enters the system in an uncontrolled or non-purpose related way, for example, in free-text fields, through APIs, or customer extensions. Note that these are also not subject to the RAL example configuration.

Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped in Customizing for *Cross-Application Components* under *Data Protection*.

Additional industry-specific, scenario-specific or application-specific configuration might be required.

For information about the application-specific configuration, see the application-specific Customizing.

More Information

You can find detailed information on data protection in the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under [Product Assistance](#) > [Cross Components](#) > [Data Protection](#).

11.1 Read Access Logging

Use

Read access to personal data is partially based on legislation, and it is subject to logging functionality. The Read Access Logging (RAL) component can be used to monitor and log read access to data and provide information such as which business users accessed personal data (for example, fields related to bank account data), and when they did so.

In RAL, you can configure which read-access information to log and under which conditions.

SAP delivers sample configurations for applications.

You can display the configurations in the system by performing the following steps:

1. In transaction SRALMANAGER, on the *Administration* tab page, choose *Configuration*.
2. Choose the desired channel, for example, WebDynpro.
3. Choose *Search*. The system displays the available configurations for the selected channel.
4. Choose Display Configuration for detailed information on the configuration. For specific channels, related recordings are also be displayed.

i Note

For a list of the delivered log domains, see the product assistance at SAP Help Portal under https://help.sap.com/s4hana_op_2020 > [Product Assistance](#) > [Cross Components](#) > [Data Protection](#).

Prerequisites

Before you can use the delivered RAL configurations, the following prerequisites are met:

- The RAL configurations have been activated.
- You have enabled RAL in each system client.

More information

For more information, see the following sections on https://help.sap.com/s4hana_op_2020:

- Enter *System Security for SAP NetWeaver AS for ABAP Only* into the search bar, press and open the search result with that title. Navigate to the section *Read Access Logging*.
- Enter *Services for Application Developers* into the search bar, press and open the search result with that title. Navigate to the section *Change Documents*.
- Enter *Read Access Logging (RAL) and OData* into the search bar, press and open the search result with that title.

For up-to-date information on the delivered RAL configurations, see SAPNote [2347271](#).

11.2 Deletion of Personal Data

Personal data in a system can be blocked as soon as the business activities for which this data is needed are completed and the residence time for the data has elapsed. After this time, only users who are assigned additional authorizations can access the data.

When the retention period has expired, personal data can be destroyed completely so that it can no longer be retrieved. Residence and retention periods are defined in the customer system.

For this purpose, SAP uses SAP Information Lifecycle Management (ILM) to help you set up a compliant information lifecycle management process in an efficient and flexible manner.

More Information

For more information, see the application-specific sections in this security guide as well as at https://help.sap.com/s4hana_op_2020 under [▶ Product Assistance](#) [▶ Cross Components](#) [▶ Data Protection](#) [▶](#).

11.3 Information Retrieval

Data subjects have the right to get information regarding their personal data undergoing processing, including the reason (purpose) for processing.

The *Information Retrieval Framework* component can be used to carry out a cross-application search for personal data of a specified data subject. The data is retrieved from the system and displayed in a structured, easy-to-read list, subdivided according to the purposes for which the data was initially collected and processed.

i Note

To be able to use the IRF, you must set up your own data model which is the basis for the retrieval process. The data model contains all relevant database tables that are searched for personal data. The IRF assists you in automatically generating an initial data model which you must then verify/ enhance with the help of the IRF modeling tools.

Apart from setting up a data model, you must also maintain the purposes relevant to your organization.

Once you have set up a data model, you can use the following reports to retrieve personal data from the system:

- *Start Data Collection* report (transaction DTINF_START_COLL) to trigger the retrieval process.
- *Process Data Collection Results* report (transaction DTINF_PROC_COLL) to get an overview of all data collection requests as well as to display and download the search results.

More Information

For more information about setting up and using the IRF, see https://help.sap.com/s4hana_op_2020 under ► *Discover* ► *Product Assistance* ► *Enterprise Technology* ► *ABAP Platform* ► *Administering the ABAP Platform* ► *Administration Concepts and Tools* ► *Solution Life Cycle Management* ► *Information Retrieval Framework (IRF)* ►.

For more information about data protection, see https://help.sap.com/s4hana_op_2020 under ► *Discover* ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

11.4 Consent Administration

Use

Any personal data collected or processed must be linked to a specific, predefined purpose, such as the fulfillment of a contract or legal obligation.

If you must obtain consent from the data subject to use their personal data, this consent data can be stored in the SAP system as consent records.

Consent Administration enables you to search for and display stored consent records as well as to import consent records as copies from either a file (stored on your device/ an application server) or via a Web Service (e.g. the SAP Consent Repository service available on the SAP Business Technology Platform). In addition, the feature helps you to manage the retention of consent data, to control access to consent data as well as to support the process of blocking and deletion of business partner master data.

More Information

- For more information about Consent Administration, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 and go to ► *Product Assistance* ► *Cross Components* ► *Data Protection* ► *Consent Administration* ►.
- For more information about the SAP Consent Repository, see [SAP Consent Repository](#).
- For more information about the JSON file structure necessary for the import of consent records, see SAP Note [2607792](#) ►.

12 SAP S/4HANA Cross Application Infrastructure

12.1 Data Security in SAP ILM

SAP ILM offers options for protecting data security from the archiving of data up to its storage and destruction. All system connections and ILM functions have authorization protection.

Related Information

[Data Security in SAP ILM System Connections \[page 37\]](#)

[Users and Authorizations in SAP ILM \[page 38\]](#)

[Security of Stored Data in SAP ILM \[page 39\]](#)

[Logs in SAP ILM \[page 40\]](#)

12.1.1 Data Security in SAP ILM System Connections

System Landscape Components

The *SAP ILM* system landscape includes the following main components:

- Application system (AS ABAP)
- WebDAV server on which ILM stores are set up
- System on which the service for the control of ILM stores runs
Since two different services are available for controlling ILM stores, two system landscape variants are possible.
 - The *Storage and Retention Service (SRS)* runs either in the application system (AS ABAP) or on a separate AS ABAP.
For more information, see [Configuring Storage and Retention Service for ILM Stores under SAP Information Lifecycle Management](#).
 - *XML Data Archiving Service (XML DAS)* runs on an AS ABAP.
For more information, see [Configuring XML Data Archiving Service for ILM Stores under SAP Information Lifecycle Management](#).

Data Security for System Connections

Communication between systems takes place with HTTP connections.

HTTP Connection between Application System and ILM Store Service

If the service (*SRS* or *XML DAS*) runs on a separate system, you need an HTTP connection from the application system to that system. You use an HTTP or HTTPS protocol. The configuration of the HTTP connection is described in the documentation for the relevant service.

If you use the local *SRS* service of the application system to control ILM stores, you do not need a connection.

HTTP Connection between ILM Store and ILM Store Service

The ILM Stores that are set up on a WebDAV server need to be connected to a service with an HTTP connection. A WebDAV protocol, which is an enhancement of the HTTP protocol, is used. The configuration of the HTTP connection is explained in the documentation for the relevant service.

User Authentication for System Connections

The application system can access the service with an HTTP connection only if the connection is made by a user who has the corresponding authorizations. This user must be created in the system on which the service run and entered in the data for the HTTP connection.

In the case of a connection from the service to the WebDAV server, user authentication is performed according to the options offered by the WebDAV server. SAP supports basic authentication with a user of the WebDAV server (with password) as well as with SSL.

12.1.2 Users and Authorizations in SAP ILM

User

To make *SAP ILM* available, you need users for the communication between the participating systems (using HTTP connections).

For more information, see Data Security in SAP ILM System Connections under SAP Information Lifecycle Management.

Authorizations

SAP delivers roles with the relevant authorizations for access to the functions of *SAP ILM*.

For more information, see the following topics under SAP Information Lifecycle Management:

Assigning Authorizations for Retention Management Cockpit

Assigning Authorizations for Retention Warehouse Cockpit

Transactions and Authorizations in SAP NetWeaver ILM

12.1.3 Security of Stored Data in SAP ILM

Security of Archived Data in the File System

When storing archived data in the file system, you have read and write access to the file system with the technical system user of the SAP system. The system temporarily moves the archive files to the file system and then deletes them after forwarding them to the ILM store. The archive files in the file system and the ILM store are stored not in plain text but in binary text in an SAP-specific, compressed format.

A logical path defines the storage location of the archived data in the file system. You need to specify this path in Customizing for the archiving object.

For more information, see:

[Data Archiving](#) in the SAP NetWeaver Library

[Security Guide for ADK-Based Data Archiving](#) in the Security Guide of the SAP NetWeaver Library

Security of Data in the ILM Store

To guarantee the non-changeability of data and the protection from early deletion, the resources (archive files) and their higher level collections (hierarchy nodes of the store) are stored on an ILM-certified WebDAV server.

Metadata Security in the Store Hierarchy

To manage the store hierarchies, the service that you use to manage ILM stores saves the metadata to the system database. Depending on which service you use, the storage location of the metadata is:

ILM Store Service	Metadata Storage Location
Storage and Retention Service (SRS)	Database of the AS ABAP on which the SRS runs
XML Data Archiving Service (XML DAS)	Database of the AS ABAP on which <i>XML DAS</i> runs <i>XML DAS</i> uses the database pool alias <i>SAP/BC_XMLA</i> .

You can guarantee the security of the metadata with the standard functions of the database you are using.

For more information, see: [Database Access Protection, Security Aspects for Database Connections](#) in the SAP NetWeaver Library.

Backup of Complete Data in the Retention Warehouse System

To ensure that the dataset you are managing in Retention Warehouse is still complete after the transfer from the legacy system, use the checksums function before and after the transfer and the ILM-compliant conversion of the data (archive files).

12.1.4 Logs in SAP ILM

In *SAP ILM*, logging depends on the service you use to control the stores.

Service Used	Type of Log File	Server	Description
<i>Storage and Retention Service (SRS)</i>	Log File for SRS	AS ABAP on which SRS runs (application system or separate system)	Can be called in application log Log object: ILM Subobject: ILM_SRS
<i>XML Data Archiving Service (XML DAS)</i>	Log File for XML DAS	AS Java on which XML DAS runs	Can be called in <i>LogViewer</i> File: applications.log Category: /Applications/Common/Archiving/XML_DAS
	Trace File for XML DAS	AS Java on which XML DAS runs	Can be called in <i>LogViewer</i> File: defaultTrace.trc Location: com.sap.archtech.daservice
<i>Service-Independent</i>	Log File of Connector	Application system (AS ABAP)	Can be called in the job log for AS ABAP
	System Log (syslog)	Application system (AS ABAP)	Entry in the system log (operation trace) with message ID DA1 and problem class S for each deletion of a resource or collection in the ILM store

Service Used	Type of Log File	Server	Description
	Log Files for ILM Functions	Application system (AS ABAP)	<p>Can be called in application log</p> <p>Log object: ILM</p> <p>Subobjects:</p> <ul style="list-style-type: none"> • ILM_ALINK_REFERENCES (ArchiveLink references) • ILM_CHANGE_RETENTION (Change of retention period) • ILM_CHECKSUM (Checksum generation) • ILM_DESTRUCTION (Data destruction) • ILM_LEGAL_CASE (Set legal holds) • ILM_LH_PROPAGATION (Using holds on data) • ILM_SWISS_KNIFE (Enhancing CDE contents in RW) • ILM_TRANS_ADMIN (Transfer of archive administration data from the legacy system to RW) • ILM_UOM (Comparing units of measure in RW) • IRM_RT (Rule determination) • GENERATE (Generating BW objects) • TRANSFER (Transferring table structures from RW to BW) • TRANSFER_VIEW (Transferring data views from RW to BW) • DELETE (Deleting BW objects and data) • WP_CREATE (Creating audit packages in RW)

12.2 Payment Card Security

12.2.1 Before You Start

Since the measures described in this guideline for security in the use and administration of payment cards apply in various applications, see the security guides for those particular applications.

The most important SAP Notes that apply to secure handling of payment card data are shown in the table below.

SAP Note	Title	Comment
1032588	Secure handling of credit card data in S/4HANA	
1151936	Key replacement for encryption of payment card data	
662340	SSF Encryption using SAPCryptolib	
1394093	Security collective note	Summarizes information about various security-relevant problems

12.2.2 Authorizations

The functions for secure handling of payment cards use the authorization concept provided by ABAP platform. Therefore, the recommendations and guidelines for authorizations as described in the *ABAP Platform Security Guide* also apply to the secure handling of payment cards.

The ABAP platform authorization concept is based on assigning authorizations to users based on roles. For the role maintenance for ABAP technology, use the profile generator (transaction PFCG).

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used as part of secure handling of payment cards.

Authorization Object	Field	Value	Description
B_CCSEC	ACTVT	03	Display of unmasked payment card numbers
B_CCSEC	ACTVT	06	Deletion of data records no longer needed and log entries for displaying payment card data
B_CCSEC	ACTVT	71	Display of log entries for displaying payment card data
SSFVADM	ACTVT	01	Generating a key version
	SSFVAPPLIC	PAYCRV	

Authorization Object	Field	Value	Description
	ACTVT	06	Deleting a key version
	SSFVAPPLIC	PAYCRV	
	ACTVT	42	Execution of migration programs for SSF application
	SSFVAPPLIC	PAYCRV	PAYCRV

12.2.3 Data Storage Security

Use

Since payment card data is needed by many different applications for operational processes, the data is stored on the database. If you choose the security level *Masked Display, and Encrypted When Saved*, the system stores payment card numbers in encrypted form on the database in the following database tables:

Database Table	Use	Comment
PCA_SECURITY_RAW	Payment Cards and SAP Business Partner	In S/4HANA systems, you must execute a migration program.
CCARDEC	Payment Cards in FI, SD and Customer Master	
CCSEC_ENC	Other payment card processes	The table is used if the indicator for periodic key replacement is not set in Customizing.
CCSEC_ENCV	Other payment card processes	The table is used if the indicator for periodic key replacement is set in Customizing.

The application database tables refer to these encrypted storage tables.

You can archive and delete the data using the following archiving objects or deletion programs:

Database Table	Deletion/Archiving	Comment
PCA_SECURITY_RAW	Archiving using archiving object CA_PCA_SEC	
CCARDEC	Deletion using program CCARDEC_DELETE	If the data is used in an unarchived FI document, customer master record, or order, the data is not deleted.

Database Table	Deletion/Archiving	Comment
CCSEC_ENC	Archiving using archiving object CA_PCA_SEC	
CCSEC_ENCV	Deletion using program RCCSECV_ DATA_DEL	The data cannot be deleted unless the last use was more than 500 days in the past.

12.2.4 Setting Up Encryption Software

To be able to encrypt payment card data in the system, you must install the function package SAPCRYPTOLIB. The function package SAPCRYPTOLIB contains the functions necessary for encryption. To execute the encryption software, you have to make general settings in Customizing for SAP NetWeaver. Choose [▶ Application Server ▶ System Administration ▶ Maintain the Public Key Information for the System ▶](#).

For more information, see SAP Note 662340.

12.2.5 Making Settings for Payment Card Security

You make settings for payment card security in Customizing for Cross-Application Components under [▶ Payment Cards ▶ Basic Settings ▶ Make Security Settings for Payment Cards ▶](#).

The following explanations refer to the settings there.

Security Level

You can select from the following options:

- No Additional Security Measures
- Masked Display, Not Encrypted When Saved
- Masked Display and Encrypted When Saved

Masked display means that when you display or change objects that contain a payment card number, the system hides part of the number.

❖ Example

For payment card number 1111222233334444, the system displays a value of 1111*****4444.

You can specify the number of visible characters at the beginning and end of the payment card number. The security standards of the payment card industry demand that a maximum of six characters are visible at the beginning, and four at the end.

This masked display is applied for all types of payment cards. If you also select encrypted saving, then the system applies this only to those payment card types that you specified explicitly in Customizing (see the section "Relevant Payment Card Types").

We recommend that you use the security level *Masked Display, and Encrypted When Saved*. You should specify the smallest number of visible characters possible that allows the payment cards to be identified (for example, using the last four characters).

Unmasked Display

If card numbers are displayed in masked format, it is still sometimes necessary to display the number unmasked. In various transactions, we therefore provide a function for unmasked display of payment card numbers. You can make two specifications for this function in Customizing:

- Access log
- Additional authorization check

You can have the system record each display of an unmasked payment card in an access log. This enables you to monitor which users have displayed which payment card numbers and when.

You can use an additional authorization check for authorization object B_CCSEC to restrict the use of the display of unmasked card numbers.

We recommend that you activate this additional authorization check and assign the appropriate authorization only to those user groups that need to access unmasked card numbers as part of their daily work. You should also activate the access log.

Analyzing Access Logs

You can run reports on accessing of payment card data. For more information, see [Security-Relevant Logs and Tracing \[page 49\]](#).

Key Replacement

By setting the *Key Replacement Active* indicator, you specify that the system supports periodic replacement of the keys (PSEs) used for encryption.

Caution

This indicator is visible only if you installed S/4HANA 6.0 with Enhancement Package 4 and activated the business function *Periodic Key Replacement for Payment Card Encryption* (PCA_XKEYV).

We recommend that you set this indicator.

Relevant Payment Card Types

You can choose the card types (such as, AMEX, Mastercard, VISA) for which you want to activate encryption. The column for this is not visible in the settings for the payment card unless you have already made settings for payment card encryption in the business partner. This means that you have to have already executed the migration program or to have set up encrypted saving of further data records. You can make these settings in Customizing for Cross-Application Components under [▶ Payment Cards ▶ Basic Settings ▶ Maintain Payment Card Type ▶](#).

12.2.6 Relevant SSF Applications

For encryption and decryption using the SSF Framework, the applications communicate using an SSF application. The keys (PSEs) used for encryption and decryption are generated for each SSF application.

If you have not activated key replacement, then, for technical reasons, various SSF applications exist for the various storage files of encrypted payment card data. If you set the [Key Replacement Active](#) indicator, then only the SSF application PAYCRV is used after that point.

Application	SSF Application, If Key Replacement Inactive	SSF Application, If Key Replacement Active
Payment Cards and SAP Business Partner	PAYCRD (in S/4HANA systems)	PAYCRV
Payment Cards in FI, SD and Customer Master	CCARD	PAYCRV
Other payment card processes	PAYCRD	PAYCRV

The SSF application PAYCRV supports management of multiple key versions. This is not the case with the SSF applications PAYCRD and CCARD. Therefore, using the SSF application PAYCRV is mandatory for the process of periodic key replacement.

12.2.7 Generating Keys

The generation of the keys (PSEs) used for encryption and decryption differs depending on the SSF application:

- **SSF Application *PAYCRV**

To generate a key version, on the SAP Easy Access screen, choose [▶ Cross-Application Components ▶ Security of Payment Card Data ▶ Encryption of Payment Cards ▶ Administration of Key Versions for PAYCRV ▶](#). The system automatically generates the PSEs and distributes them to the application servers. You can display them in the transaction STRUST (Trust Manager).

The transaction for administration of key versions, in addition to the overview of already generated key versions, also provides information on how many data records are encrypted and stored on the database for a version. There you can create new key versions and delete key versions that are no longer used.

- **SSF Applications CCARDEC and PAYCRD**

In transaction SSFA, create a new entry for an SSF application. Create the PSE in transaction STRUST, and make sure that you use the algorithm RSA.

12.2.8 Migration of Payment Card Data Stored in Unencrypted Form

You can use several migration programs to migrate payment card data stored in unencrypted form to encrypted payment card data. These programs comply with the naming convention RCCSEC_MIGRATION_*. For information on which program you can use for your system, see the documentation of the individual programs.

You execute the program to store all payment card data in your system in encrypted form. For operative processes, you do not have to execute the migration programs. In addition, you can perform the conversion in several individual steps, whereby you convert only part of the data in each step.

Note that there are special issues related to the SAP Business Partner. For more information, see this [section \[page 47\]](#).

12.2.9 Migration of Payment Card Data on SAP Business Partner

The following section is relevant for you only if you use the SAP business partner.

For the SAP business partner in S/4HANA systems to support encrypted storage of payment card data, a one-time data migration is required.

Before this migration, the system manages the payment card data in the database tables listed below (among others). In both tables, the payment card number is in plain text.

Database Table	Use
CCARD	Data of payment card
BUTOCC	Relationship between SAP business partner and payment card using CCINS and CCNUM

You migrate the data of database table CCARD completely to the database tables PCA_SECURITY_*. On the SAP Easy Access screen, choose [Cross-Application Components](#) > [Security of Payment Card Data](#) > [Encryption of Payment Cards](#) > [Migration of Credit Cards](#). The encrypted value of the credit card number is stored during this process in the table PCA_SECURITY_RAW. The relationship to the credit card is reflected in table CCARD by the field CARD_GUID, and the fields CCNUM and CCINS are initialized. The system considers only those entries in table CCARD that are still used in table BUTOCC.

Database Tables

Database Table	Use
PCA_SECURITY_*	Data of payment card
BUTOCC	Relationship between SAP business partner and payment cards using CARD_GUID

When migrating using the above program, you cannot spread the conversion over time. That means you have to completely convert the data in one run. The actual encryption can either take place directly during the migration, or you can encrypt the data later using program PCA_MASS_CRYPTING.

You are required to run the migration program even if you have not yet stored any payment card data in the business partner data (for instance, at the time of installation), but you want to store encrypted data in the future.

You cannot work with the system during the migration or after a partially successful migration, since it is not possible to predict how the executing programs will react. However, severe inconsistencies are to be expected.

To execute the migration program, you need an access code that SAP provides upon request. To request this code, enter a customer message under component AD-MD-BP. Refer to this security guide or to SAP Note 1032588.

For security reasons, the system stores a backup copy of the table entries in table CCARD_COPY. After you have ensured that the system works correctly after the migration, you can delete the backup copy using program RCC_MIGRATION_DEL_COPY.

If you are using Contract Accounts Receivable and Payable (FI-CA), and are using the business partner shadow table there to improve the performance of mass runs, also see the explanations in the Security Guide for Contract Accounts Receivable and Payable in the section [Payment Card Industry Data Security Standard \[page 132\]](#).

12.2.10 Migration to SSF Application PAYCRV

If you already encrypted credit card data in the system (using the SSF applications PAYCRD or CCARD), you can migrate this data to the SSF application PAYCRV. As a result, the system then also replaces the keys for this data on a periodic basis.

Start the migration on the SAP Easy Access screen under [Cross-Application Components](#) > [Security of Payment Card Data](#) > [Encryption of Payment Cards](#) > [Migration to SSF Application PAYCRV](#). You can migrate each of the affected database tables individually and you can enter a maximum runtime. This means that in this case you can spread the conversion out over time.

12.2.11 Migration to Current Key Version

Once you have generated a new key version, you can migrate the data, which was encrypted and stored under an older key version, to the current key version. During this process, the system decrypts the data record with

the older key version, encrypts the data with the current key version, and updates the database tables. After the migration is complete, the system does not contain any more data records that still use the older key version. At that point in time, you can specify that the older key version is deletable.

To run the migration, on the SAP Easy Access screen, choose ► [Cross-Application Components](#) ► [Security of Payment Card Data](#) ► [Encryption of Payment Cards](#) ► [Execute Conversion](#) . You can define parallel processing for the migration using the subarea. The entire dataset is divided into subareas represented by the numbers 000 to 999. The subareas contain a roughly equal number of encrypted records. You can start the migration program with intervals determined by the subarea, so that up to 1000 parallel jobs are possible. In addition, you can enter a maximum runtime. This means that you can make the conversion in stages.

12.2.12 Deleting a Key Version

Once the data of an old key version has been migrated completely to the current key version, the old key version receives the status *deletable*. To ensure the utmost security, the earliest the key version can actually be deleted is after an additional waiting period of 90 days after the successful migration.

12.2.13 Security-Relevant Logging and Tracing

Use

You can have the system log users' access to unmasked payment card data. In Customizing, choose the setting [Access Log: Logs for Unmasked Display](#) (see [Making Settings for Payment Card Security \[page 44\]](#)).

The system updates the log on database table CCSEC_LOG. You can carry out an analysis via the SAP Easy Access screen, under ► [Cross-Application Components](#) ► [Security of Payment Card Data](#) ► [Encryption of Payment Cards](#) ► [Evaluate Payment Card Log](#) . To analyze the access log, you need authorization for activity 71 of authorization object B_CCSEC.

You can delete log records if they are at least one year old. To delete the records, on the SAP Easy Access screen choose ► [Cross-Application Components](#) ► [Security of Payment Card Data](#) ► [Encryption of Payment Cards](#) ► [Delete Payment Card Log](#) . To be able to run the deletion report, you need authorization for object B_CCSEC with activity 06.

12.2.14 Recommended Implementation Steps

The following recommended implementation steps differ according to which of the following situations apply to you:

- You did not yet set a security level.
- You are already using the security level for saving payment card numbers in encrypted form, and you now want to implement the process for periodic key replacement.

Variant 1: Security Level Not Yet Set

If you have not yet set a security level in Customizing, follow these steps to implement the process for encrypted storage and periodic key replacement for payment card numbers.

1. Create a key version. To do so, on the SAP Easy Access screen, choose ► [Cross-Application Components](#) ► [Security of Payment Card Data](#) ► [Encryption of Payment Cards](#) ► [Administration of Key Versions for PAYCRV](#) ►. (See [Generating Keys \[page 46\]](#))
2. Make settings for payment card security (see [Making Settings for Payment Card Security \[page 44\]](#)).
 1. Set the security level *Masked Display, and Encrypted When Saved*.
 2. Activate the access log.
 3. Activate the additional authorization checks for unmasked display and set up the user authorizations accordingly.
 4. Set the number of visible characters at the beginning and end of the payment card number.
 5. Activate the key replacement.
3. Specify the payment card types that you want to save in encrypted form. (See [Making Settings for Payment Card Security \[page 44\]](#))
4. Migrate the payment card data that was stored in unencrypted form. (See [Migration of Payment Card Data Stored in Unencrypted Form](#))
5. If you use SAP Business Partner, migrate your payment card data on SAP Business Partner. (See [Migration of Payment Card Data on SAP Business Partner \[page 47\]](#))

Variant 2: Security Level "Masked Display, and Encrypted When Saved" Already Used

If you already set the security level *Masked Display, and Encrypted When Saved* in Customizing, and you already migrated the legacy data when implementing the security level, then perform the following steps to implement the process of periodic key replacement.

1. Create a key version. To do so, on the SAP Easy Access screen, choose ► [Cross-Application Components](#) ► [Security of Payment Card Data](#) ► [Encryption of Payment Cards](#) ► [Administration of Key Versions for PAYCRV](#) ►.
2. Activate the key replacement. (See [Making Settings for Payment Card Security \[page 44\]](#))
3. Migrate the stored encrypted data to the SSF application PAYCRV (see [Migration to SSF Application PAYCRV \[page 48\]](#)).

12.3 Data Security in Behavioral Insights

12.3.1 Roles and Authorizations

This section describes the use of roles and authorizations in SAP S/4HANA for behavioral insights (abbreviated to: Behavioral Insights).

12.3.1.1 Standard Roles

Behavioral Insights uses the standard authorization concepts provided by SAP S/4HANA. SAP delivers standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

In Behavioral Insights, PFCG delta roles are used to access content in the application. To complete the end user role, these roles must be used along with other roles delivered by SAP. These roles are designed to support your Behavioral Insights business processes.

You can use the role below as a template for your own roles:

Role	Details	Description
SAP_BR_ANALYTICS_SPECIALIST	Analytics specialist	This role is required to access ISLM apps.

12.3.1.2 Authorization Objects

The following authorization objects are shipped with Behavioral Insights.

Authorization Object	Purpose	Attributes	Field Description	CDS View	Customizing Tables/views or Programs
S_INF_MAIN	The standard authorization object used to maintain the data model used for the Information Retrieval Framework.	S_INF_COLL Possible values: <ul style="list-style-type: none">01: Add or Create02: Change03: Display39: Check43: Release	Activities that can be performed to maintain the data model used for the Information Retrieval Framework.	Not applicable	Not applicable

Authorization Object	Purpose	Attributes	Field Description	CDS View	Customizing Tables/views or Programs
S_INF_COLL	The standard authorization object used to trigger the data collection process and view the search results.	S_INF_MAIN Possible values: <ul style="list-style-type: none"> • 01: Add or Create • 03: Display • 64: Generate 	Activities that can be performed to trigger the data collection process and view the search results.	Not applicable	Not applicable

Authorization Object	Purpose	Attributes	Field Description	CDS View	Customizing Tables/views or Programs
BEI_CUSTEVT	Authorization object used to display customer master data and customer event data from Behavioral Insights.	ACTVT Possible values: <ul style="list-style-type: none"> 03: Display F4: Display in Value Help 	Activities that can be performed are displaying the data and displaying the value help.	I_ACCOUNTMASTERDATA I_BHVRLINSGT-SACCOUNTITEM I_BHVRLINSGTS-CAHEADER I_BHVRLINSGTS-CAPARTNER I_BHVRLINSGTS-CUSTOMER I_BHVRLINSGTS-CUSTOMERTY-PEVH I_BHVRLINSGTS-CUSTOMERVH I_BHVRLINSGTS-CUSTOMERWITHTHROLE I_BHVRLINSGT-SEVTCONFIGN I_BHVRLINSGT-SEXTERNALEVENT I_BHVRLINSGTSPRDTNRESULT I_BHVRLINSGTSPRDTNTOPRSLTRSN I_CORRESPONDENCEDATA I_CORRESPONDENCEDUNNING I_CUSTOMEREXTERNALVENT I_CUSTOMERLATESTSTATUS I_CUSTOMERMASTERDATA	Not applicable

Authorization Object	Purpose	Attributes	Field Description	CDS View	Customizing Tables/views or Programs
				I_CUSTOMERSTATUS I_CUSTSTATUS-SCHANGEEVENT I_CUSTXRCT-CONFIG I_DUNHISTLINEITEM I_EVENTXRCTCONFIG	
BEI_PEXEC	Authorization object used to execute the <code>predict_risk_score_wrapper</code> prediction report.	ACTVT Possible values: • 03: Display • 16: Execute	Activities that can be performed are displaying the details and executing the prediction report.	Not applicable	PREDICT_RISK_SCORE_WRAPPER (Report)
BEI_PRES	Authorization object used to display prediction results from Behavioral Insights.	ACTVT Possible values: • 03: Display • F4: Display in Value Help SCENARIOID Possible values are configured at scenario config table	Activities that can be performed are displaying the prediction results and displaying the value help. Displays the unique scenario identifier.	I_BHURLINGTSP RDTNRESULT I_BHURLINGTSP RDTNSCENCONFIG I_BHURLINGTSP RDTNSCENNA-METXT I_BHURLINGTSP RANGECONFIG I_BHURLINGTSP SNCONFIG I_BHURLINGTSP SNEVTCONFIG I_BHURLINGTSP SNTXT I_BHURLINGTSP CENARIOVH	Not applicable

Authorization Object	Purpose	Attributes	Field Description	CDS View	Customizing Tables/views or Programs
BEI_PSCEN	Authorization object used to display the data used by the Machine Learning scenarios in Behavioral Insights.	ACTVT Possible value: • 03: Display	The activity that can be performed is displaying the data.	C_LATEFILING-PREDICTDATA C_LATEFILING-TRAINDATA C_LATEPAYMENT-PREDICTDATA C_LATEPAYMENT-TRAINDATA C_RECEIVERSHIP-PREDICTDATA C_RECEIVERSHIP-TRAINDATA	Not applicable
S_TABU_DIS	Authorization object used to maintain Customizing tables in Behavioral Insights.	ACTVT Possible values: • 01: Create or Generate • 02: Change • 23: Maintain	Activities that can be performed are creating entries, changing the entries or maintaining the entries in the Customizing tables.	Not applicable	BEI_RANGE_CFG MV_BEI_CUSX-TRACT MV_BEI_EVT_CFG MV_BEI_EVT-CATCFG MV_BEI_EVTXTRCT MV_BEI_PSCEN_CFG MV_BEI_PXTRCT MV_BEI_RSN_CFG

12.3.2 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries.

12.3.2.1 Deletion of Personal Data

Behavioral Insights might process data that is subject to the data protection laws that apply in specific countries as described in [1825544](#).

Behavioral Insights provides SAP NetWeaver Information Lifecycle Management (ILM)-based archiving and deletion features for the following entities:

- BEI_RESULT_H
- BEI_RESULT_I
- BEI_EXT_EVENT

Business partner records are archived when the business purpose of the business partners is completed. The archival process is based on the residence rules defined for each data object. Data is archived until the retention period expires and the data is then also deleted from the archive store.

Residence and retention rules are defined based on the value specified in the *Time Reference* field that is maintained for the ILM object. These rules can differ based on the value specified in the *Condition Field*, that is maintained in the ILM object.

The following table displays the archiving ILM objects in Behavioral Insights with their corresponding details:

Archiving object/ILM object	Tables	Time Reference Field	Condition field	Programs
BEI_PRSLT	BEI_PRSLT_H	PREDICTION_DATE-TIME	SCENARIO_ID	BEI_PRSLT_WRI
	BEI_PRSLT_I			BEI_PRSLT_DEL
				BEI_PRSLT_READ
BEI_EXTEVT	BEI_EXT_EVENT	EVENT_END_DATE	EVENT_ID	BEI_EXTEVT_WRI
				BEI_EXTEVT_DEL
				BEI_EXTEVT_READ

For more information about archiving and deleting data, see the [SAP Data Archiving Guide](#).

Capability

The source tables and the ILM object details where deletion of data is possible are mentioned as follows:

Source Table	ILM Object
BEI_RESULT_H	BEI_PRSLT
BEI_RESULT_I	BEI_PRSLT
BEI_EXT_EVENT	BEI_EXTEVT

12.3.2.2 Read-Access Logging

Prerequisites

Before you can use the delivered RAL configurations, the following prerequisites must be met:

- The RAL configurations have been activated.
- RAL is enabled in each system client.

Description

Read-access to personal data is partially based on legislation, and it is subject to logging. The Read-Access Logging (RAL) component can be used to monitor and log read-access to data and provide information such as which business users accessed personal data and when they did so. In RAL, you can configure which read-access information is logged and the conditions under which this is done. SAP delivers sample configurations for applications.

In Behavioral Insights, the DPP compliant data is stored in the BEI_RESULT_H, BEI_INFLNCG_FACTORS_I and BEI_EXT_EVENT tables.

You can display the configurations in the system by performing the following steps:

1. In the SRALMANAGER transaction, on the *Administration* tab page, choose *Configuration*.
2. Choose *BW ANALYTICS*.
3. Choose *Search*. The system displays the available configurations for the selected channel.
4. Choose *Display Configuration* to display the detailed information about the configuration. Related recordings can also be displayed for specific channels.

In Behavioral Insights, the C_BHVRLINSGTSCUSTEVTHISTQ, C_BHVRLINSGTSPRDTNHISTQ and C_BHVRLINSGTSPRDTNRSLSNQCDS views are enabled for read-access logging. Customers can configure the fields that are to be logged.

12.3.2.3 Change Logs

Whenever the records in the configuration tables are updated or deleted, this activity is logged in the ABAP platform using the standard change document feature. Change documents facilitate auditing and can be used to log what has changed, and when and how the changes were made.

Configuration change logs can only be accessed using the SCU3 transaction by the user who has the necessary authorization. An application-specific authorization group BEIC, is assigned to all configuration tables, which is associated with the standard authorization object S_TABU_DIS. Only a user who has been assigned the PFCG role, which is mapped to the authorization object S_TABU_DIS and where the authorization group field value is set as BEIC, can view the configuration change logs.

12.3.2.4 Information Retrieval

Data subjects have the right to obtain information about their data that is being processed. The information retrieval feature allows you to comply with the relevant legal requirements for data protection by allowing you to search for and retrieve all personal data for a specified data subject. The search results are displayed in a comprehensive and structured list containing all personal data for the data subject, subdivided according to the purpose for which the data was collected and processed.

Process

Perform the following steps to create and enable the IRF models:

1. Generate the data model using the `DTINF_ADJUST_MODEL` transaction.
2. Create a purpose using the `DTINF_MAINTAIN_PURP` transaction to collect the data.
3. Run the data collection report using the `DTINF_START_COLL` transaction to trigger the information retrieval process.
4. Process the data collection results report using the `DTINF_PROC_COLL` transaction to see an overview of all data collection requests and to display and download the search results.

Information retrieval is implemented using the standard SAP NetWeaver Information Retrieval Framework (IRF) and the IRF implementation is based on the ILM objects. Data is retrieved for the tables defined in the ILM object. BUT000 is the business partner master data table and the source table for information retrieval of data in Behavioral Insights.

The following table displays the ILM objects, the source table and the Behavioral Insights-specific tables that are used for the information retrieval process:

ILM object	Source table	Behavioral Insights tables
BEI_PRSLT	BUT000	BEI_PRSLT_H, BEI_PRSLT_I
BEI_EXTEVT	BUT000	BEI_EXT_EVENT

13 SAP S/4HANA Enterprise Business Applications

13.1 Asset Management

13.1.1 Maintenance Operations

13.1.1.1 Authorizations in Plant Maintenance

Standard Roles

SAP delivers business role templates which follow the naming convention SAP_BR_*. The delivered business role templates are designed to cover typical activities of business users with a certain job profile.

Example

The delivered business role template SAP_BR_MAINTENANCE_TECHNICIAN is designed for maintenance technicians. The role contains business catalogs which cover all the functions that a maintenance technician requires to carry out their work effectively and safely.

Another example business role template SAP_BR_MAINTENANCE_PLANNER is designed for maintenance planners. The role contains business catalogs which cover a broad range of functions necessary for planning and executing maintenance activities.

Each business catalog contains one or more applications and is designed to support segregation of duty.

i Note

For more information about how to create roles, see [Role Administration \[page 13\]](#).

13.1.2 Resource Scheduling

13.1.2.1 Deletion of Personal Data in Resource Scheduling

Use

SAP S/4HANA Asset Management for resource scheduling might process data (personal data) that is subject to the data protection laws applicable in specific countries.

For more information about data protection, see the product assistance for SAP S/4HANA on SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Resource Scheduling for Maintenance Planners	Using these SAP Fiori apps, app users assign work centers to themselves. This is a prerequisite for using the resource scheduling apps.
Manage Work Center Utilization	
Maintenance Scheduling Board	
	If you have the required authorization (authorization object RSH_US_DEL), you can delete these work center assignments for any app user. To do so, use the Deletion of Work Center Assignments in Resource Scheduling report (RSH_DELETE_EAM_USER_SETTINGS).
	i Note Use transaction SE38 in the back-end system to execute the report. For more detailed information, see the report documentation in the system.

13.1.3 Environment, Health and Safety

13.1.3.1 User Administration and Authentication

Environment, Health, and Safety (EHS) uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

For more generic information see [User Administration and Authentication \[page 10\]](#) in the *Introduction* section.

13.1.3.1.1 User Management

The table below shows the standard users that are necessary for operating *Environment, Health, and Safety* (EHS). For more generic information see [User Management \[page 10\]](#) in the *Introduction* section.

User ID	Type	Password	Description
Business processing user	Dialog user	To be entered	Business user of <i>EHS</i>
E-mail inbound processing user	Communication user	Not needed	User to process the incoming e-mails of <i>EHS</i>
Workflow engine batch user	Background user	Not needed	User for the background processing of workflows in <i>EHS</i>

You need to create the users after the installation. Users are not automatically created during installation. In consequence there is no requirement to change their user IDs and passwords after the installation.

i Note

Several business processes within EHS use SAP Business Workflow and e-mail inbound and outbound processing. It is not recommended that you grant the corresponding system users (such as WF_BATCH for Workflow System or SAPCONNECT for e-mail inbound processing) all authorizations of the system (SAP_ALL).

13.1.3.1.2 Communication Destinations

The table below shows an overview of the communication destinations used by *Environment, Health, and Safety* (EHS). For more generic information, see the corresponding chapter in the *Introduction* section.

Destination	Delivered	Type	Description
<OH system>	No	RFC	Connection to the SAP EHS Management for SAP S/4HANA, Occupational Health application
<PM system>	No	RFC	Connection to <i>Plant Maintenance</i> system
<EWM system>	No	RFC	Connection to the <i>Extended Warehouse Management</i> system

For detailed information about communication destinations, see Customizing for *Environment, Health, and Safety* under ► *Foundation for EHS* ► *Integration* ► *Specify Destinations for Integration* ►.

13.1.3.2 ICF Security in Environment, Health, and Safety

To use an app in Environment, Health, and Safety, you have to activate the internet communication framework (ICF) service that is needed for this app.

For general information, see [ICF Security \[page 21\]](#) in the *Introduction* section.

Incident Management

To use *Incident Management* apps, proceed as follows:

- In your front-end system, open transaction SICF. Under `/default_host/sap/bc/ui5_ui5/sap/`, activate the following UI5 services:
 - `repincidentst1` (*Report Incident*)
 - `injillanalyss1` (*Injuries and Illnesses - Detailed Analysis*)
 - `incdntanalyss1` (*Incidents - Detailed Analysis*)
 - `ehsimhrs_mngs1` (*Manage Hours Worked*)
 - `ehsiminj_logs1` (*Manage Injury/Illness Log*)
 - `ehsiminj_mngs1` (*Injury/Illness Log - Detailed Analysis*)
 - `ehsimtsk_invs1` (*Manage Investigation Step Tasks*)
 - `ehsimtsk_rels1` (*Manage Incident Tasks*)
 - `ehstask_cals1` (*Task Calendar*)
 - `ehstask_defst1` (*Manage Task Definition*)
 - `ehstask_instst1` (*Display Task Instance*)
 - `ehstask_libst1` (*Reuse Component for EHS Task Management*)
 - `ehstask_mnotst1` (*Manage Maintenance Notification Task*)
 - `ehstask_mocst1` (*Manage Change Request Task*)
 - `ehstask_monst1` (*Monitor Tasks*)
 - `smr_rpt_mngs1` (*Manage Summary Reports*)

- `ehsim_incmngs1` (*Manage Incidents*)
 - `smr_rpt_gens1` (*Manage Incident Summary Reports*)
 - `ehs_loc_roless1` (*Manage Location Roles*)
- In your back-end system, open transaction SICF. Under `/default_host/sap/bc/webdynpro/sap/`, activate all Web Dynpro services that start with `ehhss` and `ehfnd`.

Health and Safety Management

To use *Health and Safety Management* apps, proceed as follows:

- In your front-end system, open transaction SICF. Under `/default_host/sap/bc/ui5_ui5/sap/`, activate the following UI5 services:
 - `/sap/bc/ui5_ui5/sap/sbrt_appss1` (*Approved Chemicals, Risk Overview*)
 - `/sap/bc/ui5_ui5/sap/ehschm_reps1` (*Chemical Risk Report*)
 - `/sap/bc/ui5_ui5/sap/ehschm_achs1` (*Monitor Approved Chemicals*)
 - `/sap/bc/ui5_ui5/sap/ehscha_mygs1` (*My Chemical Approvals*)
 - `/sap/bc/ui5_ui5/sap/ehsrisk_lsts1` (*Monitor Risks*)
 - `/sap/bc/ui5_ui5/sap/ehsras_lsts1` (*My Risk Assessment Projects*)
- In your back-end system, open transaction SICF. Under `/default_host/sap/bc/webdynpro/sap/`, activate all Web Dynpro services that start with `ehhss` and `ehfnd`.

Environment Management

To use *Environment Management* apps, proceed as follows:

- In your front-end system, open transaction SICF. Under `/default_host/sap/bc/ui5_ui5/sap/`, activate the following UI5 services:
 - `ehsmy_colls1` (*My Data Collections*)
 - `ehstask_cals1` (*Task Calendar*)
 - `ehstask_defs1` (*Manage Task Definition*)
 - `ehstask_insts1` (*Display Task Instance*)
 - `ehstask_mnots1` (*Manage Maintenance Notification Task*)
 - `ehstask_mocs1` (*Manage Change Request Task*)
 - `ehstask_mons1` (*Monitor Tasks*)
 - `em_impdt_data1` (*Import Data*)
 - `em_mon_data1` (*Monitor Data*)
 - `ehstask_libs1` (*Reuse Component for EHS Task Management*)
 - `ehstask_reqs1` (*Manage Compliance Requirement Tasks*)
 - `ehsemtsk_rels1` (*Manage Compliance Scenario Tasks*)
 - `ehsem_cas1` (*Compliance Analysis*)
 - `ehs_loc_roless1` (*Manage Location Roles*)

- In your back-end system, open transaction SICF. Under `/default_host/sap/bc/webdynpro/sap/`, activate all Web Dynpro services that start with `ehenv` and `ehfnd`.

13.1.3.3 Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

In *Environment, Health, and Safety* (EHS), the *XML export for Incident Management* saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by EHS and for which programs these file names and paths apply:

Logical File Names Used

The following logical file name has been created in order to enable the validation of physical file names:

- `EHSS_INCIDENTS_XML`
 - Program `R_EHSS_ALL_INC_TO_XML` is using this logical file name and parameters used in this context.

Logical Path Names Used

The logical file names listed above all use the logical file path `EHSS_BO_XML_EXPORT_PATH`.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the *Security Audit Log*.

For more information on data storage security, see the respective chapter in the ABAP Platform Security Guide.

13.1.3.4 Data Protection

Data protection is very important in the following examples:

- In the incident management process, you have critical person-related information regarding absences or injuries.
- In the health and safety management process, personal data about the risk assessment lead and the other persons involved in a risk assessment are displayed.
- In the environment management process, data about persons assigned to, compliance scenarios, and persons involved in tasks, is displayed.

Environment, Health, and Safety (EHS) assumes that agreements for storage of personal data are covered in individual work contracts. This also applies to notifications on initial data storage.

For more generic information, see [Data Protection \[page 31\]](#) in the *Introduction* section.

13.1.3.4.1 Deletion of Personal Data

Use

The *Environment, Health, and Safety* (EHS) component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data in EHS.

For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under [Product Assistance](#) [Cross Components](#) [Data Protection](#).

Relevant Application Objects and Available Deletion Functionality

The following tables list the relevant application objects and the available deletion functionality for *Incident Management*, *Health and Safety Management*, and *Environment Management*.

Application Objects and Available Deletion Functionality in Incident Management

Application Objects	Provided Deletion Functionality
<i>Incidents</i>	Archiving object EHHSS_INC
<i>Incident Summary Reports</i>	Archiving object EHHSS_ISR

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under [Product Assistance](#) [Enterprise Business Applications](#) [Asset Management](#) [Environment, Health, and Safety](#) [Incident Management \(EHS-SUS-IM\)](#) [Data Archiving in Incident Management](#).

Application Objects and Available Deletion Functionality in Health and Safety Management

Application Objects	Provided Deletion Functionality
<i>Risk Revisions</i>	Archiving object EHHSS_RSV
<i>Risks</i>	Archiving object EHHSS_RSK
<i>Risk Assessments</i>	Archiving object EHHSS_RAS
<i>Safety Instructions</i>	Archiving object EHHSS_SI
<i>Control Evaluations</i>	Archiving object EHHSS_CEVL
<i>Control Inspections</i>	Archiving object EHHSS_CINS
<i>Control Replacements</i>	Archiving object EHHSS_CRPL
<i>Sampling Campaigns</i>	Archiving object EHHSS_SPLC
<i>Samplings</i>	Archiving object EHFND_SPLG
<i>Chemical Approvals</i>	Archiving object EHFND_CHA
<i>Assignment of Person to Locations</i>	Archiving object EHFND_LOCP
<i>Assignment of Person to Jobs</i>	Archiving object EHFND_JOBP
<i>Sampled Person</i>	Data destruction object EHFND_SPLNG_SAMPLED_PERSON

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Asset Management* ► *Environment, Health, and Safety* ► *Health and Safety Management (EHS-SUS-HS)* ► *Technical Solution Information* ►. You can find the information under the following nodes:

- *Data Archiving in Health and Safety Management*
- *Data Destruction in Health an Safety Management*

Application Objects and Available Deletion Functionality in Environment Management

Application Objects	Provided Deletion Functionality
<i>Compliance Scenarios and Tasks</i>	Archiving object EHENV_SCEN
<i>Compliance Requirement Tasks</i>	Archiving object EHFND_REQT

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Asset Management* ► *Environment, Health, and Safety* ► *Environment Management (EHS-SUS-EM)* ► *Data Archiving in Environment Management* ►.

Relevant Applications and Available End of Purpose Checks

In addition to destroying data used for incident management, health and safety management, or environment management processes, EHS provides end of purpose checks (EoP) for central business partners. These checks determine whether dependent data for a certain central business partner is still relevant for business activities in EHS.

The following table lists the registered applications and the function module used for the end of purpose checks in EHS.

Application	End of Purpose Check	Further Information
<i>Incident Management</i> (EHS_INC)	EHHSS_INC_EOP_CHECK_BP	The check determines whether the business partner is used in: <ul style="list-style-type: none"> • Incidents • Tasks in incidents
<i>Health and Safety Management</i> (EHS_HS)	EHHSS_HS_EOP_CHECK_BP	The check determines whether the business partner is used in: <ul style="list-style-type: none"> • Risk assessment projects • Tasks in risk assessment projects • Risks • Control inspections • Control evaluations • Control replacements
<i>Health and Safety Management</i> (EHS_HS_EXPOSURE)	EHHSS_EXP_EOP_CHECK_BP	The check determines whether the business partner is assigned to: <ul style="list-style-type: none"> • Job positions • Location positions • Samplings as sampled person
<i>Environment Management</i> (EHS_ENV)	EHENV_EOP_CHECK_BP	The check determines whether the business partner is used in compliance scenarios and their tasks.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing under [Cross-Application Components](#) > [Data Protection](#) > [Blocking and Unblocking of Data](#) > [Business Partner](#).

13.1.3.4.2 Read Access Logging of Personal Data in Incident Management

Use

In *Read Access Logging (RAL)*, you can configure which read-access information to log and under which conditions.

SAP delivers sample configurations for applications.

Incident Management logs data of illnesses or injuries that are maintained in the *Edit Incident* screen (Web Dynpro app EHHSS_INC_REC_OIF_V3). Since this information is potentially sensitive and access to this information is in some cases legally regulated, you can use *RAL* to log the date when the data was accessed and by whom.

In the following configurations, the following fields are logged:

Configuration	Fields Logged	Business Context
<i>Involved Person - Basic Information</i>	<concatenate name> <ul style="list-style-type: none"> • <i>Injured Person Name</i> • <i>Phone Number</i> • <i>Email</i> <i>Role(s)</i> <i>Incident Type</i> <i>Privacy Case</i> <i>Injured on Site</i> <i>Injured on Duty</i> <i>Additional Criteria</i> <i>Fatality</i> <i>Location of Death</i> <i>Cause of Death</i> <i>Statement of Involved Person</i>	Logs basic information of the person who is involved in the incident.

Configuration	Fields Logged	Business Context
<i>Involved Person - Injury-Illness Information</i>	<concatenate name> <ul style="list-style-type: none"> <i>Injured Person Name</i> <i>Phone Number</i> <i>Email</i> <i>Classification</i> <i>Injury/Illness Type</i> <i>Injury/Illness Description</i> <i>Body Part</i> <i>Body Part Description</i> <i>Body Side</i>	Logs information on the injuries or the illness of the person who is involved in the incident.
<i>Involved Person - Treatment Information</i>	<concatenate name> <ul style="list-style-type: none"> <i>Injured Person Name</i> <i>Phone Number</i> <i>Email</i> <i>First Physician</i> <i>Further Treatment Provider</i> <i>Treatment Beyond First Aid</i> <i>Emergency Room</i> <i>Inpatient Overnight</i> <i>Unconsciousness</i> <i>Immediate Resuscitation</i> <i>Comment</i> <i>To First Aid</i> <i>To Further Treatment</i>	Logs information on the treatment of the person who is involved in the incident.
<i>Involved Person - Reports and Documents</i>	<concatenate name> <ul style="list-style-type: none"> <i>Injured Person Name</i> <i>Phone Number</i> <i>Email</i> <i>File Name</i> (of report forms) <i>File Name</i> (of documents)	Logs the files of reports and documents that are assigned to the involved person.

Configuration	Fields Logged	Business Context
<i>Incident - Reports and Documents</i>	<i>File Name</i> (of report forms) <i>Reference</i> (Report forms of person references) <i>File Name</i> (of documents) <i>Reference</i> (documents of person references)	Logs the files of reports and documents that are assigned to the incident.

Further Information

You can find the configurations as described in the [Read Access Logging \[page 33\]](#) chapter.


13.1.3.4.3 Change Logging

Personal data may be subject to changes. If these changes are logged, you can check which employee made which change and when. *Environmental, Health, and Safety (EHS)* generates change documents for changes in specific fields of the relevant objects that contain personal data.

Under *Display Change Document Objects* (transaction SCDO), you can find the delivered change document objects (EHS change document objects start with EHFND*, EHHSS*, and EHENV*). Under *Maintain Logging Setting* (transaction S_AUT01), you can specify the fields to be logged.

For objects for which you activated the change logging, you can access the change documents by choosing the relevant entry from the *You can also* link. You can enter parameters to limit the changes that are displayed. To view change documents, you need the authorization object EHFND_CHDC. In addition, under *Evaluate New Audit Trail* (transaction S_AUT10) in *Enhancement Mode*, you can display all changes for the change document objects in *EHS*.

More Information

- For more information about the use of change documents in *EHS*, go to https://help.sap.com/s4hana_op_2020, enter *Foundation for EHS (EHS-SUS-FND)* into the search bar, press , open the search result with that title, and navigate to **Technical Solution Information** > *Creation of Change Documents* .
- For more technical information about logging changes, go to https://help.sap.com/s4hana_op_2020, enter *Changing Table and Data Element Logging* into the search bar, press , and open the search result with that title.

- For more information about change documents, go to https://help.sap.com/s4hana_op_2020, enter *Logging Using Change Documents* into the search bar, press , and open the search result with that title.

13.1.3.5 Virus Scanning

The interactive forms of *Environment, Health, and Safety* (EHS) can contain Java Script. Therefore, Java Script must be enabled in Adobe Acrobat Reader. In addition, e-mails with PDF attachments that contain Java Script must not be filtered out in the e-mail inbound and outbound process.

For more generic information see [Virus Scanning \[page 24\]](#) in the *Introduction* section.

13.1.3.6 Other Security-Relevant Information

The following information is relevant for the security of *Environment, Health, and Safety* (EHS).

13.1.3.6.1 Dispensable Functions with Impacts on Security

Environment, Health, and Safety (EHS) can be integrated with *HR Time Management* in Customizing. If the *Personnel Time Management* (PT) integration is activated, time data (including absences) from HR is displayed in the incident. An additional option is available to trigger the creation of HR absences from the incident. For all actions, HR authorizations are checked.

13.1.3.6.2 Security Settings for the Report Incident App

You use *SAP Cloud Platform Mobile Services* to implement the *Report Incident* app. For more information on the security settings, go to the SAP Help Portal at <https://help.sap.com> and search for **SAP Cloud Platform Mobile Services**.

13.1.3.6.3 Whitelisting of Calculation Functions in the Environment Management Calculation Engine

The calculation engine allows the execution of custom function modules specified with the `FUNC` predicate in the calculated expression. In order to eliminate abuse of this functionality, only whitelisted function modules are allowed to be executed using the `FUNC` predicate.

For more information, see the Customizing activity under ► [Environment, Health, and Safety](#)
► [Environment Management](#) ► [General Configuration](#) ► [Specify Allowed ABAP Function Modules in User-Defined Calculations](#) ►.

13.1.4 Management of Change

The following chapters of the Security Guide provide an overview of the security-relevant information that applies to Management of Change.

13.1.4.1 ICF Security in Management of Change

To use apps in Management of Change, you have to activate the internet communication framework (ICF) service that is needed for the specific app.

For general information, see [ICF Security \[page 21\]](#).

In your front-end system, open [HTTP Service Hierarchy Maintenance](#) (transaction SICF). Under / default_host / sap / bc / ui5_ui5 / sap /, activate the following UI5 services:

- moc_manactys1 ([Manage Change Activities](#))
- moc_manchgreqs1 ([Manage Change Request - MOC](#))

In your back-end system, open [HTTP Service Hierarchy Maintenance](#) (transaction SICF) and activate the Web Dynpro services under ► [default_host](#) ► [sap](#) ► [bc](#) ► [webdynpro](#) ► [moc](#) ►.

13.1.4.2 Data Protection and Privacy

Data protection is very important in Management of Change and its processes, because personal data of the persons involved in change requests and activities are displayed.

Management of Change assumes that agreements for storage of personal data are covered in individual work contracts. This also applies to notifications on initial data storage.

For more generic information, see [Data Protection \[page 31\]](#).

13.1.4.2.1 Deletion of Personal Data

Management of Change might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use [SAP Information Lifecycle Management \(ILM\)](#) to control the blocking and deletion of personal data in Management of Change.

For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

Relevant Application Objects and Available Deletion Functionality

The following table lists the relevant application objects and the available deletion functionalities for Management of Change.

Application Objects and Available Deletion Functionalities in Management of Change

Application Object	Provided Deletion Functionalities
Activity	Archiving object / IAM/ACT Related ILM object IAM_ACTIVITY
Change request (issue)	Archiving object / IAM/ISSUE Related ILM object IAM_ISSUE

For more information about application objects and deletion functionalities, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► [Product Assistance](#) ► [Enterprise Business Applications](#) ► [Asset Management](#) ► [Management of Change](#) ► [Data Management in Management of Change](#) ►.

Configuration: Simplified Blocking and Deletion

In Management of Change, you configure the settings related to the blocking and deletion of business partner master data in Customizing for [Cross-Application Components](#) under [Data Protection](#):

- Define the settings for authorization management under [Authorization Management](#).
For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing under ► [Blocking and Unblocking](#) ► [Business Partner](#) ►.

For more information about simplified blocking and deletion, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ► [Simplified Blocking and Deletion](#) ►.

13.1.4.2.2 Change Log

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to track the changes that have been made to this data. When these changes are logged, you should be able to check which employee made which changes, the date and time, the previous value, and the current value. It is also possible to analyze errors in this way.

Setting Up Change Logs for Management of Change

Management of Change processes personal data of business partners that are involved in change requests and activities. If any changes are made regarding the business partner, the system logs the following information on personal data per change request and activity:

- The user who has changed data
- Data and the time of the change
- The change type (update, insert, deletion, single field documentation)
- The identifying keys and their values of the data records
- The heading name for the attribute that has been changed

You can define the fields to be logged under *Display Change Document Objects* (transaction SCDO).

You use the authorization object `IAM/CHGLOG` to control the change logging for change requests and activities.

Displaying Change Logs in Management of Change

In the *Display Change Log - Change Activity* and *Display Change Log - Change Request* apps, it is possible to call up a change log for each change request and each activity.

More Information

- For more information on change documents, see the application help for SAP NetWeaver on the SAP Help Portal at https://help.sap.com/s4hana_op_2020:
 - Open the function-oriented view and go to **Application Server ABAP** > **Other Services** > **Services for Application Developers** > **Change Documents**.
 - Open the *ABAP Platform Security Guide* and go to **Security Aspects for Lifecycle Management** > **Auditing and Logging**.
- For more information on logging changes of change requests and activities in Management of Change, see the product assistance on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under **Product Assistance** > **Enterprise Business Applications** > **Asset Management** > **Management of Change** > **Data Management in Management of Change** > **Logging Changes**.
- For more information on archiving change documents in Management of Change, see the product assistance on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under **Product Assistance** > **Enterprise Business Applications** > **Asset Management** > **Management of Change** > **Data Management in Management of Change** > **Data Archiving in Management of Change**.

13.2 Finance

13.2.1 Financial Accounting

Network and Communication Security

Communication with external systems takes place using the standard channels provided by SAP basis technology:

- Application Link Enabling(ALE)/IDoc
- Standard interfaces to BI, CRM, and SRM systems
- Batch-Input
Ensure that no unauthorized access can take place at the time of data transfer using encryption and with the help of your network.
- Remote Function Call(RFC) / Business Application Programming Interface (BAPI)
- File Interface
Ensure that no unauthorized access can take place at the time of data transfer using encryption and with the help of your network.
- SAP Process Integration (PI)
- E-mail, fax

❖ Example

- Financial Accounting has interfaces to *Taxware* and *Vertex* software used for performing tax calculations.
- Electronic advance return for tax on sales/purchases:
 - There is an interface for the electronic advance return for tax on sales and purchases using *Elster*. Communication takes place by means of XI.
 - You can digitally sign the electronic advance return for tax on sales/purchases.
- Payments and payment advice notes are dispatched using IDoc, and dunning notices are sent by e-mail or fax.

Communication Destinations

All the technical users generally available can be used.

Data Storage Security

Many of the *Financial Accounting* transactions access sensitive data. Access to this kind of data, such as financial statements, is protected by standard authorization objects.

13.2.1.1 Deletion of Personal Data in Financial Accounting

Use

The `Financial Accounting` (FI) component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Available Deletion Functionality

ILM Objects in Financial Accounting (FI)

ILM Object	Description
AM_ASSET	Asset - Master Data, Values and Transactions
APPREQUEST	IM: Appropriation Request
CA_SEPA	Single Euro Payments Area (Mandate)
EC_PCA_ITM	Profit Center Acctg: Actual and Plan Line Items
EC_PCA_MD	Profit Center Master Data
EC_PCA_SUM	Profit Center Accounting: Totals Records
FI_ACCOUNT	G/L Account Master Data
FI_DOCUMNT	Financial Accounting Documents
FI_DUNNING_DESTRUCTION	Deleting Dunning Data
FI_INTEREST_DESTRUCTION	Deleting Interest Data
FI_PAYRQ	Payment Requests
FI_SCHECK	Prenumbered Checks

ILM Object	Description
FI_SL_DATA	FI Special Ledger: Totals and Line Items
FI_TCJ_DOC	FI Cash Journal Documents
FI_TF_CRE	Vendor Transaction Figures
FI_TF_DEB	Customer Transaction Figures
FI_TF_GLC (obsolete)	G/L Account Transaction Figures
FI_TF_GLF	G/L Transaction Figures (New)
FILOC_ES_RFASLD11B	ILM object for Spanish EC sales list
GLE_ECS	ECS: Archiving Object for ECS
MM_ACCTIT	MM- Accounting interface posting data
MM_MATBEL	Materials Management: Material Documents
SAPPCE_DP	Down Payment Chain
FINS_PLAN	Plan data records of table ACDOCP

Available Check

Implemented Solution: End of Purpose Check

The following points are checked in the system:

- Checks whether an item belonging to this customer exists
- Checks that at least one parked document or fully saved document exist for this customer
- Checks whether a recurring entry original document exist that refers to the customer
- Checks whether a link to a vendor is maintained in the master record of the customer, and whether the clearing between the customer and vendor is active
- Checks whether the customer is used as an alternative payee
- Checks whether at least one saved document for this customer exists in the cash journal

If one of the points mentioned above doesn't apply, the system doesn't lock the customer. If these points don't apply, the system determines the last payment that was made for this customer and uses it as a reference date for the retention rules that are defined in ILM Customizing.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of `business partner master data` in `Customizing for Cross-Application Components` under `Data Protection`.

13.2.1.2 General Ledger Accounting (FI-GL)

13.2.1.2.1 Data Storage Security

Logical Path and File Names

The FI-GL component saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by the FI-GL component. They also show the programs for which these file names and paths apply.

Logical File Names and Paths for FI-GL and FI-SL

Logical File Names

The following logical file names have been created to enable the validation of physical file names:

- **FI_COPY_COMPANY_CODE_DATA_FOR_GENERAL_LEDGER_0X**
 - Programs using this logical file name:
 - RFBISA00
 - RFBISA01
 - RFBISA51
 - Parameter used in this context:
 - `<PARAM_1>` *Program Name*
- **FI_INFOSYS_TRANSPORT**
 - Programs using this logical file name:
 - RGRJTE00
 - RGRLTE00
 - RGRMTE00
 - RGR RTE00

- RGRSTE00
- RGRVTE00
- RGRXTE00
- RGSSTE00
- RGSVTE00
- RGRJT100
- RGRMT100
- RGSST100
- RGSVT100
- Parameter used in this context:
 - <PARAM_1> Program name
- **FI_VALUATION**
 - Programs using this logical file name:
 - FAGL_FCV
 - FAGL_FC_VALUATION
 - SAPF100
 - Parameters used in this context:
 - <PARAM_1> *Program name*
 - <PARAM_2> Key date (from the selection screen)
 - <PARAM_3> Valuation area (from the selection screen) for FAGL_FCV and FAGL_FC_VALUATION
valuation method (from the selection screen) for SAPF100

Logical Path Names

The logical file names listed above all use the logical file path **FI_ROOT**.

Logical File Names and Paths for FI-GL-IS (Information System)

Logical File Names

The following logical file names have been created to enable the validation of physical file names:

- **FI_EXTERNAL**
Programs using this logical file name and parameters used in this context:

Program	<PARAM_1>	<PARAM_2>	<PARAM_3>
RFAWVZ58	Program name (SY-REPID)	String 'AWV'	Parameter 'Key Date'
RFAWVZ5A	Program name (SY-REPID)	String 'AWV'	Parameter 'Key Date'
RFAWVZ5P	Program name (SY-REPID)	String 'AWV'	
RFAWVZ5A_NACC	Program name (SY-REPID)	String 'AWV'	Parameter 'Key Date'

RFAWVZ5P_NACC	Program name (SY-REPID)	String 'AWV'	
RFBIDETO	Program name (SY-REPID)	Parameter 'Client'	
RFBIKRTO	Program name (SY-REPID)	Parameter 'Client'	
RFFROE84	Program name (SY-REPID)	Parameter 'Customers/vendors'	Parameter 'Key Date'
RFFRDDEO	Program name (SY-REPID)	Parameter 'Company Code'	Parameter 'Type'
RFFRLIST	Program name (SY-REPID)		
RFFRMOD1	Program name (SY-REPID)		
RFDPTFO	Program name (SY-REPID)	Concatenated parameters <Company Code>_<Year>_<Period>	String 'READ' or 'WRITE'
RFLBOX00	Program name (SY-REPID)	Parameter 'Procedure'	Parameter 'Input Record Format'
RFLBOX80	Program name (SY-REPID)	Parameter 'Procedure'	Parameter 'Input Record Format'
RFLBOXIN	Program name (SY-REPID)	String 'LOCKBOX'	String 'BAI'
RFSBLIW0	Program name (SY-REPID)		

- **FI_POSTING**

Programs using this logical file name and parameters used in this context:

Program	<PARAM_1>	<PARAM_2>	<PARAM_3>
RFBIBLTO	Program name (SY-REPID)		
RFEBCK00	Program name (SY-REPID)	Parameter 'Document Type'	Parameter 'Session name'
RFEBCKT0	Program name (SY-REPID)		
SAPF100A	Program name (SY-REPID)	Parameter 'Key Date'	

- **FI_TAX**

Programs using this logical file name and parameters used in this context:

Program	<PARAM_1>	<PARAM_2>	<PARAM_3>
RFASLD02	Program name (SY-REPID)	Parameter year for 'Reporting Quarter'	Parameter 'Reporting Quarter'

RFASLD11	Program name (SY-REPID)	Parameter year for 'Reporting Quarter'	Parameter 'Reporting Quarter'
RFASLD11B	Program name (SY-REPID)	Parameter year for 'Reporting Quarter'	Parameter 'Reporting Quarter'
RFUMPT00	Program name (SY-REPID)	Parameter 'Company Code'	
RFUSVB10	Program name (SY-REPID)	Parameter 'Posting Date' (lower value)	Parameter 'Posting Date' (higher value)
RFKQSU30	Program name (SY-REPID)		
RFUMPT00	Program name (SY-REPID)		
RFUSVS12	Program name (SY-REPID)	Parameter 'Entity Responsible'	See note 1
RFUSVS14	Program name (SY-REPID)	Concatenated parameters <Company Code>_<Year>	See note 1
RFUVPT00	Program name (SY-REPID)	Parameter 'Company Code'	See note 2

Notes:

- Note 1
If the file specified in the parameter "File for Leasing" is accessed, PARAM_3 contains the value READ; consequently, the file content is read only and added to the output file.
If the file specified in the parameter "UNIX File for Output" is accessed, PARAM_3 contains the value "WRITE".
- Note 2
If the file listed in the parameter "File Name - Application Server" on the "Periodic File O" tab page is accessed, PARAM_3 contains the string PERIOD_WRITE.
If the file listed in the parameter "ECSL File Name (AS)" on the "Periodic File O" tab page is accessed, PARAM_3 contains the string PERIOD_READ.
If the file listed in the parameter "XML File App. OP" on the "Annual File O/P" tab page is accessed, PARAM_3 contains the string YEAR_READ.
If the file listed in the parameter "File Name - Application Server" on the "Annual File O/P" tab page is accessed, PARAM_3 contains the string YEAR_WRITE.
- **FI_RFASLD12_FILE**
Programs using this logical file name and parameters used in this context:

Program	<PARAM_1>
RFASLD02	Program name (SY-CPROG)

Logical Path Names

The logical file names listed above use the following logical file paths:

Logical File Name	Logical File Path
FI_EXTERNAL	FI_ROOT
FI_POSTING	
FI_TAX	
FI_RFASLD12_FILE	FI_ERVJAB_FILE_PATH

13.2.1.2.2 Specific Read Access Logging Configuration

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions.

SAP delivers sample configurations for applications.

For the transactions ACC_ECS_LIST and ACC_ECS_MAINTAIN, two configurations are available to log the read access to the fields below in the Error Correction and Suspense Accounting system. You can find the configurations as described in the [Read Access Logging \[page 33\]](#) chapter.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Configuration	Fields Logged	Business Context
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCINS	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCNUM	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCFOL	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	DATAB	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	DATBI	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCNAME	Error Correction and Suspense Accounting>

Configuration	Fields Logged	Business Context
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CSOUR	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	AUTWR	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCWAE	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	SETTL	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	AUNUM	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	AUTRA	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	AUDAT	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	AUTIM	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	MERCH	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	LOCID	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	TRMID	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCBTC	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCTYP	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	CCARD_GUID	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	DP_TOKEN	Error Correction and Suspense Accounting>
FIN_ACC_ECS_MAINTAIN and FIN_ACC_ECS_LIST	HBKID	Error Correction and Suspense Accounting>

13.2.1.2.3 Authorizations

Standard Authorization Objects for Accounting Enhancements for Banking

The table below shows the security-relevant authorizations:

Authorization Object	Field	Value	Description
GLE_ADB_GR	ACTVT	16	Execute and persist Average Daily Balance calculation for group reporting
		48	Execute Average Daily Balance calculation for group reporting in simulation mode
GLE_ECS	ACTVT	2	Change ECS Document Item
		3	Display ECS Document Item
		6	Delete ECS Document Item
		36	Extended maintenance
		43	Approve ECS Document Item
		96	Reject ECS Document Item
		A8	Process mass activity on ECS documents

13.2.1.3 Bank Accounting (FI-BL)

Important SAP Notes

For a list of additional security-relevant SAP HotNews and SAP Notes, see the SAP Support Portal at <http://support.sap.com/securitynotes>.

13.2.1.4 Asset Accounting (FI-AA)

Important SAP Notes

For a list of additional security-relevant SAP HotNews and SAP Notes, see the SAP Support Portal at <http://support.sap.com/securitynotes>.

Standard Roles

Role	Description
SAP_BR_AA_ACCOUNTANT	Asset Accountant
SAP_AUDITOR_BA_FI_AA	AIS Fixed Assets
SAP_AUDITOR_BA_FI_AA_A	AIS - Fixed Assets (Authorizations)

Standard Authorization Objects

For the list of standard authorization objects available for Asset Accounting, see transaction SU21, Object Class *Asset Accounting* (AM).

Network and Communication Security

Asset Accounting provides BAPIs for communicating with third-party systems.

Communication Destinations

For workflow tasks, you sometimes need either the *WF-BATCH* user or a user that you can use for background steps of this kind. To execute the decision steps required before reaching these background steps, you need a user that is explicitly assigned.

13.2.1.5 Special Purpose Ledger (FI-SL)

Data Storage Security

Protect access to the file system with logical paths and file names

The Special Purpose Ledger saves data in files in the file system. Therefore, it is important to allow access explicitly to certain files in the file system without allowing access to other files (also called file traversals). You achieve this by entering logical paths and file names in the system, which are assigned to the physical paths and file names. This assignment is validated at runtime. If access to a file is requested that does not match any stored assignment, then an error occurs.

Access to the file system is protected for the following programs by the logical file name listed.

Program	Logical File Name Used by the Program	Parameter Used in Context	Logical Path Name Used by the Program
RGRJTE00	FI_INFOSYS_TRANSPORT	<PARAM_1> <i>Program Name</i>	FI_ROOT
RGRLTE00			
RGRMTE00			
RGR RTE00			
RGRSTE00			
RGRVTE00			
RGRXTE00			
RGSSTE00			
RGSVTE00			
RGRJT100			
RGRMT100			
RGSST100			
RGSVT100			
SAPMGLRV	FI_ROLLUP	<PARAM_1> <i>Program Name</i> (SY-CPROG)	FI_ROOT
SAPFGRWE	FI_REPORT_WRITER	<PARAM_1> <i>Program Name</i> (SY-CPROG – generated program name)	FI_ROOT

Activating the Validation of Logical Paths and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-dependent). To determine which paths are used by your system, you can activate the appropriate settings in the Security Audit Log.

13.2.1.6 Corporate Close - Consolidation Foundation

13.2.1.6.1 Deletion of Personal Data

Use

The **Real-Time Consolidation** (FIN-RTC) component in SAP S/4HANA might process data (personal data) that is subject to the data protection laws applicable in specific countries.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Consolidation Methods <ul style="list-style-type: none"> • Transaction codes RTCTM and RTCRM • Fiori App Define Validation Methods 	RTC_DPP_METHOD
Consolidation Models (transaction code RTCMD)	RTC_DPP_MODEL
Validation Rules (Fiori app Define Validation Rules)	RTC_DPP_VALIDATION_RULE
Data Release Lock (Fiori app Consolidation Data Release Monitor)	RTC_DPP_DATA_RELEASE_LOCK
Data Release Requests <ul style="list-style-type: none"> • Fiori app Consolidation Data Release Cockpit • Fiori app Consolidation Data Release Monitor 	RTC_DPP_DATA_RELEASE_REQUEST
Rule Result Comments (Fiori app Consolidation Data Release Cockpit)	RTC_DPP_RULE_RESULT_COMMENTS

Application	Provided Deletion Functionality
Task Logs (all programs that run currency translation and post journal entries, for example, transaction code <code>RTCCT</code> and Fiori app <i>Consolidation Data Release Cockpit</i>)	RTC_DPP_TASK_LOG

i Note

For the deletion programs mentioned in the table above, you can also **Display Records**.

Run Deletion Programs

SAP recommends scheduling regular jobs to run the deletion programs using the *Define Background Job* (SM36) transaction.

13.2.1.7 Corporate Close - Group Reporting

13.2.1.7.1 Deletion of Personal Data

Use

The **Group Reporting** (FIN-CS) component in SAP S/4HANA might process data (personal data) that is subject to the data protection laws applicable in specific countries.

Procedure

You can use the app *Data Protection for Consolidation* (transaction code `CXDPP`) to anonymize user information and delete personal data for data protection purposes.

You can anonymize user data in the following records by selecting *Anonymize Information* and a time period:

- Task Logs
- Replication of Flow Data
- Replication of Hierarchies

- Data Monitor Status
- Data Entry Layouts
- Consolidation Monitor Status
- Validation Parsing
- Rules Parsing
- Methods
- Global Parameters
- Activation of Analysis Help
- Consolidation Unit, Name
- Consolidation Unit, Contact Person

You can select the option [Delete Data Records](#) for data in [Global Parameters](#) and [Activation of Analysis Help](#).

You can select [Display Data Records](#) to view the user data included in the data records mentioned in the table above.

13.2.1.7.2 Virus Scanning

You can activate and set up a virus scan interface of your choice. When you upload an xls spreadsheet, make sure that the virus scanner you selected detects xls-bombs (like zip bombs).

For more information see [Virus Scanning \[page 24\]](#).

13.2.1.7.3 Allowlisting

For the [Import Consolidation Master Data](#) app, the following MIME Type is on the allowlist:

- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet.

Make sure that you have included the above mentioned MIME Type in the allowlist.

For more information, see [General Recommendations for Virus Scan Profiles \[page 25\]](#).

13.2.1.7.4 Malicious Content

If the virus scanner detects malicious content when uploading and importing data in the [Import Consolidation Master Data](#) app, the process is terminated. SAP recommends that customers do not turn off this function.

13.2.1.8 Central Finance (FI-CF)

The following functions are available for Central Finance:

Schedule Clean-Up Report in Source System

Data relating to FI/CO documents is temporarily stored in log tables in the source system before it can be transferred to Central Finance. To delete the temporary information from these tables, a clean-up program (`RFIN_CFIN_CLEANUP`) is run and must be scheduled regularly (for example, once a month). In the configuration of this program, you can define for how many periods a temporarily stored data record is kept before being deleted by the clean-up program (for example, so that an incorrect posting can be corrected).

Read Access Log for the Application Log

The application log for the Central Finance initial load may contain sensitive, personal data. Therefore, we provide a read access log for this application log (`CFIN_INITIAL_LOAD`) for the channel `DYNP`.

13.2.1.9 Joint Venture Accounting

13.2.1.9.1 Deletion of Personal Data in Joint Venture Accounting

Use

The *Joint Venture Accounting* component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Available Deletion Functionality

Application Object	Provided Deletion Functionality
Joint Venture partner data	Data destruction object JVA_PARTNER_DESTRUCTION

For more information, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Finance* ► *Accounting and Financial Close* ► *Joint Venture Accounting* ► *Data Destruction in Joint Venture Accounting* ►.

Relevant Application Objects and Available End of Purpose Check

Application Object	Implemented Solution	Further Information
Joint Venture partner data	End of Purpose Check (EoP)	<p>The EoP check is integrated into the ILM objects</p> <ul style="list-style-type: none"> • FI_ACCRECV (customer master data) for checking customer master data • FI_ACCPAYB (vendor master data) for checking vendor master data

For more information, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Finance* ► *Accounting and Financial Close* ► *Joint Venture Accounting* ► *End of Purpose Check (EoP) for Business Partner* ►.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of Joint Venture partner data in Customizing under ► *Cross-Application Components* ► *Data Protection* ►.

13.2.1.9.2 Deletion of Personal Data in Project Risk Management for Contractors

Use

The *Project Risk Management for Contractors* component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Available Deletion Functionality

Application Object	Provided Deletion Functionality
Joint Venture partner data	Data destruction object / SAPPCE / JVA_PARTNER_DESTR

For more information, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Finance* ► *Accounting and Financial Close* ► *Joint Venture Accounting* ► *Project Risk Management for Contractors* ► *Data Destruction* ►.

Relevant Application Objects and Available End of Purpose Check

Application	Implemented Solution	Further Information
Joint Venture partner data	End of Purpose Check (EoP)	<p>The EoP check is integrated into the ILM objects</p> <ul style="list-style-type: none"> FI_ACCRECV (customer master data) for checking customer master data FI_ACCPAYB (vendor master data) for checking vendor master data

For more information, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Finance* ► *Accounting and Financial Close* ► *Joint Venture Accounting* ► *Project Risk Management for Contractors* ► *End of Purpose Check (EoP) for Business Partner* ►.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of Joint Venture partner data in Customizing under ► [Cross-Application Components](#) ► [Data Protection](#) ►.

13.2.2 Controlling

13.2.2.1 Deletion of Personal Data in Controlling

Use

The Controlling (CO) component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

Available Deletion Functionality

ILM Objects in Controlling (CO)

ILM Object	Description
CO_ALLO_ST	Completely canceled documents contrib., val., ...
CO_CCMAST	Cost Center Master Data
CO_CEL_RCL	Reconciliation ledger: Totals and line items
CO_COPC	Archiving Product Costing Data
CO_ORDER	Orders with transaction data
CO_PROCESS	Business process, including transaction data
CO_TRANS	CO Line Items and Totals
COPAA_XXXX	Costing-based line items (Transaction: KE0I)
COPAB_XXXX	Costing-based object level (Transaction: KE0I)

ILM Object	Description
COPA2_XXXX	Account-based line items (Transaction: KE0I)
COPAC_XXXX	Profitability segments (Transaction: KE0I)
PM_ORDER	Service and Maintenance Orders
FICO_MYUSLOG	My Unusual Items

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for Cross-Application Components under Data Protection.

13.2.2.2 Network and Communication Security

Controlling is integrated with *Microsoft Office*. For information on security aspects with *Microsoft Office* applications, refer to the documentation of those products.

Communication in *Manager Self-Service* (MSS) and in the *Web Application for the Business Unit Analyst* (BUA) is based on *Remote Function Calls* (RFCs).

13.2.2.2.1 Communication Destinations

Technical users are required for communication over ALE, for batch reporting, and for third-party providers that access Controlling data.

13.2.3 Governance, Risk and Compliance for Finance

13.2.3.1 International Trade

The following security information applies to SAP S/4HANA for international trade only.

13.2.3.1.1 Intrastat

Related Information

[Personal Data in Intrastat Declarations \[page 95\]](#)

[Manage Authorizations for Generic UIs for Intrastat \[page 95\]](#)

13.2.3.1.1.1 Personal Data in Intrastat Declarations

Personal data of the contact person of the provider of information, for example first name, last name and e-mail address, is written into Intrastat declaration files to be compliant with the file formats defined by authorities. These file formats are country-specific and can be changed by authorities at any time.

Intrastat declaration files are saved outside the SAP S/4HANA system. Therefore, the management of those files and the deletion of personal data in those files must be done outside the SAP S/4HANA system.

13.2.3.1.1.2 Manage Authorizations for Generic UIs for Intrastat

Related Information

[Generic UIs - Application Job for Intrastat \[page 95\]](#)

13.2.3.1.1.2.1 Generic UIs - Application Job for Intrastat

Context

On the back-end server, you have to assign the OData service authorization to a PFCG role. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs*

into the search bar, press `Enter`, and open the search result with that title. In addition, manual actions are required.

1. Assign Fiori catalog to PFCG role.
2. Assign additional authorization default for required application job catalog entry.
3. Fill authorization field P_PROGNAM with report name for authorization object S_PROGNAM

Business Catalog	Application Job Catalog Entry	Report Name	Fiori ID
SAP_SLL_BC_INTRASTAT_SEL	SAP_SD_FT_RVEXST00	RVEXST00	F2507 Select Dispatches and Customer Returns - Intrastat Declaration
SAP_SLL_BC_INTRASTAT_SEL	SAP_MM_FT_RMIMST00	RMIMST00	F2508 Select Receipts and Returns to Supplier - Intrastat Declaration

13.2.3.1.1.3 Dependent Business Catalog for Intrastat

You can manage authorization fields in PFCG role by using transaction PFCG. The authorization field is used in Business Partner display catalog.

Business Catalog: SAP_CMD_BC_BP_DISP

Master Data - Business Partner Display

Authorization Object	Description	Authorization Field
B_BUPA_GRP	Authorization Group for Business Partners	BEGRU
B_BUPA_RLT	Business Partner Role	RLTYP

Business Partner Display Catalog Used by Intrastat Apps (POI)

If you assign business catalog SAP_SLL_BC_INTRASTAT_DECLN in a backend role, you also assign business catalog SAP_CMD_BC_BP_DISP in the same backend role. If you assign business catalog SAP_SLL_BC_POI_MANAGE in a backend role, you also assign business catalog SAP_CMD_BC_BP_DISP in the same backend role. Specify business partner role type B_BUPA_RLT with ACTVT = 03 & RLTYP = 'SLLSTL'. 'SLLSTL' is the contact person created as provider of information.

13.2.3.1.2 International Trade Classification

Related Information

[Manage Authorization for Generic UIs for International Trade Classification \[page 97\]](#)

[Generic UIs - Application Log for International Trade Classification \[page 97\]](#)

13.2.3.1.2.1 Manage Authorization for Generic UIs for International Trade Classification

Related Information

[Generic UIs - Application Log for International Trade Classification \[page 97\]](#)

[Dependent Business Catalog for International Trade Classification \[page 98\]](#)

13.2.3.1.2.1.1 Generic UIs - Application Log for International Trade Classification

Context

Manual action required.

1. Assign Fiori catalog to PFCG role.
2. Fill authorization data for authorization object S_APPL_LOG.
 1. Log object - ALG_OBJECT
 2. Log sub-object - ALG_SUBOBJ

Business Catalog	Log Object	Log Sub-Object	Fiori ID
SAP_SLL_BC_CMMDTYCODE_ ACTV	/SAPSL/CLSMD	/SAPSL/CNT_ACT_CHK /SAPSL/CNT_CONS_CHK	F4888 Application Log for Classification Master Data
SAP_SLL_BC_CTRLCLASS_A CTV	/SAPSL/CLSMD	/SAPSL/CNT_ACT_CHK /SAPSL/CNT_CONS_CHK	F4888 Application Log for Classification Master Data

Business Catalog	Log Object	Log Sub-Object	Fiori ID
SAP_SLL_BC_TRIFNMBR_AC TV	/SAPSL/CLSMD	/SAPSL/CNT_ACT_CHK /SAPSL/CNT_CONS_CHK	F4888 Application Log for Classification Master Data

13.2.3.1.2.2 Dependent Business Catalog for International Trade Classification

If you assign business catalog `SAP_SLL_BC_CLS_CMMDTYCODE` in backend role, you also assign business catalog `SAP_CMD_BC_PRODUCT_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_CLS_TRIFNMBR` in backend role, you also assign business catalogs `SAP_CMD_BC_PRODUCT_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_CLS_ISSRVCCODE` in backend role, you also assign business catalog `SAP_CMD_BC_PRODUCT_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_CLS_LEGCTRL` in backend role, you also assign business catalog `SAP_CMD_BC_PRODUCT_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_CLS_OVERVIEW` in backend role, you also assign business catalog `SAP_CMD_BC_PRODUCT_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_PROD_CLS_DISP` in backend role, you also assign business catalog `SAP_CMD_BC_PRODUCT_DSP` in the same backend role.

13.2.3.1.3 International Trade Compliance

Related Information

[Manage Authorization for Generic UIs for International Trade Compliance \[page 98\]](#)

[Dependent Business Catalog for International Trade Compliance \[page 100\]](#)

13.2.3.1.3.1 Manage Authorization for Generic UIs for International Trade Compliance

Related Information

[Generic UIs - Attachment for License Master \[page 99\]](#)

13.2.3.1.3.1.1 Generic UIs - Application Job for International Trade Compliance

Context

Manual action required.

1. Assign Fiori catalog to PFCG role.
2. Assign additional authorization default for required application job catalog entry.
3. Fill authorization field P_PROGNAM with report name for authorization object S_PROGNAM.

Business Catalog	Application Job Catalog Entry	Report Name	Fiori ID
SAP_SLL_BC_COMPLDOC_MA NAGE	SAP_SLL_TCD_RECHECK_MA SS	/SAPSLI/ TCD_RECHECK_MASS	F4285 Schedule Recheck Documents - Trade Compliance

13.2.3.1.3.1.2 Generic UIs - Attachment for License Master

Context

On the back-end server, you have to assign the OData service authorization to a PFCG role. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

Procedure

1. Assign Fiori catalog SAP_SLL_BC_LICENSE_MANAGE to PFCG role.

2. Input value for authorization object S_GOS_ATT manually:

- BOROBJTYPE = ITRLICMSTR
- ACTIVITY = 02 and

13.2.3.1.3.2 Dependent Business Catalog for International Trade Compliance

If you assign business catalog SAP_SLL_BC_LICENSE_MANAGE in backend role, you also assign business catalog SAP_CMD_BC_BP_DISP in the same backend role.

If you assign business catalog SAP_SLL_BC_LICENSE_MANAGE in backend role, you also assign business catalog SAP_CMD_BC_PRODUCT_DSP in the same backend role.

If you assign business catalog SAP_SLL_BC_CMPLCDOC_MANAGE in backend role, you also assign business catalog SAP_SLL_BC_LICENSE_DISP in the same backend role.

If you assign business catalog SAP_SLL_BC_LICASSGMT_DISP in backend role, you also assign business catalog SAP_CMD_BC_BP_DISP in the same backend role.

If you assign business catalog SAP_SLL_BC_LICASSGMT_DISP in backend role, you also assign business catalog SAP_CMD_BC_PRODUCT_DSP in the same backend role.

13.2.3.1.4 Integration

Related Information

[Integration with SAP Global Trade Services \[page 100\]](#)

[Integration with SAP Watch List Screening \[page 104\]](#)

[Integration with Content Data Provider \[page 105\]](#)

13.2.3.1.4.1 Integration with SAP Global Trade Services

Related Information

[Manage Authorization for Generic UIs for GTS Integration \[page 101\]](#)

13.2.3.1.4.1.1 Manage Authorization for Generic UIs for GTS Integration

Related Information

[Generic UIs - Application Job for Global Trade Services Integration \[page 101\]](#)

[Generic UIs - Application Log for Global Trade Services Integration \[page 103\]](#)

13.2.3.1.4.1.1.1 Generic UIs - Application Job for Global Trade Services Integration

Context

On the back-end server, you have to assign the OData service authorization to a PFCG role. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

1. Assign Fiori catalog to PFCG role.
2. Assign additional authorization default for required application job catalog entry.
3. Fill authorization field P_PROGNAM with report name for authorization object S_PROGNAM

Business Catalog	Application Job Catalog Entry	Report Name	Fiori ID
SAP_SLL_BC_PI_BASIS	SAP_SLL_PI_DOCUMENT_RE PROCESS	/SAPSLI/ DOCUMENT_REPROCESS_R3	F3050 Schedule Reprocess- ing of Documents - Global Trade Services
SAP_SLL_BC_PI_PMD_TRAN S	SAP_SLL_PI_CREMAS_DIST RIBUTE	/SAPSLI/ CREMAS_DISTRIBUTE_R3	F2804 Schedule Transfer of Suppliers - Global Trade Services
SAP_SLL_BC_PI_PMD_TRAN S	SAP_SLL_PI_DEBMAS_DIST RIBUTE	/SAPSLI/ DEBMAS_DISTRIBUTE_R3	F2806 Schedule Transfer of Customers - Global Trade Services

Business Catalog	Application Job Catalog Entry	Report Name	Fiori ID
SAP_SLL_BC_PI_PMD_TRANS	SAP_SLL_PI_MATMAS_DIST RIBUTE	/SAPSL/ MATMAS_DISTRIBUTE_R3	F2805 Schedule Transfer of Products - Global Trade Services
SAP_SLL_BC_PI_CP_TRANS	SAP_SLL_PI_CPMAS_DISTR IBUTE	/SAPSL/ CPMAS_DISTRIBUTE_R3	F2803 Schedule Transfer of Contact Persons - Global Trade Services
SAP_SLL_BC_PI_BOM_TRANS	SAP_SLL_PI_BOMMAT_DIST RIBUTE	/SAPSL/ MATMAS_DISTRIBUTE_R3	F2807 Schedule Transfer of Bill of Materials - Global Trade Services
SAP_SLL_BC_PI_MM_DOC_TRANS	SAP_SLL_MM0A_DISTRIBUTE E_R3	/SAPSL/ MM0A_DISTRIBUTE_R3	F3742 Schedule Transfer of Purchasing Documents - Global Trade Services
SAP_SLL_BC_PI_PREF_TRANS	SAP_SLL_API_6850_PRPAR _KNM_PUT	/SAPSL/ API_6850_PRPAR_KNM_PUT	F3743 Schedule Transfer of Customer Product Name - Global Trade Services
SAP_SLL_BC_PI_PREF_TRANS	SAP_SLL_API_6850_PRPAR _PUT	/SAPSL/ API_6850_PRPAR_PUT	F3744 Schedule Transfer of Supplier Product Name - Global Trade Services
SAP_SLL_BC_PI_PREF_TRANS	SAP_SLL_MINMAX_DISTRIBUTE UTE_R3	/SAPSL/ MINMAX_DISTRIBUTE_R3	F3745 Schedule Transfer of Min./Max. Material Prices - Global Trade Services
SAP_SLL_BC_PI_PREF_TRANS	SAP_SLL_MM0C_DISTRIBUTE E_R3	/SAPSL/ MM0C_DISTRIBUTE_R3	F3741 Schedule Transfer of Material Documents - Global Trade Services
SAP_SLL_BC_PI_PREF_TRANS	SAP_SLL_SD0C_DISTRIBUTE E_RIMAR3	/SAPSL/ SD0C_DISTRIBUTE_RIMAR3	F3740 Schedule Transfer of Billing Documents - Global Trade Services
SAP_SLL_BC_PI_PREF_TRANS	SAP_SLL_PRCMAT_DISTRIBUTE UTE_R3	/SAPSL/ PRCMAT_DISTRIBUTE_R3	F3746 Schedule Transfer of Product Prices - Global Trade Services
SAP_SLL_BC_PI_PREF_TRANS	SAP_SLL_PSDMAT_DISTRIBUTE UTE_R3	/SAPSL/ PSDMAT_DISTRIBUTE_R3	F3747 Schedule Transfer of Procurement Indicators - Global Trade Services
SAP_SLL_BC_PI_IDLV_TRANS	SAP_SLL_PI_MM0B_DISTRIBUTE	/SAPSL/ MM0B_DISTRIBUTE_R3	F4541 Schedule Transfer of Inbound Deliveries - Global Trade Services

Business Catalog	Application Job Catalog Entry	Report Name	Fiori ID
SAP_SLL_BC_PI_SD_DOC_T RANS	SAP_SLL_PI_SD0A_DISTRI BUTE	/SAPSL/SD0A_DISTRIBUTE_R3	F4540 Schedule Transfer of Sales Documents - Global Trade Services
SAP_SLL_BC_PI_SD_DOC_T RANS	SAP_SLL_PI_SD0B_DISTRI BUTE	/SAPSL/SD0B_DISTRIBUTE_R3	F4539 Schedule Transfer of Outbound Deliveries - Global Trade Services

13.2.3.1.4.1.1.2 Generic UIs - Application Log for Global Trade Services Integration

Context

On the back-end server, you have to assign the OData service authorization to a PFCG role. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

1. Assign Fiori catalog to PFCG role.
2. Fill authorization data for authorization object S_APPL_LOG.
 1. Log Object -ALG_OBJECT
 2. Log Sub Object - ALG_SUBOBJ

Business Catalog	Log Object	Log Sub Object	Fiori ID
SAP_SLL_BC_PI_BASIS	/SAPSL/MD_GTS_DIST	/SAPSL/CPMAS_DIST /SAPSL/CREMAS_DIST /SAPSL/DEBMAS_DIST /SAPSL/MATMAS_DIST /SAPSL/BOMMAT_DIST /SAPSL/PRCMAT_DIST /SAPSL/PSDMAT_DIST /SAPSL/CPN_DIST /SAPSL/SPN_DIST	Application Log for Changed Master Data - Global Trade Services

13.2.3.1.4.1.2 Dependent Business Catalog for SAP Global Trade Services Integration

If you assign business catalog `SAP_SLL_BC_PI_BOM_TRANS` in the backend role, you also assign the business catalog `SAP_PLM_BC_MBOM_DISP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_PI_BOM_TRANS` in the backend role, you also assign the business catalog `SAP_CMD_BC_PRODUCT_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_PI_CP_TRANS` in the backend role, you also assign the business catalogs `SAP_CMD_BC_SUPPLIER_DSP` and `SAP_CMD_BC_CUSTOMER_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_PI_MM_DOC_TRANS` in the backend role, you also assign the business catalogs `SAP_CMD_BC_PRODUCT_DSP`, `SAP_CMD_BC_SUPPLIER_DSP`, and `SAP_CMD_BC_CUSTOMER_DSP` in the same backend role.

If you assign business catalog `SAP_SLL_BC_PI_PREF_TRANS` in the backend role, you also assign the business catalogs `SAP_SD_BC_BIL_DOC_DISPL`, `SAP_CMD_BC_PRODUCT_DSP`, `SAP_CMD_BC_SUPPLIER_DSP`, and `SAP_CMD_BC_CUSTOMER_DSP` in the same backend role.

13.2.3.1.4.2 Integration with SAP Watch List Screening

Related Information

[Manage Authorization for Generic UIs for Screening Integration \[page 104\]](#)

13.2.3.1.4.2.1 Manage Authorization for Generic UIs for Screening Integration

Related Information

[Generic UIs - Application Job for Watch List Screening Integration \[page 105\]](#)

13.2.3.1.4.2.1.1 Generic UIs - Application Job for Watch List Screening Integration

Context

On the back-end server, you have to assign the OData service authorization to a PFCG role. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

1. Assign Fiori catalog to PFCG role.
2. Assign additional authorization default for required application job catalog entry.
3. Fill authorization field P_PROGNAM with report name for authorization object S_PROGNAM

Business Catalog	Application Job Catalog Entry	Report Name	Fiori ID
SAP_SLL_BC_SCR_BASIS	SAP_SLL_SD0C_DISTRIBUT E_RIMAR3	/SAPSL/ WLS_POSTPROCESSING	F3052 Schedule Postpro- cessing - Watch List Screen- ing

13.2.3.1.4.3 Integration with Content Data Provider

Related Information

[Manage Authorizations for Generic UIs for Content Integration \[page 105\]](#)

13.2.3.1.4.3.1 Manage Authorizations for Generic UIs for Content Integration

Related Information

[Generic UIs - Application Job for Content Integration \[page 106\]](#)

13.2.3.1.4.3.1.1 Generic UIs - Application Job for Content Integration

Context

On the back-end server, you have to assign the OData service authorization to a PFCG role. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

1. Assign Fiori catalog to PFCG role.
2. Assign additional authorization default for required application job catalog entry.
3. Fill authorization field P_PROGNAM with report name for authorization object S_PROGNAM

Business Catalog	Application Job Catalog Entry	Report Name	Fiori ID
SAP_SLL_BC_CMMDTYCODE_ SCHD	SAP_SLL_CLSCT_COMCO_RE Q	/SAPSL/ CLSCT_COMCO_REQ	F3051 Schedule Content Request to Data Provider - Commodity Codes
SAP_SLL_BC_CTRLCLASS_S CHD	SAP_SLL_CLSCT_CONCL_RE Q	/SAPSL/ CLSCT_CONCL_REQ	F3568 Schedule Content Request to Data Provider - Control Classes
SAP_SLL_BC_TRIFNMBR_SC HD	SAP_SLL_CLSCT_TARNO_RE Q	/SAPSL/ CLSCT_TARNO_REQ	F3569 Schedule Content Request to Data Provider - Customs Tariff Numbers

13.2.3.1.5 Deletion of Personal Data in International Trade

International Trade might process data (personal data) that is subject to the data protection laws applicable in specific countries.

i Note

SAP S/4HANA for international trade does **not** use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. SAP S/4HANA for international trade uses SAP Business Partner (BP) instead to control the blocking and deletion of personal data.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for defining the settings for blocking. Choose Customizing, then [Cross-Application Components](#) under [Data Protection](#).

13.2.3.1.6 Standard Authorization Objects in International Trade

The following table shows the default authorization objects that you need for international trade.

Authorization Object	Description
ITM_BUKRS	Authorization for Company Code
ITM_LGREG	Authorization for Legal Regulation
ITM_LMGM	Authorization for Legal Regulation / License Type
/ECRS/RPHD	Intrastat Declaration
/ECRS/POIA	Provider of Information
/ECRS/SP	Selection Program for Intrastat Reporting
ITM_CLS_NC	Trade Classification: Auth. for Numbering Scheme Content
ITM_CLS_LR	Trade Classification: Authorization for Legal Regulation
ITM_CLS_NS	Trade Classification: Authorization for Numbering Scheme

13.2.4 Treasury Management

13.2.4.1 SAP Bank Communication Management (incl. SAP Integration Package for SWIFT)

About this Document

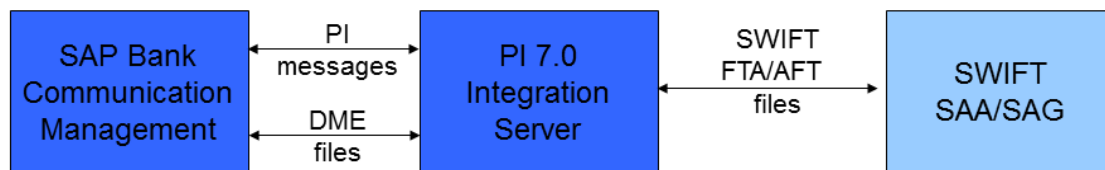
The Security Guide provides an overview of the specific security-relevant information that applies to the SAP *Bank Communication Management* including the SAP *Integration Package for SWIFT*.

13.2.4.1.1 Technical System Landscape

Use

SAP Bank Communication Management is responsible for the creation and approval of batches, the payment status monitor and bank statement monitor. Use of the *SAP Integration package for SWIFT* is **optional**; it provides a file interface to the *Swift Alliance Access/Alliance Gateway* (SWIFT is **not** SAP software and not part of *SAP Bank Communication Management*).

The figure below shows an overview of the technical system landscape for *SAP Bank Communication Management*.



For more information about recommended security zone settings, see *ABAP Platform Security Guide*.

13.2.4.1.2 User Management

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

The user types that are required for the SAP *Bank Communication Management* include:

- Individual users
Dialog users are used for SAP GUI for Windows connections.
- Technical users
Communication users are used for XI communication.

Standard Users

The table below shows the standard users that are necessary for operating the SAP *Bank Communication Management*.

System	User ID	Type	Password	Description
SAP Bank Communication Management	For example: BRMXIUSER	Communication user	You specify the initial password during the installation. The user ID and password are stored in the XI channel for the connection.	
XI Integration Server	For example: SWIFTADMIN	Default user	You specify the initial password during the installation.	Member of user group SWIFT_ADMINISTRATOR as described in the <i>SAP Integration Package for SWIFT Configuration Guide</i> .

You need to create these users before XI configuration.

Assign role SAP_XI_IS_SERV_USER to user BRMXIUSER and role SWIFT_ADMINISTRATOR to user SWIFTADMIN.

Creation of role SWIFT_ADMINISTRATOR is described in the *SAP Integration Package for SWIFT Configuration Guide*.

13.2.4.1.3 Communication Destinations

The table below shows an overview of the communication destinations used by SAP *Bank Communication Management*.

Destination	Delivered	Type	User, Authorizations
INTEGRATION_SERVER	No	RFC	XIAPPLUSER Role SAP_XI_APPL_SERV_USER
LCRSAPRFC	No	RFC	
SAPSLDAPI	No	RFC	

These destinations are not application-specific but they are required for the operation of the Exchange Infrastructure.

13.2.4.1.4 Data Storage Security

Master and transaction data of *SAP Bank Communication Management* is saved in the database of the SAP system in which *SAP Bank Communication Management* is installed.

Access to this data is restricted through the authorizations for authorization object `F_STAT_MON`. You can add this authorization object to the role or user that is used by you for payment medium creation.

Payment order related transaction data is distributed to connected systems using XI, especially if the optional Integration Package for SWIFT is used.

Access to data on natural persons in particular is subject to data protection requirements and must be restricted by assigning authorizations.

Using Logical Path and Filenames to Protect Access to the File System

SAP Bank Communication Management saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by *SAP Bank Communication Management* and for which programs these file names and paths apply:

Logical File Names Used in SAP Bank Communication Management

The following logical file names have been created in order to enable the validation of physical file names:

- `FI_RFEBKATO_FILE`
 - Program using this logical file name and parameters used in this context:
 - `RFEBKATO`
- `FI_RFEBKATX_FILE`
 - Program using this logical file name and parameters used in this context:
 - `RFEBKATX`
- `FI_RFEBKAT1_FILE`
 - Program using this logical file name and parameters used in this context:
 - `RFEBKAT1`
- `FI_RFEBESTO_FILE`
 - Program using this logical file name and parameters used in this context:
 - `RFEBESTO`
- `FI_RFEBLBT1_FILE`

- Program using this logical file name and parameters used in this context:
 - RFEBLBT1
- FI_RFEBLBT2_FILE
 - Program using this logical file name and parameters used in this context:
 - RFEBLBT2

Parameters used in this context: <PARAM_1> Program name

Logical Path Name Used in SAP Bank Communication Management

The logical file names listed above all use the logical file path FI_FTE_TEST_FILES .

13.2.4.2 SAP In-House Cash (FIN-FSCM-IHC)

In the following sections you can find information about the specific security functions for the *SAP In-House Cash* (FIN-FSCM-IHC) component.

In addition, you can access further information at the following places:

For information about the specific security functions for the component *Bank Customer Accounts* (IS-B-BCA), see *Bank Customer Accounts (BCA) [page 818]* in the Banking section.

Reason: *SAP In-House Cash* (FIN-FSCM-IHC) uses *Bank Customer Accounts* as the basis for various functions.

For information about the specific security functions for the component *Bank Accounting* (FI-BL), see the under *Bank Accounting (FI-BL) [page 84]* in the Banking section.

Reason: *SAP In-House Cash* (FIN-FSCM-IHC) uses various functions of *Bank Accounting* , such as the creation of data media for central payments.

13.2.4.2.1 Security Aspects of Data, Data Flow and Processes

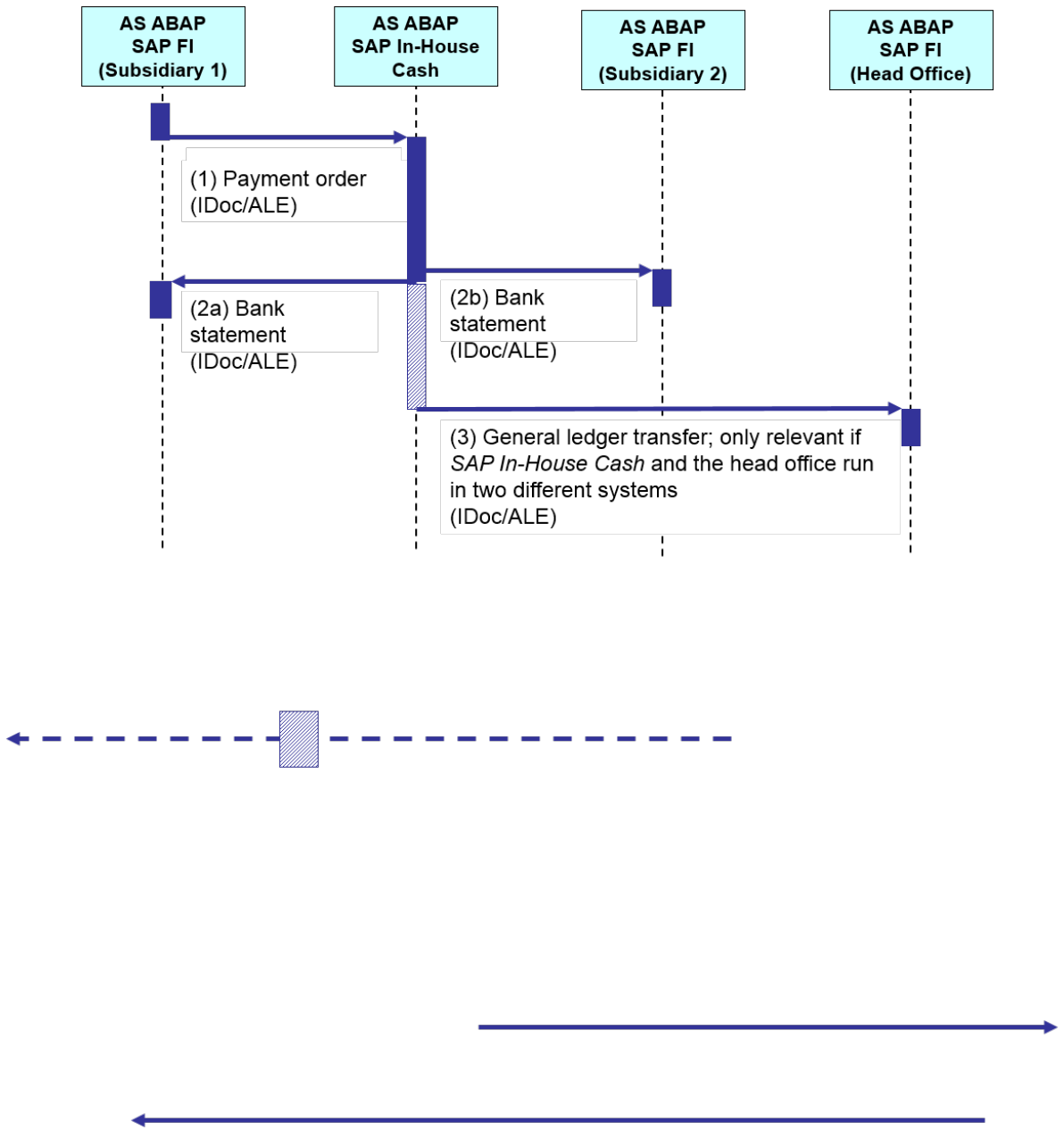
The following sections show an overview of the data flow in the processes of *SAP In-House Cash* .

i Note

The appropriate Security Guides apply for all of the external systems that you require when using the *SAP In-House Cash* component. Include these Security Guides in your cross-application security concept.

13.2.4.2.1.1 Internal Payments

The figure below shows an overview of internal payments between two subsidiary companies and the transfer of the balances to the general ledger.



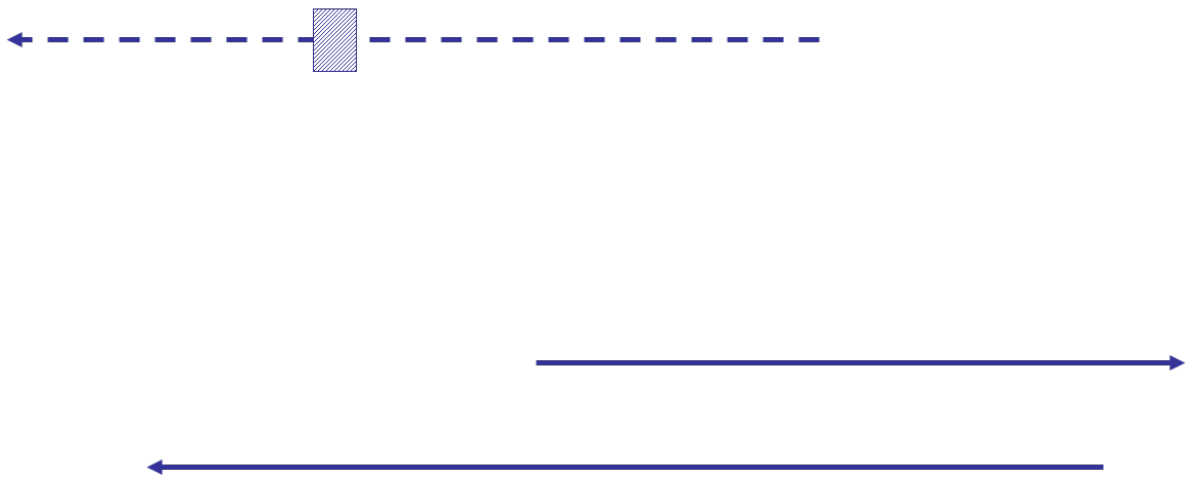
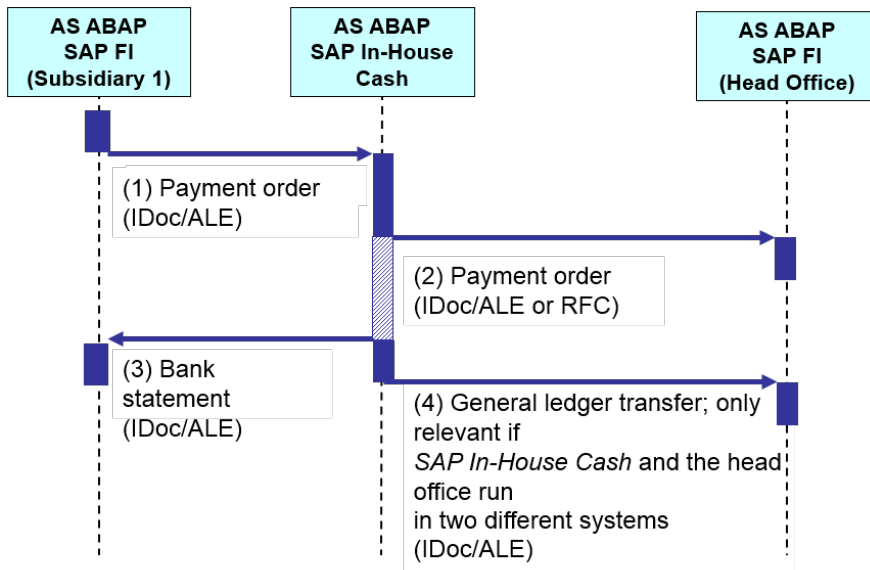
The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	Payment order (IDoc/ALE)	User type: dialog user or technical user
2a	Bank statement (IDoc/ALE)	User type: dialog user or technical user

Step	Description	Security Measure
2b	Bank statement (IDoc/ALE)	User type: dialog user or technical user
3	General ledger transfer; only relevant if <i>SAP In-House Cash</i> and the head office are running in two different systems (IDoc/ALE)	User type: dialog user or technical user

13.2.4.2.1.2 Head Office Payments

The following figure shows an overview of the data flow if the head office takes over the payments for the payables of a single subsidiary company.



The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	Payment order (IDoc/ ALE)	User type: dialog user or technical user
2	Payment order (IDoc/ ALE or RFC)	User type: dialog user or technical user

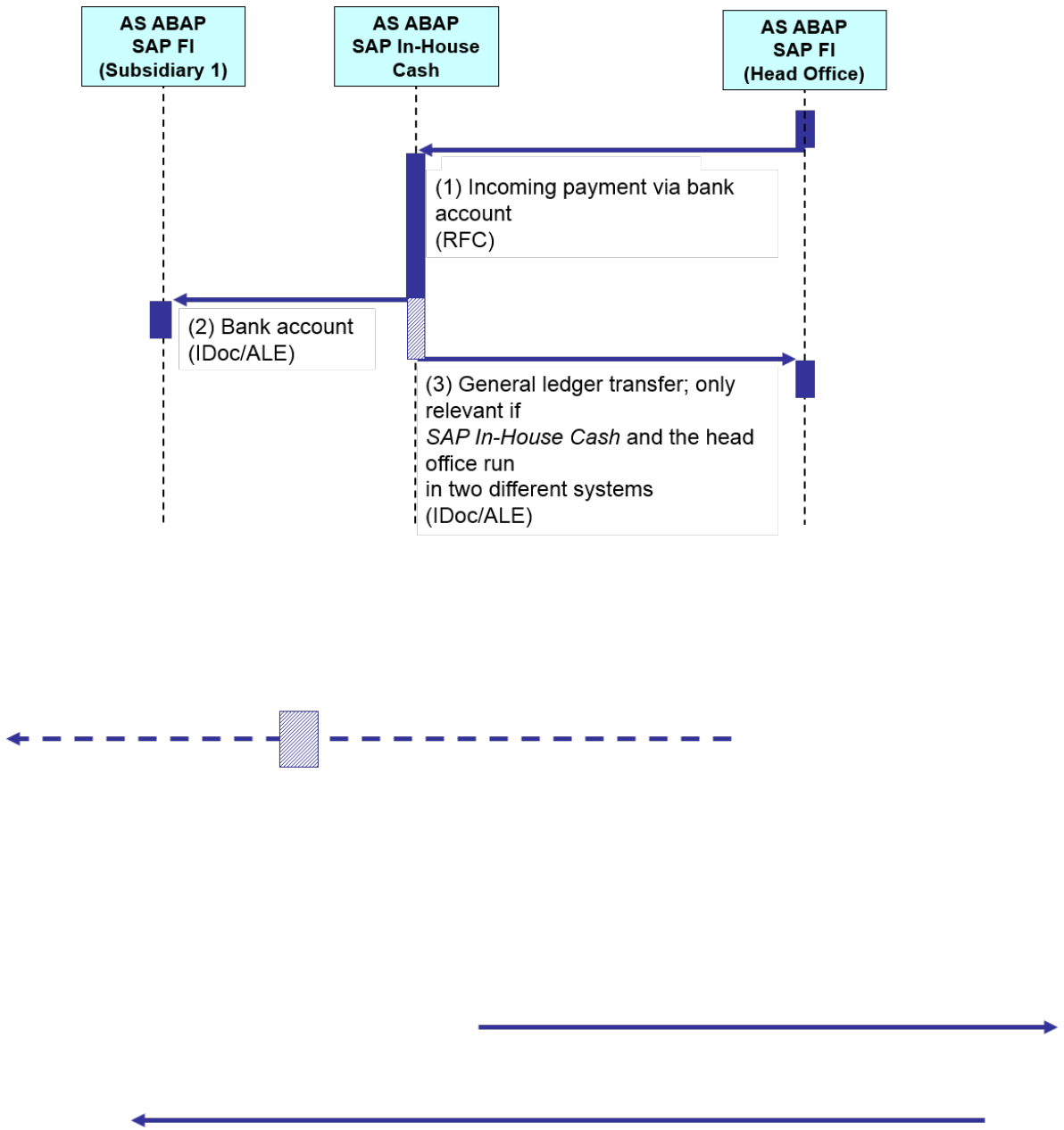
Step	Description	Security Measure
3	Bank statement (IDoc/ ALE)	User type: dialog user or technical user
4	General ledger transfer; only relevant if <i>SAP In-House Cash</i> and the head office are running in two different systems (IDoc/ ALE)	User type: dialog user or technical user

i Note

The type of communication for the second step depends on your settings. If you have activated the *In-House Cash (Enterprise)* (IHC_EP) application, then communication is by RFC. Otherwise it is by IDoc/ ALE . You can find these settings in Customizing of *SAP In-House Cash* under *Basic Settings* → *Business Transaction Events/Event Control* → *Activate SAP Components* .

13.2.4.2.1.3 Central Incoming Payments

The figure below shows an overview of an incoming payment that is intended for a subsidiary company of the head office.



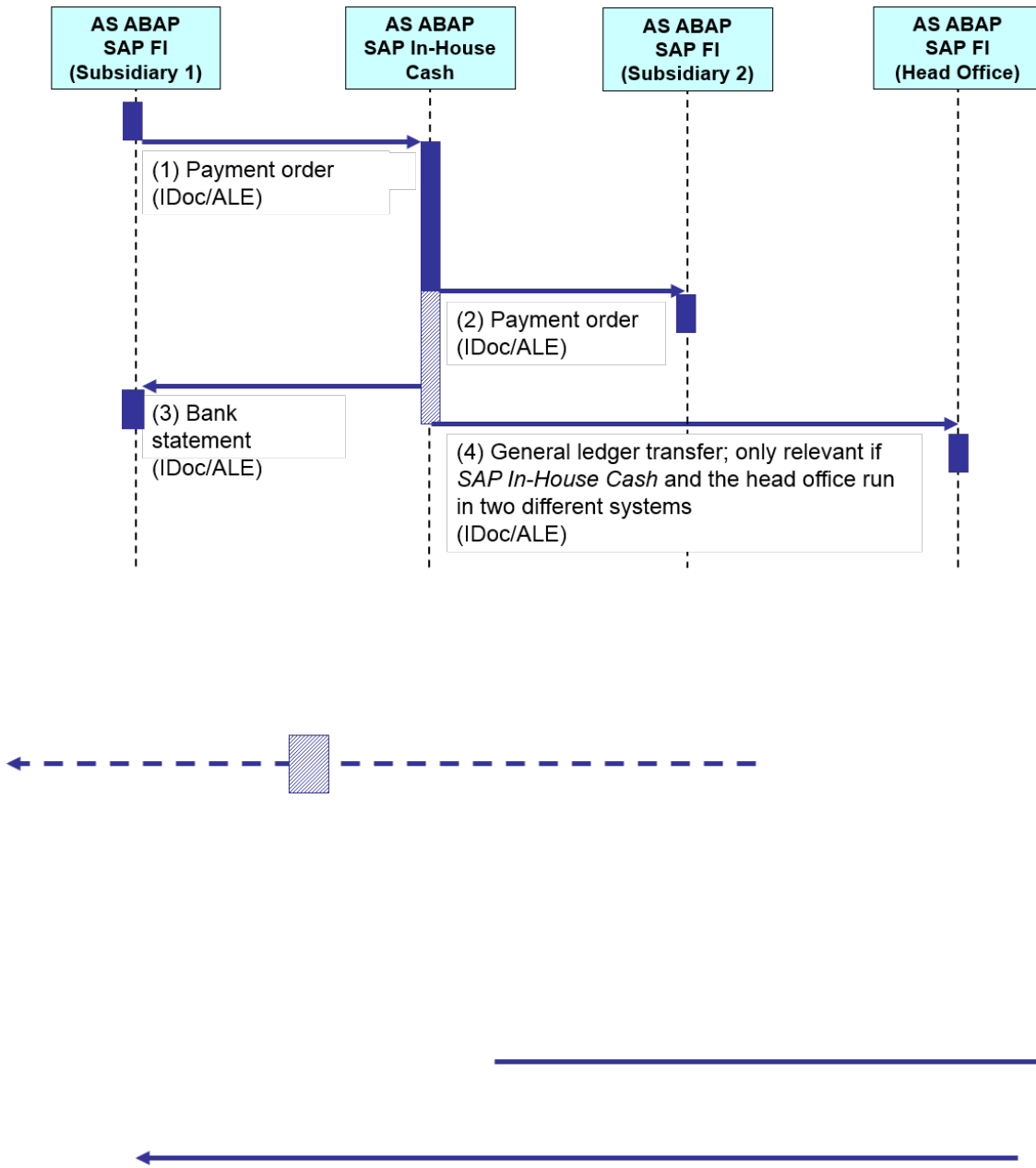
The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	Incoming payment via bank statement (RFC)	Access authorization via RFC user
2	Bank statement (IDoc/ALE)	User type: dialog user or technical user

Step	Description	Security Measure
3	General ledger transfer; only relevant if <i>SAP In-House Cash</i> and the head office are running in two different systems (IDoc/ALE)	User type: dialog user or technical user

13.2.4.2.1.4 Local Payments

The figure below shows an overview of the data flow if a subsidiary company uses the house bank of a different subsidiary company for its payment that is located in the country of the payment recipient. This avoids having to make a foreign payment. The process flow is similar to [Head Office Payments \[page 113\]](#).



The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	Payment order(IDoc/ALE)	User type: dialog user or technical user
2	Payment order(IDoc/ALE)	User type: dialog user or technical user
3	Bank statement(IDoc/ALE)	User type: dialog user or technical user

Step	Description	Security Measure
4	General ledger transfer; only relevant if <i>SAP In-House Cash</i> and the head office are running in two different systems (IDoc/ALE)	User type: dialog user or technical user

13.2.4.3 Cash and Liquidity Management

Network and Communication Security

Communication with external systems is possible using standard interfaces via BAPI, IDoc, and XI.

Communication Destinations

In certain cases, a technical user may be required for the use of BAPIs.

Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For more information, see [Internet Communication Framework Security \(ICF\) \[page 119\]](#).

Data Storage Security

You can use logical path and file names to protect access to the file system. For more information, see [Data Storage Security \[page 121\]](#).

13.2.4.3.1 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For Cash and Liquidity Management, the following services are needed:

- Web Dynpro services
 - WDA_FCLM_BAM_ACC_MASTER
 - WDA_FCLM_BAM_ACC_REVIEW

- WDA_FCLM_BAM_ADAPT_SIGN
- WDA_FCLM_BAM_BANK_DATA
- WDA_FCLM_BAM_CHGREQ
- WDA_FCLM_BAM_HIERARCHY
- WDA_FCLM_BAM_HIER_BP
- WDA_FCLM_BAM_HIER_MAINTAIN
- WDA_FCLM_BAM_MASS_CHANGE
- WDA_FCLM_BAM_REVIEW_REPORT
- WDA_FCLM_BAM_REQOVERVIEW
- WDA_FCLM_REPORT
- WDA_FCLM_UPLOAD_DOWNLOAD
- WDA_FCLM_BAM_SENTITEMS
- WD_FCLM_FPM_OVP_CFA
- WD_FCLM_FPM_OVP_FD
- WD_FCLM_FPM_OVP_FO
- Workflow services
 - ibo_wda_inbox
 - swf_formabsenc
 - swf_workplace
 - UCT_DISPLAY_DOCUMENT
 - UCT_DISPLAY_INBOX
 - UCT_DISPLAY_SIGNOFF
 - UCT_DISPLAY_CHANGE
 - USMD_CREQUEST_PROTOCOL2
 - USMD_SSW_RULE
 - USMD_WF_NAVIGATION
- POWL services
 - POWL
 - POWL_COLLECTOR
 - powl_composite
 - POWL_EASY
 - POWL_ERRORPAGE
 - POWL_MASTER_QUERY
 - POWL_PERS_COMP

Use the transaction **SICF** to activate these services. If your firewalls use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly. For more information about ICF security, see the respective chapter in the ABAP Platform Security Guide.

13.2.4.3.2 Data Storage Security

Using Logical Paths and File Names to Protect Access to the File System

Cash and Liquidity Management saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following list shows the logical paths and file names that are used in Cash and Liquidity Management and the programs for which these file names and paths apply. The logical paths and file names have been created to activate the validation of physical file names:

Logical file names used in Cash and Liquidity Management:

- FCLM_CM_MEMO_RECORD_EXPORT
 - Name of the program that uses this logical file name:
RFTS6510_CREATE_STRUCTURE (transaction RFTS6510CS)
 - Parameters used in this context:
No parameters
 - Logical path name:
FCLM_CM_MEMO_RECORD_EXPORT
- FCLM_CM_MEMO_RECORD_IMPORT
 - Name of the program that uses this logical file name:
RFTS6510 (transaction RFTS6510)
 - Parameters used in this context:
No parameters
 - Logical path name:
FCLM_CM_MEMO_RECORD_IMPORT

Activating the Validation of Logical Paths and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-dependent). To determine which paths are used by your system, you can activate the appropriate settings in the Security Audit Log.

13.2.4.3.3 Data Protection

13.2.4.3.3.1 Deletion of Personal Data

Use

Cash and Liquidity Management might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. Cash and Liquidity Management uses SAP ILM to support the deletion of personal data as described in the following sections.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Bank Account Master Data	<p>You can destroy the bank account contact person data, namely the general contacts and the bank relationship managers that are maintained in the bank account master data.</p> <p>For more information about this object, see the <i>Data Management in Cash and Liquidity Management</i> topic. You can find this topic in the <i>Product Assistance</i> under ► Finance ► Treasury and Risk Management ► Cash and Liquidity Management ►.</p>	Destruction object BAM_AMD
One Exposure from Operations	<p>You can destroy personal data that are stored in the database table FQM_FLOW, including business partners, customers, and suppliers.</p> <p>For more information about this object, see the <i>Data Management in Cash and Liquidity Management</i> topic. You can find this topic in the <i>Product Assistance</i> under ► Finance ► Treasury and Risk Management ► Cash and Liquidity Management ►.</p>	Destruction object FQM_FLOW

Application	Detailed Description	Provided Deletion Functionality
One Exposure from Operations	<p>As an alternative to the ILM destruction object <code>FQM_FLOW</code>, you can use this transaction to delete flows with certainty level <code>ACTUAL</code> in One Exposure and substitute them with aggregation flows. It helps to reduce the data volume in database table <code>FQM_FLOW</code> and delete personal data.</p> <p>For more information, see the corresponding program documentation.</p>	Transaction <code>FQM_AGGREGATE_FLOWS</code>
One Exposure from Operations	<p>As an alternative to the ILM destruction object <code>FQM_FLOW</code>, you can use this transaction to delete transactional data in One Exposure from Operations to ensure data protection and privacy. The deleted data will no longer be displayed in cash management reports.</p> <p>For more information, see the corresponding program documentation.</p>	Transaction <code>FQM_DELETE</code>

Relevant Application Objects and Available EoP/WUC Functionality

Application	Implemented Solution	Further Information
One Exposure from Operations	<p>EoP check with function module</p> <p><code>FQM_BUPA_WUC_CHECK</code></p>	It checks if business partners are still relevant for One Exposure from Operations in the <code>FQM_FLOW</code> table.
Bank Account Master Data	<p>EoP check with function module</p> <p><code>FCLM_BAM_EOP_CHECK</code></p>	<p>It checks if business partners are still relevant for bank account management in the following tables:</p> <ul style="list-style-type: none"> <code>FCLM_BAM_AMD</code> <code>FCLM_BAM_BNKABP2</code>

For more information about the above checks, see the [Data Management in Cash and Liquidity Management](#) topic. You can find this topic in the [Product Assistance](#) under [► Finance](#) [► Treasury and Risk Management](#) [► Cash and Liquidity Management](#) [►](#).

Process Flow for Destroying Business Partners in Bank Account Master Data

To destroy business partner data in the bank account master data, proceed as follows:

1. Before deleting data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
3. Run transaction `IRMPOL` and maintain the required residence and retention policies for the central business partner (ILM object: `BAM_AMD`).
4. You delete data by using the transaction `ILM_DESTRUCTION` for the ILM object `BAM_AMD`.



Process Flow for Destroying Business Partners, Customers, and Suppliers in One Exposure from Operations

To destroy business partner, customer and supplier data in One Exposure from Operations, proceed as follows:

1. Before deleting data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
3. Run transaction `IRMPOL` and maintain the required residence and retention policies for the central business partner (ILM object: `FQM_FLOW`).
4. You delete data by using the transaction `ILM_DESTRUCTION` for the ILM object `FQM_FLOW`.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management under **► Cross-Application Components ► Data Protection ► Authorization Management** .
- Check the following settings for blocking in Customizing for *Cross-Application Components* under **► Data Protection ► Blocking and Unblocking of Data ► Business Partner** 
 - In the *Define Application Names for EoP Check* Customizing activity (view `V_BUTEOPAPP`), you find the following applications in the view:
 - *One Exposure from Operations* (`FQM`)
 - *Bank Account Management* (`FIN_FSCM_CLM_BAM`)
 - In the *Define Application Function Modules Registered for EoP Check* Customizing activity (view `V_BUTEOPFM`), you find a list of application function modules. Each application that consumes business partners registered their function module in this view. These function modules are called by the blocking/unblocking report when performing the end-of-purpose checks.
 - `FQM`: Function module `FQM_BUPA_WUC_CHECK`

- FIN_FSCM_CLM_BAM: Function module FCLM_BAM_EOP_CHECK

For more information about configuration, see the Customizing documentation.

13.2.4.4 Treasury and Risk Management

13.2.4.4.1 Data Storage Security

Using Logical Paths and File Names to Protect Access to the File System

SAP Treasury and Risk Management (FIN-FSCM-TRM) saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following list shows the logical paths and file names that are used in *SAP Treasury and Risk Management* (FIN-FSCM-TRM) and the programs for which these file names and paths apply. The logical paths and file names have been created to activate the validation of physical file names:

Logical file names used in *SAP Treasury and Risk Management*

- FTRM_FTR_DEALDATA_AMORTIZATION_SCHEDULES_IMPORT
 - Program that uses this logical file name:
 - RFTR_INTF_MAINFLOWS_UPLOAD
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_FTR_DEALDATA_IMPORT.
- FTRM_TCR_MARKETDATA_DF_IMPORT
 - Program that uses this logical file name:
 - RFTBDF06 [function *Datafeed: Import External Market Data in Datafeed Notation* (transaction TBD5)]
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_DF_IMPORT.
- FTRM_TCR_MARKETDATA_DF_SECURITIES_IDS_IMPORT_FOR_CUSTOMIZING
 - Program that uses this logical file name:
 - RFTBDF05 [function *Datafeed: Import Security ID Numbers* (transaction TBD2)]
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_DF_IMPORT.
- FTRM_TCR_MARKETDATA_FF_REQUEST_LIST_EXPORT
 - Program that uses this logical file name:
 - RFTBFF01 [function *Market Data File Interface: Generate Rates and Prices Request List* (transaction TBDN)]

- No parameters are used in this context:
- The logical file name uses the logical file path FTRM_TCR_MARKETDATA_FF_EXPORT.
- FTRM_TCR_MARKETDATA_FF_IMPORT
 - Program that uses this logical file name:
 - RFTBFF01 [function *Market Data File Interface: Import Rates and Prices* (transaction TBDM)]
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_FF_IMPORT.
- FTRM_TCR_MARKETDATA_FF_ERRORLOG_EXPORT
 - Program that uses this logical file name:
 - RFTBFF01 [function *Market Data File Interface: Import Rates and Prices* (transaction TBDM)]
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_FF_EXPORT.
- FTRM_TCR_MARKETDATA_FF_SECURITIES_YEAR_END_PRICES_IMPORT
 - Program that uses this logical file name:
 - RFDWZFF0
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_FF_IMPORT.
- FTRM_TCR_MARKETDATA_FF_STATISTICS_IMPORT
 - Program that uses this logical file name:
 - RFTBFF20 [function *Market Data File Interface: Import Statistics Data* (transaction TVMD)]
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_FF_IMPORT.
- FTRM_TCR_TEMP_TCURC_EXPORT (*Treasury: Sequential Output File for TCURC*)
 - Program that uses this logical file name:
 - RZKLAODC
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TCR_TEMP_EXPORT.
- FTRM_TCR_TEMP_TCURT_EXPORT (*Treasury: Sequential Output File for TCURT*)
 - Program that uses this logical file name:
 - RZKLAODT
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_TCR_TEMP_EXPORT.
- FTRM_FTR_RED_SCHEDULE (*Treasury: Redemption Schedule Parser*)
 - Program that uses this logical file name:
 - FTBAS_SCHEDULE_BATCH_LOAD
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_FTR_RED_SCHEDULE.
- FTRM_AN_LIMIT
 - Program that uses this logical file name:
 - RFTBLBI1 (*Batch Input Report for Creating Limits*)
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_AN_LIMIT.

- FTRM_AN_INT_LIMIT
 - Program that uses this logical file name:
 - RFTBLBI1 (*Batch Input Report for Creating Limits*)
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_AN_INT_LIMIT.
- FTRM_TCR_MARKETDATA_FF_DERIVATIVE_PRICES_ERRORLOG_EXPORT
 - Program that uses this logical file name:
 - RFTBFF30 (*Import DTB Derivative Prices*: transaction TVDT)
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_FF_EXPORT.
- FTRM_TCR_MARKETDATA_FF_DERIVATIVE_PRICES_IMPORT
 - Program that uses this logical file name:
 - RFTBFF30 (*Import DTB Derivative Prices*: transaction TVDT)
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_TCR_MARKETDATA_FF_IMPORT.
- FTRM_AN_BATCH_INPUT_DER
 - Programs using this logical file name:
 - RJBDBTC3 (*Batch Input for Derivatives*)
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_AN_BATCH_INPUT_DER.
- FTRM_AN_BATCH_INPUT_MM
 - Programs using this logical file name:
 - RJBDBTC2 (*Batch Input for Derivatives*)
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_AN_BATCH_INPUT_MM.
- FTRM_AN_BATCH_INPUT_FX
 - Programs using this logical file name:
 - RJBDBTC1 (*Batch Input for FX Transactions*)
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_AN_BATCH_INPUT_FX.
- FTRM_AN_BATCH_INPUT_ERR_FILE
 - Programs using this logical file name:
 - Include MJBHF01
 - No parameters are used in this context.
 - The logical file name uses the logical file path FTRM_AN_BATCH_INPUT_ERR_FILE.
- FTRM_TARO_SEND
 - Programs using this logical file name:
 - R_TLR_TARO_SEND
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TARO_SEND (this is where the send program puts the files to be sent to the repository)
- FTRM_TARO_IMPORT

- Programs using this logical file name:
 - R_TLR_TARO_IMPORT and R_TLR_TARO_IMPORT_REPORTS
- No parameters are used in this context:
- The logical file name uses the logical file path FTRM_TARO_IMPORT (this is where the system expects files sent by the repository)
- FTRM_TARO_ARCHIVE
 - Programs using this logical file name:
 - R_TLR_TARO_IMPORT and R_TLR_TARO_IMPORT_REPORTS
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TARO_ARCHIVE (this is where imported files are stored if they were successfully imported)
- FTRM_TARO_ERROR
 - Programs using this logical file name:
 - R_TLR_TARO_IMPORT and R_TLR_TARO_IMPORT_REPORTS
 - No parameters are used in this context:
 - The logical file name uses the logical file path FTRM_TARO_ERROR (this is where imported files are stored if they were NOT successfully imported but caused an error)

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log. For more information, see about data storage security, see the respective chapter in the ABAP Platform Security Guide.

13.2.5 Financial Operations

13.2.5.1 Contract Accounting

13.2.5.1.1 Data Storage Security

Contract Accounts Receivable and Payable (FI-CA) saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following list shows the logical file names and paths used by Contract Accounts Receivable and Payable (FI-CA) and for which programs these file names and paths apply:

Logical File Names Used in FI-CA and Logical Path Names

The following logical file names have been created in order to enable the validation of physical file names:

Program	Logical File Name Used by the Program	Logical Path Name Used by the Program
RFKIBI_FILE00	FICA_DATA_TRANSFER_DIR	FICA_DATA_TRANSFER_DIR
RFKIBI_FILEP01		
RFKKBI_FILEEDIT		
RFKKBIBG		
RFKKZEDG		
RFKKRLDG		
RFKKCMDG		
RFKKCRDG		
RFKKAVDG		
RFKKBIB0		
RFKKZE00		
RFKKRL00		
RFKKCM00		
RFKKCR00		
RFKKAV00		
RFKKKA00		
RFKKBIT0		
RFKKPCSF	FI-CA-CARD-DATA-S	FI-CA-CARD-DATA-S
RFKKPCDS		
RFKKCVSPAY	FI-CA-CVS	FI-CA-CVS

RFKK_CVSPAY_CONFIRM		
RFKKCVSCONFIRMDB		
RFKK_CVSPAY_CONFIRM_TEST		
RFKK_DOC_EXTR_EXP	FI-CA-DOC-EXTRACT-DIR	FI-CA-DOC-EXTRACT-DIR
RFKK_DOC_EXTR_AEXP		
RFKK_DOC_EXTR_IMP		
RFKK_DOC_EXTR_EXTR		
RFKK_DOC_EXTR		
RFKK_DOC_EXTR_DEL		
Class CL_FKK_TEXT_FILE		
RFKKBIXBITUPLOAD	FI-CA-BI-SAMPLE FI-CA-BI-SAMPLE-DIR	FI-CA-BI-SAMPLE-DIR
RFKKCOL2	FI-CA-COL-SUB	FI-CA-COL-SUB
RFKKCOLL		
Transaction FP03DM (Mass Activity)		
Transaction FPCI (Mass Activity)	FI-CA-COL-INFO	FI-CA-COL-INFO
RFKKCOPM	FI-CA-COL-READ	FI-CA-COL-READ
READFILE		
RFKKCOPG	FI-CA-COL-TEST	FI-CA-COL-TEST
RFKKRDI_REPORT	FI-CA-RDI	FI-CA-RDI
RFKKRDI_REPORT_DIS		
SAPFKPY3	FI-CA-DTA-NAME	FI-CA-DTA-NAME
RFKKCHK01	FI-CA-CHECKS-EXTRACT	FI-CA-CHECKS-EXTRACT
Class CL_FKK_INFICO_SEND	FI-CA-INFICO	FI-CA-INFICO
RFKKBE_SAL1	FICA_BE_SAL	FICA_BE_SAL
RFKKBE_SAL2	FICA_BE_SAL_XML	FICA_BE_SAL_XML
RFKK1099	FI-CA-1099	FI-CA-1099

RFKKOP03	FICA_OPEN_ITEMS	FICA_OPEN_ITEMS
RFKKOP04		
RFKKOP07		
RFKKES_SAL1	FICA_TAX_REP_GEN	FICA_TAX_REP_GEN
RFKKES_SAL2		
RFKKRDI_REPORT	FI-CA-RDI	FI-CA-RDI
RFKKRDI_REPORT_DIS		
Transaction EMIGALL	ISMW_FILE	ISMW_ROOT

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information about data storage security, see the chapter in the ABAP Platform Security Guide.

13.2.5.1.2 Data Protection

Contract Accounts Receivable and Payable (FI-CA) processes personal data of business partners that might be subject to data protection legislation applicable in some countries.

Contract Accounts Receivable and Payable (FI-CA) uses SAP ILM to support the deletion of this personal data. SAP delivers an end of purpose check for Contract Accounts Receivable and Payable (FI-CA). You register the end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the SAP Business Partner.

Display of Blocked Data

Only if a user has special authorization, is it possible to display blocked business partner master data. However, it is still not possible to create, change, copy, or perform follow-up activities on this blocked business partner data.

However, FI-CA-specific data relating to a blocked business partner (as for example the contract account) users can display without having special authorization.

For more information on the blocking and deletion of personal data, on the end of purpose check and on displaying blocked data in Contract Accounts Receivable and Payable, see the Product Assistance of Contract Accounts Receivable and Payable under [Basic Functions](#) > [SAP Business Partner](#) > [Blocking and Deleting Personal Data](#).

Process Flow

Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM). You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available. You do the following:

1. Run transaction `IRMPOL` and maintain the required residence and retention policies for the central business partner (ILM object: `CA_BUPA`).
2. Run transaction `FDPDR_BP_INIT` once for existing business partners for which you want to execute the end of purpose checks. New business partners you create are automatically included in the end of purpose checks.
3. Run transaction `FDPDR1` to prepare the end of purpose check of the central business partner. The function module `MKK_BUPA_EOP_CHECK` saved for Contract Accounts Receivable and Payable (FI-CA) in table `BUTEOPFM` provides the EoP check result obtained by transaction `FDPDR1` to transaction `BUPA_PRE_EOP`.
4. Run transaction `BUPA_PRE_EOP` to enable the end of purpose check function for the central business partner.

Business users can request unblocking of blocked data by using the transaction `BUP_REQ_UNBLK`.

If you have the needed authorizations, you can unblock data by running the transaction `BUPA_PRE_EOP`.

You delete data by using the transaction `ILM_DESTRUCTION` for the ILM objects of Contract Accounts Receivable and Payable (FI-CA).

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for Cross-Application Components under [Data Protection](#).

Define the settings for authorization management under [Authorization Management](#). For more information, see the Customizing documentation.

Define the settings for blocking under [Blocking and Unblocking Business Partner](#). For more information, see the Customizing documentation.

You configure the settings specific for Contract Accounts Receivable and Payable in the Customizing for Contract Accounts Receivable and Payable under [Technical Settings](#) > [Data Protection](#) and [Data Deletion](#). For more information, see the Customizing documentation.

13.2.5.1.3 Payment Card Security According to PCI-DSS

i Note

The **Payment Card Industry Data Security Standard (PCI-DSS)** was jointly developed by major credit card companies in order to create a set of common industry security requirements for the protection of cardholder data. Compliance with this standard is relevant for companies processing credit card data. For more information, see <http://www.pcisecuritystandards.org>.

The following sections of the security guide support you in implementing payment card security aspects and outline steps that need to be considered to be compliant with the PCI-DSS.

Please note that the PCI-DSS covers more than the steps and considerations given here. Complying with the PCI-DSS lies completely within the customer's responsibility, and we cannot guarantee the customer's compliance with the PCI-DSS.

For current information about PCI-DSS in general, see SAP Note [1609917](#).

Contract Accounts Receivable and Payable (FI-CA) processes all payment transactions with your business partners. For this purpose, Contract Accounts Receivable and Payable also processes credit card data. For processing credit card transactions, Contract Accounts Receivable and Payable follows the rules laid down by the Payment Card Industry Data Security Standard.

Credit card data arrives in Contract Accounts Receivable in the following ways:

- You receive documents, which already contain credit card data in their supplements, by means of the IDoc interface or by means of BAPIs.
- You receive payments that already contain credit card data with the payment lot transfer program (RFKKZE00).
- External payment collectors and external cash desk services transfer credit card data using enterprise services with the payment to Contract Accounts Receivable and Payable.
- Financial Customer Care transfers credit card data for documents from SAP Customer Relationship Management using RFC.
- Customers or your employees add credit card data as follows:
 - Employees enter credit card data in the master records of business partners and prepaid accounts.
 - Employees enter payment card data in the *Maintain Bank Data* (FPP4) transaction.
 - Employees enter credit card data for payments in the cash desk, in the cash journal, in payment specifications and in promises to pay.
 - Customers enter credit card data online in SAP Biller Direct. SAP Biller Direct transfers the data to Contract Accounts Receivable and Payable.
- You adopt billable items with payment information using the generated RFC interfaces /1FE/<billable item class>_BIT_CREATE_API.

The program for payment (such as the payment run or the cash desk) generates payment documents with supplements containing the credit card data. Contract Accounts Receivable and Payable transfers this credit card data to the payment card company or the clearing house using transaction FPPCDS (creation of file) or FPCS (online transfer).

Contract Accounts Receivable and Payable stores the data as follows:

Object	Table(s)
Business Partner Master Record	BUT0CC
	CCARD
Payments in Payment Lot or Credit Card Lot	DFKKZP
Document	DFKKOPC
	DFKKOPKC
	DFKK_PCARD

Payment Data for a Payment Run	DPAYH
Payment Data for a Payment Using SAP Biller Direct or Financial Customer Care	DFKKOPC
Payment Specifications	DFKKIP_GRP
Promises to pay	DFKKPPD_PAY
Master Record of Prepaid Account	FKKPREPACC
Billable Items	Generated tables: <ul style="list-style-type: none"> • /1FE/0<billable item class>OPY • /1FE/0<billable item class>1PY

You must restrict the display of the necessary objects by assigning authorizations, while at the same time ensuring that this authorization protection cannot be circumvented by database programs or customer-specific ABAP reports.

You can also make additional security settings for payment card data. For more information, see SAP Note [1032588](#) and the SAP S/4HANA Security Guide, section "Payment Card Security".

Archiving

Only masked credit card information can be archived. Clear text credit card information should not be archived. Archiving encrypted credit card information is problematic because archived data should not be changed. Encrypted credit card information has to be re-encrypted with a different key, for example, with key rotation, as required by PCI-DSS. This change of data is not possible in an archive.

In technologies that are agnostic to the semantics of the data, such as Process Integration (PI), ABAP Web Services, or Forward Error Handling (FEH), archiving has to be disabled. IDocs that contain credit card information should not be archived.

Interfaces (IDoc/Services)

⚠ Caution

According to PCI-DSS, IDoc segments are not allowed to store payment card numbers in clear text. However, during processing of an IDoc in the IDoc Framework, all values are stored temporarily, including the clear text credit card number.

For more information about how to process customer-specific IDocs containing credit card information, go to https://help.sap.com/s4hana_op_2020, enter *Handling Sensitive Data in IDocs* into the search bar, press , and open the search result with that title.

If you exchange data between systems using IDoc messages, and this data contains unencrypted credit card information, you have to implement access restrictions and a deletion concept at the level of the file system.

Contract Accounts Receivable and Payable processes payment card data in the following interfaces:

Type of Interface	Technical Name	Description
-------------------	----------------	-------------

BAPI	BAPI_CTRACPREPAIDACCOUNT_CREA	<i>BAPI - FI-CA Prepaid Account: Create</i>
BAPI	BAPI_CTRACPREPAIDACCOUNT_CHNG	<i>BAPI - FI-CA Prepaid Account: Change</i>
BAPI	BAPI_CTRACPREPAIDACCOUNT_GETD	<i>BAPI - FI-CA Prepaid Account: Read detailed data</i>
BAPI	BAPI_CTRACDOCUMENT_CREATE	<i>BAPI: FI-CA Post Document</i>
RFC	FKK_PREP_PCARD_STORE	<i>Prepaid: Store Payment Data in DFKK_PCARD</i>
RFC	Event 1421 (function module FKK_SAMPLE_1421)	<i>Parallel Billing Call Settlement</i>
RFC	FKK_BUPA_MAINTAIN_SINGLE	<i>Maintain Business Partner</i>
RFC	/1FE/<billable item class>_BIT_CREATE_API	Generated RFC interfaces for transferring billable items with payment information
Enterprise Service	CashPointPaymentCreateNotification_In	<i>External Cash Point Payment</i>
Web Service	ECC_CASHPOINTPAYMENTCRTNO	<i>External Cash Point Payment</i>
File	Report RFKKPCDS	<i>Payment cards: Settlement</i>
ALE/IDoc	ALE_CTRACDOCUMENT_CREATE	<i>BAPI -> IDoc: ALE_CTRACDOCUMENT_CREATE(FI-CA Post document)</i>

RFC Debugging

⚠ Caution

Disable RFC debugging when you process credit card information in a productive system. Do not activate the *Set RFC Trace* option in your productive system. If this option is active, the system saves all input data of an RFC call in clear text to a file. If credit card numbers (PAN) are included in calls to some function module, then this data would be stored to this file. Since these numbers have to be stored encrypted according to the PCI-DSS standard, activating this option would result in no longer being PCI compliant.

Forward Error Handling (FEH)

⚠ Caution

Disable Forward Error Handling for all services that contain credit card numbers in SAP Customizing.

Card Verification Values (CVV)

⚠ Caution

Do not process asynchronous services that contain a card verification code (CAV2, CID, CVC2, CVV2) or their values.

Note that in SAP services, these values correspond to the GDT `.PaymentCardVerificationValueText`. The reason is that the payload of asynchronous services is persisted in the database until the service is processed and persisting card verification values is not allowed according to PCI-DSS.

Synchronous services can be processed because their payload is not persisted.

Access Logs

You can configure your system so that it logs access to payment card data via Dynpro and Web Dynpro. You make the settings in the SAP Customizing Implementation Guide under ► [Cross-Application Components](#) ► [Payment Cards](#) ► [Basic Settings](#) ► [Make Security Settings for Payment Cards](#) ▾. Choose a security level for which payment card data is to be displayed masked, and set the indicator *Additional authorization check for masked display*.

You can use the `CCSEC_LOG_SHOW` transaction to evaluate access to payment card data. To evaluate the access log, a user requires authorization for activity 71 of authorization object `B_CCSEC`.

For payment card data, you can also use Read Access Logging (RAL), which covers a large number of access channels, such as Remote Function Call and Web services.

13.2.5.2 Settlement Management

13.2.5.2.1 Deletion of Personal Data in Settlement Management

The Settlement Management (LO-AB) application might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ▾.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
Customer Settlement List	<p>See the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under Product Assistance</p> <ul style="list-style-type: none"> ➤ <i>Enterprise Business Applications</i> ➤ <i>Finance</i> ➤ <i>Financial Operations</i> ➤ <i>Settlement Management</i> ➤ <i>Document Categories in Settlement Management</i> ➤ <i>Customer Settlement List</i> ➤ 	<p>ILM object AB_DOCUMENT assigned to archiving object WBU.</p> <p>For more information see the product assistance for SAP S/4HANA on the SAP Help S/4HANA on the SAP Help Portal at Portal at https://help.sap.com/s4hana_op_2020</p> <ul style="list-style-type: none"> ▮ <i>Product Assistance</i> ➤ <i>Enterprise Business Applications</i> ➤ <i>Finance</i> ➤ <i>Financial Operations</i> ➤ <i>Settlement Management</i> ➤ <i>Functions for Document Processing</i> ➤ <i>Archiving of Settlement Management Documents</i> ➤ <i>Customer Settlement Lists (LO-AB)</i> ➤ <p>Report: WLF_UPDATE_AB_EOP_FROM_ARCHIVE</p>
Customer Settlement	<p>https://help.sap.com/s4hana_op_2020</p> <ul style="list-style-type: none"> ▮ <i>Product Assistance</i> ➤ <i>Enterprise Business Applications</i> ➤ <i>Finance</i> ➤ <i>Financial Operations</i> ➤ <i>Settlement Management</i> ➤ <i>For more information see the product assistance for SAP Document Categories in Settlement Management</i> ➤ <i>Customer Settlement</i> ➤ 	<p>ILM object AB_DOCUMENT assigned to archiving object WCI.</p> <p>For more information see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <ul style="list-style-type: none"> ▮ <i>Product Assistance</i> ➤ <i>Enterprise Business Applications</i> ➤ <i>Finance</i> ➤ <i>Financial Operations</i> ➤ <i>Settlement Management</i> ➤ <i>Functions for Document Processing</i> ➤ <i>Archiving of Settlement Management Documents</i> ➤ <i>Customer Settlements (LO-AB)</i> ➤ <p>Report: WLF_UPDATE_AB_EOP_FROM_ARCHIVE</p>

Application Object	Detailed Description	Provided Deletion Functionality
Supplier Billing Document	<p>See the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Document Categories in Settlement Management</i> ▶ <i>Supplier Billing Document</i> ▶</p>	<p>ILM object AB_DOCUMENT assigned to archiving object WLF.</p> <p>For more information see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Functions for Document Processing</i> ▶ <i>Archiving of Settlement Management Documents</i> ▶ <i>Supplier Billing Documents (LO-AB)</i> ▶</p> <p>Report: WLF_UPDATE_AB_EOP_FROM_ARCHIVE .</p>
Settlement Document List	<p>See the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Document Categories in Settlement Management</i> ▶ <i>Settlement Document List</i> ▶</p>	<p>ILM object AB_DOCUMENT assigned to archiving object WRECH.</p> <p>For more information see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Functions for Document Processing</i> ▶ <i>Archiving of Settlement Management Documents</i> ▶ <i>Settlement Document Lists (LO-AB)</i> ▶</p> <p>Report: WLF_UPDATE_AB_EOP_FROM_ARCHIVE .</p>

Application Object	Detailed Description	Provided Deletion Functionality
Supplier Settlement List	<p>See the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Document Categories in Settlement Management</i> ▶ <i>Supplier Settlement List</i> ▶.</p>	<p>ILM object AB_DOCUMENT assigned to archiving object WREG.</p> <p>For more information see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Functions for Document Processing</i> ▶ <i>Archiving of Settlement Management Documents</i> ▶ <i>Supplier Settlement Lists (LO-AB)</i> ▶.</p> <p>Report: WLF_UPDATE_AB_EOP_FROM_ARCHIVE</p>
Expense Settlement	<p>See the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Document Categories in Settlement Management</i> ▶ <i>Expense Settlement</i> ▶.</p>	<p>ILM object AB_DOCUMENT assigned to archiving object WSI.</p> <p>For more information see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Functions for Document Processing</i> ▶ <i>Archiving of Settlement Management Documents</i> ▶ <i>Expense Settlements (LO-AB)</i> ▶.</p> <p>Report: WLF_UPDATE_AB_EOP_FROM_ARCHIVE</p>

Application Object	Detailed Description	Provided Deletion Functionality
Settlement Document	<p>See the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Document Categories in Settlement Management</i> ▶ <i>Settlement Document</i> ▶</p>	<p>ILM object AB_DOCUMENT assigned to archiving object WZR.</p> <p>For more information see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Functions for Document Processing</i> ▶ <i>Archiving of Settlement Management Documents</i> ▶ <i>Settlement Documents (LO-AB)</i> ▶</p> <p>Report: WLF_UPDATE_AB_EOP_FROM_ARCHIVE .</p>
Condition Contract	<p>See the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020</p> <p>▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Finance</i> ▶ <i>Financial Operations</i> ▶ <i>Settlement Management</i> ▶ <i>Condition Contract Management</i> ▶ <i>Condition Contract</i> ▶</p>	<p>ILM object WCB_COCO assigned to archiving object WCB_COCO.</p> <p>Report: WCB_UPDATE_EOP_FROM_ARCHIVE.</p>

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Settlement Management (LO-AB)	End of purpose (EoP) check	SAP delivers an end of purpose check for Settlement Management (LO-AB). All applications register either an end of purpose (EoP) check in the Customizing settings for the blocking and deletion of business partner data or a where-used check (WUC). For information about the Customizing of blocking and deletion for LO-AB, see <i>Configuration: Simplified Blocking and Deletion</i> .

Configuration: Simplified Blocking and Deletion

You configure the settings the related to the blocking and deletion of customer and supplier master data in Customizing for *Logistics - General* under ► *Business Partner* ► *Deletion of Customer and Supplier Master Data*. ►

13.2.5.2.2 Certificate-Based Authentication with SAP Commissions

In the SAP S/4HANA Personnel Settlement integration with SAP Commissions, communication is triggered based on an OData call over http, based on an RFC connection of type **G**. Basic authentication is used. The communication channel between SAP S/4HANA Utilities and SAP Commissions is secured by HTTPS SSL encryption.

To establish secure communication, you must obtain the server certificate from the SAP Commissions server instance and then use the Trust Manager (transaction STRUST) to import it into the SAP S/4HANA system.

13.2.6 Billing and Revenue Innovation Management

13.2.6.1 Convergent Invoicing, Receivables Mngmt and Payment Handling

The following section provides an overview of the security-relevant information that applies to Convergent Invoicing and Receivable Management and Payment Handling as part of Contract Accounts Receivable and Payable (FI-CA).

13.2.6.1.1 Data Storage Security

Contract Accounts Receivable and Payable (FI-CA) saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following list shows the logical file names and paths used by Contract Accounts Receivable and Payable (FI-CA) and for which programs these file names and paths apply:

Logical File Names Used in FI-CA and Logical Path Names

The following logical file names have been created in order to enable the validation of physical file names:

Program	Logical File Name Used by the Program	Logical Path Name Used by the Program
RFKIBI_FILE00	FICA_DATA_TRANSFER_DIR	FICA_DATA_TRANSFER_DIR
RFKIBI_FILEP01		
RFKKBI_FILEEDIT		
RFKKBIBG		
RFKKZEDG		
RFKKRLDG		
RFKKCMDG		
RFKKCRDG		
RFKKAVDG		
RFKKBIB0		

RFKKZE00		
RFKKRL00		
RFKKCM00		
RFKKCR00		
RFKKAV00		
RFKKKA00		
RFKKBIT0		
RFKKPCSF	FI-CA-CARD-DATA-S	FI-CA-CARD-DATA-S
RFKKPCDS		
RFKKCVSPAY	FI-CA-CVS	FI-CA-CVS
RFKK_CVSPAY_CONFIRM		
RFKKCVSCONFIRMDB		
RFKK_CVSPAY_CONFIRM_TEST		
RFKK_DOC_EXTR_EXP	FI-CA-DOC-EXTRACT-DIR	FI-CA-DOC-EXTRACT-DIR
RFKK_DOC_EXTR_AEXP		
RFKK_DOC_EXTR_IMP		
RFKK_DOC_EXTR_EXTR		
RFKK_DOC_EXTR		
RFKK_DOC_EXTR_DEL		
Class CL_FKK_TEXT_FILE		
RFKKBIXBITUPLOAD	FI-CA-BI-SAMPLE FI-CA-BI-SAMPLE-DIR	FI-CA-BI-SAMPLE-DIR
RFKKCOL2	FI-CA-COL-SUB	FI-CA-COL-SUB
RFKKCOLL		
Transaction FP03DM (Mass Activity)		
Transaction FPCI (Mass Activity)	FI-CA-COL-INFO	FI-CA-COL-INFO
RFKKCOPM	FI-CA-COL-READ	FI-CA-COL-READ

READFILE		
RFKKCOPG	FI-CA-COL-TEST	FI-CA-COL-TEST
RFKKRDI_REPORT	FI-CA-RDI	FI-CA-RDI
RFKKRDI_REPORT_DIS		
SAPFKPY3	FI-CA-DTA-NAME	FI-CA-DTA-NAME
RFKKCHK01	FI-CA-CHECKS-EXTRACT	FI-CA-CHECKS-EXTRACT
Class CL_FKK_INFCO_SEND	FI-CA-INFCO	FI-CA-INFCO
RFKKBE_SAL1	FICA_BE_SAL	FICA_BE_SAL
RFKKBE_SAL2	FICA_BE_SAL_XML	FICA_BE_SAL_XML
RFKK1099	FI-CA-1099	FI-CA-1099
RFKKOP03	FICA_OPEN_ITEMS	FICA_OPEN_ITEMS
RFKKOP04		
RFKKOP07		
RFKKES_SAL1	FICA_TAX_REP_GEN	FICA_TAX_REP_GEN
RFKKES_SAL2		
RFKKRDI_REPORT	FI-CA-RDI	FI-CA-RDI
RFKKRDI_REPORT_DIS		
Transaction EMIGALL	ISMW_FILE	ISMW_ROOT

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information about data storage security, see the chapter in the ABAP Platform Security Guide.

13.2.6.1.2 Data Protection

Contract Accounts Receivable and Payable (FI-CA) processes personal data of business partners that might be subject to data protection legislation applicable in some countries.

Contract Accounts Receivable and Payable (FI-CA) uses SAP ILM to support the deletion of this personal data. SAP delivers an end of purpose check for Contract Accounts Receivable and Payable (FI-CA). You register the end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the SAP Business Partner.

Display of Blocked Data

Only if a user has special authorization, is it possible to display blocked business partner master data. However, it is still not possible to create, change, copy, or perform follow-up activities on this blocked business partner data.

However, FI-CA-specific data relating to a blocked business partner (as for example the contract account) users can display without having special authorization.

For more information on the blocking and deletion of personal data, on the end of purpose check and on displaying blocked data in Contract Accounts Receivable and Payable, see the Product Assistance of Contract Accounts Receivable and Payable under [▶ Basic Functions ▶ SAP Business Partner ▶ Blocking and Deleting Personal Data ▶](#).

Process Flow

Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM). You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available. You do the following:

1. Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA).
2. Run transaction FPDPR_BP_INIT once for existing business partners for which you want to execute the end of purpose checks. New business partners you create are automatically included in the end of purpose checks.
3. Run transaction FPDPR1 to prepare the end of purpose check of the central business partner. The function module MKK_BUPA_EOP_CHECK saved for Contract Accounts Receivable and Payable (FI-CA) in table BUTEOPFM provides the EoP check result obtained by transaction FPDPR1 to transaction BUPA_PRE_EOP.
4. Run transaction BUPA_PRE_EOP to enable the end of purpose check function for the central business partner.

Business users can request unblocking of blocked data by using the transaction BUP_REQ_UNBLK.

If you have the needed authorizations, you can unblock data by running the transaction BUPA_PRE_EOP.

You delete data by using the transaction ILM_DESTRUCTION for the ILM objects of Contract Accounts Receivable and Payable (FI-CA).

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for Cross-Application Components under [Data Protection](#).

Define the settings for authorization management under [Authorization Management](#). For more information, see the Customizing documentation.

Define the settings for blocking under *Blocking and Unblocking Business Partner*. For more information, see the Customizing documentation.

You configure the settings specific for Contract Accounts Receivable and Payable in the Customizing for Contract Accounts Receivable and Payable under ► *Technical Settings* ► *Data Protection* ▾ and *Data Deletion*. For more information, see the Customizing documentation.

13.2.6.1.3 Payment Card Security According to PCI-DSS

i Note

The **Payment Card Industry Data Security Standard (PCI-DSS)** was jointly developed by major credit card companies in order to create a set of common industry security requirements for the protection of cardholder data. Compliance with this standard is relevant for companies processing credit card data. For more information, see <http://www.pcisecuritystandards.org> .

The following sections of the security guide support you in implementing payment card security aspects and outline steps that need to be considered to be compliant with the PCI-DSS.

Please note that the PCI-DSS covers more than the steps and considerations given here. Complying with the PCI-DSS lies completely within the customer's responsibility, and we cannot guarantee the customer's compliance with the PCI-DSS.

For current information about PCI-DSS in general, see SAP Note [1609917](#) .

Contract Accounts Receivable and Payable (FI-CA) processes all payment transactions with your business partners. For this purpose, Contract Accounts Receivable and Payable also processes credit card data. For processing credit card transactions, Contract Accounts Receivable and Payable follows the rules laid down by the Payment Card Industry Data Security Standard.

Credit card data arrives in Contract Accounts Receivable in the following ways:

- You receive documents, which already contain credit card data in their supplements, by means of the IDoc interface or by means of BAPIs.
- You receive payments that already contain credit card data with the payment lot transfer program (RFKKZE00).
- External payment collectors and external cash desk services transfer credit card data using enterprise services with the payment to Contract Accounts Receivable and Payable.
- Financial Customer Care transfers credit card data for documents from SAP Customer Relationship Management using RFC.
- Customers or your employees add credit card data as follows:
 - Employees enter credit card data in the master records of business partners and prepaid accounts.
 - Employees enter payment card data in the *Maintain Bank Data* (FPP4) transaction.
 - Employees enter credit card data for payments in the cash desk, in the cash journal, in payment specifications and in promises to pay.
 - Customers enter credit card data online in SAP Biller Direct. SAP Biller Direct transfers the data to Contract Accounts Receivable and Payable.
- You adopt billable items with payment information using the generated RFC interfaces /1FE/<billable item class>_BIT_CREATE_API.

The program for payment (such as the payment run or the cash desk) generates payment documents with supplements containing the credit card data. Contract Accounts Receivable and Payable transfers this credit card data to the payment card company or the clearing house using transaction `FPPCDS` (creation of file) or `FPCS` (online transfer).

Contract Accounts Receivable and Payable stores the data as follows:

Object	Table(s)
Business Partner Master Record	BUT0CC CCARD
Payments in Payment Lot or Credit Card Lot	DFKKZP
Document	DFKKOPC DFKKOPKC DFKK_PCARD
Payment Data for a Payment Run	DPAYH
Payment Data for a Payment Using SAP Biller Direct or Financial Customer Care	DFKKOPC
Payment Specifications	DFKKIP_GRP
Promises to pay	DFKKPPD_PAY
Master Record of Prepaid Account	FKKPREPACC
Billable Items	Generated tables: <ul style="list-style-type: none"> • /1FE/0<billable item class>0PY • /1FE/0<billable item class>1PY

You must restrict the display of the necessary objects by assigning authorizations, while at the same time ensuring that this authorization protection cannot be circumvented by database programs or customer-specific ABAP reports.

You can also make additional security settings for payment card data. For more information, see SAP Note [1032588](#) and the SAP S/4HANA Security Guide, section "Payment Card Security".

Archiving

Only masked credit card information can be archived. Clear text credit card information should not be archived. Archiving encrypted credit card information is problematic because archived data should not be changed. Encrypted credit card information has to be re-encrypted with a different key, for example, with key rotation, as required by PCI-DSS. This change of data is not possible in an archive.

In technologies that are agnostic to the semantics of the data, such as Process Integration (PI), ABAP Web Services, or Forward Error Handling (FEH), archiving has to be disabled. IDocs that contain credit card information should not be archived.

Interfaces (IDoc/Services)

⚠ Caution

According to PCI-DSS, IDoc segments are not allowed to store payment card numbers in clear text. However, during processing of an IDoc in the IDoc Framework, all values are stored temporarily, including the clear text credit card number.

For more information about how to process customer-specific IDocs containing credit card information, go to https://help.sap.com/s4hana_op_2020, enter *Handling Sensitive Data in IDocs* into the search bar, press , and open the search result with that title.

If you exchange data between systems using IDoc messages, and this data contains unencrypted credit card information, you have to implement access restrictions and a deletion concept at the level of the file system.

Contract Accounts Receivable and Payable processes payment card data in the following interfaces:

Type of Interface	Technical Name	Description
BAPI	BAPI_CTRACPREPAIDACCOUNT_CREA	<i>BAPI - FI-CA Prepaid Account: Create</i>
BAPI	BAPI_CTRACPREPAIDACCOUNT_CHNG	<i>BAPI - FI-CA Prepaid Account: Change</i>
BAPI	BAPI_CTRACPREPAIDACCOUNT_GETD	<i>BAPI - FI-CA Prepaid Account: Read detailed data</i>
BAPI	BAPI_CTRACDOCUMENT_CREATE	<i>BAPI: FI-CA Post Document</i>
RFC	FKK_PREP_PCARD_STORE	<i>Prepaid: Store Payment Data in DFKK_PCARD</i>
RFC	Event 1421 (function module FKK_SAMPLE_1421)	<i>Parallel Billing Call Settlement</i>
RFC	FKK_BUPA_MAINTAIN_SINGLE	<i>Maintain Business Partner</i>
RFC	/1FE/<billable item class>_BIT_CREATE_API	Generated RFC interfaces for transferring billable items with payment information
Enterprise Service	CashPointPaymentCreateNotification_In	<i>External Cash Point Payment</i>
Web Service	ECC_CASHPOINTPAYMENTCRTNO	<i>External Cash Point Payment</i>
File	Report RFKKPCDS	<i>Payment cards: Settlement</i>
ALE/IDoc	ALE_CTRACDOCUMENT_CREATE	<i>BAPI -> IDoc: ALE_CTRACDOCUMENT_CREATE(FI-CA Post document)</i>

RFC Debugging

⚠ Caution

Disable RFC debugging when you process credit card information in a productive system. Do not activate the *Set RFC Trace* option in your productive system. If this option is active, the system saves all input data of an RFC call in clear text to a file. If credit card numbers (PAN) are included in calls to some function module, then this data would be stored to this file. Since these numbers have to be stored encrypted according to the PCI-DSS standard, activating this option would result in no longer being PCI compliant.

Forward Error Handling (FEH)

⚠ Caution

Disable Forward Error Handling for all services that contain credit card numbers in SAP Customizing.

Card Verification Values (CVV)

⚠ Caution

Do not process asynchronous services that contain a card verification code (CAV2, CID, CVC2, CVV2) or their values.

Note that in SAP services, these values correspond to the GDT `.PaymentCardVerificationValueText`. The reason is that the payload of asynchronous services is persisted in the database until the service is processed and persisting card verification values is not allowed according to PCI-DSS.

Synchronous services can be processed because their payload is not persisted.

Access Logs

You can configure your system so that it logs access to payment card data via Dynpro and Web Dynpro. You make the settings in the SAP Customizing Implementation Guide under [▶ Cross-Application Components ▶ Payment Cards ▶ Basic Settings ▶ Make Security Settings for Payment Cards](#). Choose a security level for which payment card data is to be displayed masked, and set the indicator *Additional authorization check for masked display*.

You can use the `CCSEC_LOG_SHOW` transaction to evaluate access to payment card data. To evaluate the access log, a user requires authorization for activity 71 of authorization object `B_CCSEC`.

For payment card data, you can also use Read Access Logging (RAL), which covers a large number of access channels, such as Remote Function Call and Web services.

13.2.7 Real Estate Management

13.2.7.1 Real Estate Management

Authorizations

Standard Roles of Real Estate Management

Role	Description
SAP_RE_APPL	Real Estate Management (including administration and Customizing)
SAP_EP_RW_REFX_I	AC - Flexible Real Estate Management
SAP_EP_RW_REFX_II	AC - Flexible Real Estate Management - support processes

Network and Communication Security

External heating expenses settlement is available in Real Estate Management. To make this settlement possible, the necessary files must be generated in the SAP system in an internal SAP format. You then need to send the data medium to the settlement company.

Trace and Log Files

The change documents provide information on changes to the authorization group and to the person responsible for the object.

Data Storage Security

Using Logical Paths and File Names to Protect Access to the File System

Flexible Real Estate Management (RE-FX) saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths that are used by Flexible Real Estate Management (RE-FX), and for which programs these file names and paths apply:

Logical File Names Used in Flexible Real Estate Management (RE-FX)

The logical file name `REFX_CREATE_TAPE` makes it possible to validate physical file names in Flexible Real Estate Management (RE-FX). The following programs use this logical file name:

- RFRESCMLTAPE
- RFRESCMLTAPECO
- RFRESCSETTLE
- RFRESCSETTLESC
- RFRESCCONTINUE
- RFRESCBOOKING
- RFRESCSETTLCO
- RFRESCCONTINUECO
- RFRESCPOSTCO

Logical Path Names Used in Flexible Real Estate Management (RE-FX)

The logical file names of Flexible Real Estate Management (RE-FX) listed above all use the logical file path `REFX_ROOT`.

Activating the Validation of Logical Path and File Names

The logical paths and file names are entered in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

13.2.7.2 Deletion of Personal Data in RE-FX

Use

The Flexible Real Estate Management (RE-FX) component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 **► Product Assistance ► Cross Components ► Data Protection ►**.

Relevant Archiving Objects

Archiving Object	Technical Name
Architectural Object	REFX_AO
Adjustment Measure	REFX_AT
Business Entity	REFX_BE

Archiving Object	Technical Name
Buildings	REFX_BU
Comparative Group of Apartments	REFX_CG
Real Estate Contract	REFX_CN
Cash Flow of Contracts	REFX_CNCF
Joint Liability	REFX_JL
Land Register	REFX_LR
RE: Move Planning	REFX_MP
Notice of Assessment	REFX_NA
Contract Offer	REFX_OF
Offered Object	REFX_OO
Option Rate Determination per Object/Subobject	REFX_OR
Other Public Register	REFX_PE
Participation Group	REFX_PG
Parcel of Land	REFX_PL
Property	REFX_PR
RE Document	REFX_RADOC
Parcel Update	REFX_RC
Rental Object	REFX_RO
Cash Flow of Rental Objects	REFX_ROCF
RE Search Request	REFX_RR
Reservation	REFX_RS
Recurring Reservation	REFX_RSREC
Service Charge Settlement	REFX_SCSE
Settlement Unit	REFX_SU
Correction Object	REFX_TC

Available Check

Implemented Solution: End of Purpose (EoP) check

For more information, see SAP Note [2134204](#).

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of `business partner master data` in `Customizing for Cross-Application Components` under `Data Protection`.

13.2.7.3 Deletion of Personal Legacy Data After Migration from Classic Real Estate Management

You might still have legacy data from the classic SAP ERP component *Real Estate Management* (RE) that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. You can use SAP ILM to support the deletion of personal data as described in the following sections.

Relevant Application Objects in Real Estate Management (RE) and Available Deletion Functionality

The following ILM objects enhance archiving objects with the information for data retention.

Application Object	Deletion Functionality: ILM Object	SAP Note
Application	RE_REQUEST	2578654 2582007
Buildings	RE_BUILDING	2553910 2571648
Business Entity	RE_BUSN_EN	2553219 2550341
Land Register	RE_LANDREG	2536591

Application Object	Deletion Functionality: ILM Object	SAP Note
Lease-Out Flows	RE_FLOW_DT	2582005
		2578652
Management Contract	RE_MGT_CNT	2555859
		2574929
Offer	RE_OFFER	2580858
		2578653
Property	RE_PROPERTY	2562465
		2570217
Real Estate General Contract	RE_GNRL_CN	2522322
Rental Agreement	RE_RNTL_AG	2582008
		2575665
Rental Request	RE_RNTL_RQ	2602104
Rental Unit	RE_RNTL_UN	2580857
		2574745
Service Charge Settlement	RE_SC_SE	2572928
Settlement Unit	RE_STLM_UN	2578655
		2582010

Process Flow

- Before archiving data, you must define residence times and retention periods in SAP Information Lifecycle Management (ILM) by doing the following:
 - Run transaction `IRMPOL` and maintain the required residence and retention policies for the Real Estate Business Partner (ILM object: `TRTM_BPAR`).
 - Run transaction `IRMPOL` and define the required retention policies for the ILM objects of *Real Estate Management* (RE).
 - You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
- To determine which business partners have reached end of purpose and can be archived, you do the following:
 - Run transaction `SARA` and call up archiving object `TRTM_BPAR`.

- Specify the Real Estate Business Partner you want to archive in the write variant of the archiving object. Before archiving, the write program checks whether business partner data is still used by the relevant objects in *Real Estate Management* (RE).
 - If the business partner data is no longer used in ongoing business activities, i.e. all related Real Estate objects were either archived or the assignment of the business partner to the relevant Real Estate object was removed, the business partner is archived and thus blocked in the system. Only users with special authorizations can then access the archived data.
3. To delete personal data, you do the following:
- Run transaction IRMPOL for the ILM objects of *Real Estate Management* (RE).
 - Run transaction IRMPOL for ILM object TRTM_BPAR.

More Information

- For more information about the ILM enablement of the Real Estate Business Partner, see SAP Note [2590872](#)
- For more information about the ILM objects used in *Real Estate Management* (RE), see SAP Library at https://help.sap.com/viewer/p/SAP_ERP under ► *SAP ERP Central Component* ► *Financials* ► *Real Estate (RE)* ► *Real Estate Management Archiving* .

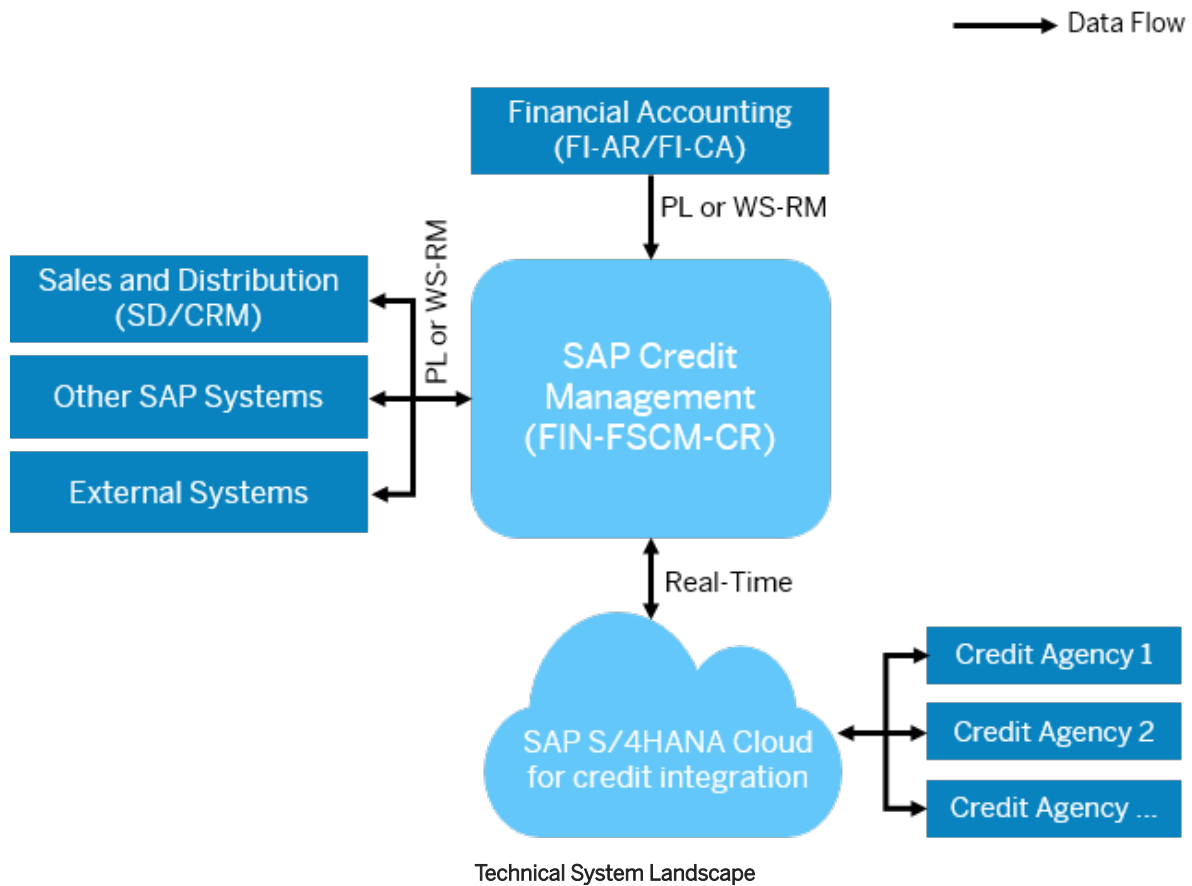
13.2.8 Receivables Management

13.2.8.1 SAP Credit Management

13.2.8.1.1 Technical System Landscape

Use

This figure shows an overview of the technical system landscape for *SAP Credit Management*.



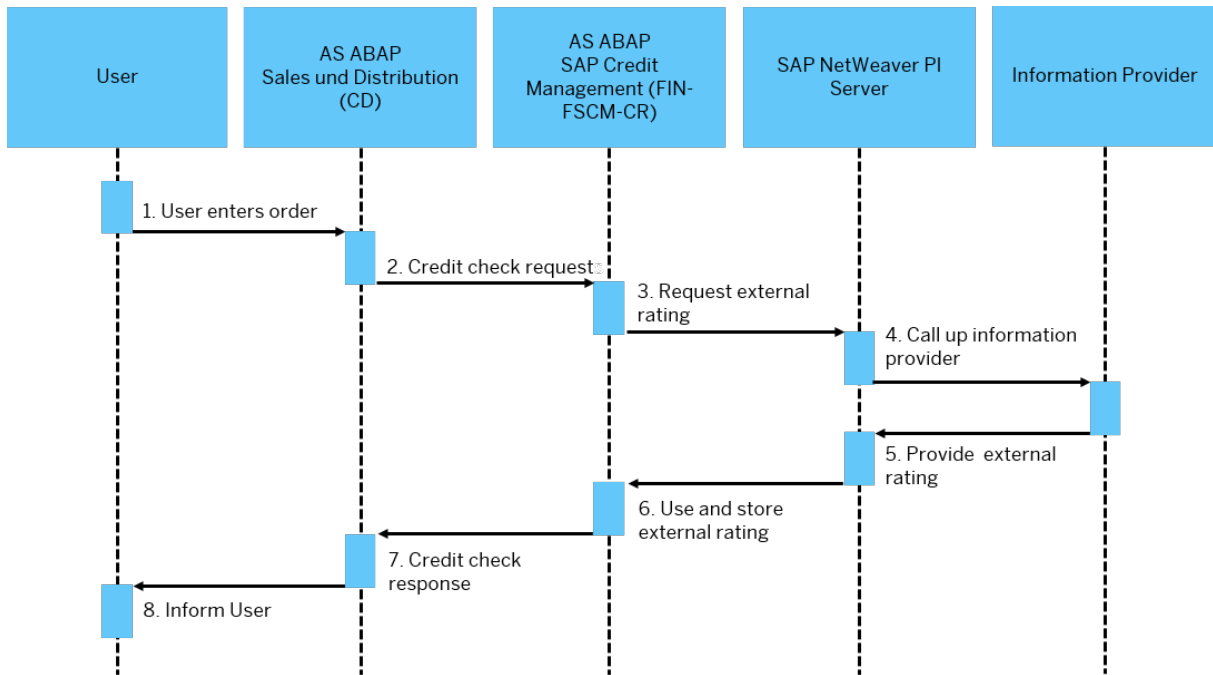
To exchange messages with external information providers, you have to use the Integration Server. For accounting systems as well as Sales and Distribution (SD) systems, you can configure the communication either via the Integration Server or via a point to point connection using Web Services Reliable Messaging (WSRM). The SAP Business Information Warehouse is connected via Remote Function Call (RFC).

For more information about recommended security zone settings, see *ABAP Platform Security Guide*.

For *SAP Credit Management* the business package for the Credit Manager provides you with portal content so that you can use the functions from *SAP Credit Management* in the portal. Security-relevant information about the use of the portal content is available in the *ABAP Platform Security Guide* for the usage types Enterprise Portal Core (EPC) and SAP Enterprise Portal (EP) in the portal security guide.

13.2.8.1.2 Security Aspects of Data, Data Flow, and Processes

This figure shows an example of a data flow for the *SAP Credit Management* application.



This table shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	User enters order	User types: dialog or internet user
2	Credit check request	Communication protocol HTTPS or HTTP
3	Request external rating	Communication protocol HTTPS or HTTP
4	Call up information provider	Communication protocol HTTPS or HTTP
5	Provide external rating	Not applicable
6	Use and store external rating	Not applicable
7	Credit check response	Communication protocol HTTPS or HTTP
8	Inform user	Not applicable

13.2.8.1.3 User Management

Standard Users

This table shows the standard users that are necessary for operating *SAP Credit Management*.

System	User ID	Type	Password	Description
<i>SAP Credit Management</i> , client systems	For example, CREDITXUSER	Communication user	You specify the initial password during the installation. The user ID and password are stored in the XI channel for the connection.	This is required for communication between <i>SAP Credit Management</i> and client systems using the XI channel.

You need to create this user before XI configuration. Assign both roles `SAP_FIN_FSCM_CR_USER` and `SAP_XI_IS_SERV_USER` to the user. The user and password are added to the XI channel logon data that you create when you configure your exchange server.

13.2.8.1.4 Authorizations

Defining Authorizations

You can control the right of access to SAP Credit Management data by assigning authorizations – separately by credit segment and activity – to the authorization object `F_UKM_SGMT`. The fields of this authorization object are:

- You can restrict the access to credit segment-independent master data of SAP Credit Management (for example, the score) by using the authorization object for business partner roles (`B_BUPA_RLT`) with the role Business Partner Credit Management (`UKM000`).
- You can restrict the access to logs (application logs) of *SAP Credit Management* using the authorization object `S_APPL_LOG`.

For SAP Credit Management, the following forms are relevant for object name and subobject:

Object Name	Subobject	Meaning
FIN-FSCM-CR	BW-SCORING	Transfer of score from BW
FIN-FSCM-CR	COMMITMENT	Credit exposure update
FIN-FSCM-CR	CREDITCHECK	Credit check

Object Name	Subobject	Meaning
FIN-FSCM-CR	MONITOR	Update entries for external credit information
FIN-FSCM-CR	SEARCH_ID	Search ID at credit information provider
FIN-FSCM-CR	REPLICATE	Replicate FI-CA score
FIN-FSCM-CR	EVENTING	Log of events occurred
FIN-FSCM-CR-MASS	ERROR	Logs of mass changes, can be differentiated by the severity of the error
	ERROR_BIG	
	ERROR_PROG	
	ERROR_UPD	
	INFO	
	STATISTICS	
	SUCCESS	
	WARNING	

Integration with Sales and Distribution

Business scenario:

A sales representative carries out a credit check. The credit check fails. In the background, a documented credit decision is automatically created in SAP Credit Management.

Authorization Concept:

- **One System Scenario:**

The sales representative doesn't need any authorizations in SAP Credit Management.

The documented credit decision is created by the workflow user `SAP_WFRT`. To this user, you must assign a copy of the business role `SAP_FIN_CR_DCD_WF`. This business role includes all necessary authorizations for creating documented credit decisions in SAP Credit Management.

- **Multiple System Scenario:**

You need to configure the web service

`DocumentedCreditDecisionERPBusinessTransactionDocumentNotification_In`.

To the sales representative carrying out the credit check, you must assign all authorizations necessary for creating a documented credit decision. To this sales representative, you must assign a copy of the business role `SAP_FIN_CR_DCD_WF`. This business role includes all necessary authorizations for creating documented credit decisions in SAP Credit Management.

13.2.8.1.5 Communication Destinations

Use

This table shows an overview of the communication destinations (RFC) used by *SAP Credit Management*.

Connection Destinations when Using the Integration Server

Destination	Delivered	User, Authorizations
INTEGRATION_SERVER	No	XIAPPLUSER Role SAP_XI_APPL_SERV_USER
LCRSAPRFC	No	
SAPSLDAPI	No	

These destinations are not application-specific but they are required for the operation of SAP Process Integration.

For point to point connections via Web Services Reliable Messaging (WSRM), you use the SOA Manager in both systems to create the logical port and the endpoint.

13.2.8.1.6 Data Storage Security

Use

Master and transaction data of *SAP Credit Management* are saved in the database of the SAP system in which *SAP Credit Management* is installed. They are not distributed to connected systems via XI, however they can be optionally extracted to SAP Business Information Warehouse.

Access to this data is restricted through the authorizations for authorization object F_UKM_SGMT. Authorizations for this authorization object are provided for role SAP_FIN_FSCM_CR_USER in the standard delivery; you can copy the role and adapt it as required. For more information about authorization object F_UKM_SGMT, see the configuration guide of *SAP Credit Management*.

Access to data on natural persons in particular is subject to data protection requirements and must be restricted by assigning authorizations.

13.2.8.1.7 Security-Relevant Logging and Tracing

Use

All changes to the master data of *SAP Credit Management* are recorded as change documents in the business partner record. Changes automatically executed by the system as a follow-on process to an event appear under the name of the communication user if the event was triggered by an XI message.

Example

A credit check is initiated by SD; the system detects that the validity date of the credit limit has expired and determines a new credit limit on the basis of the Customizing settings.

13.2.8.2 SAP Dispute Management

13.2.8.2.1 Technical System Landscape

Use

You can use *SAP Dispute Management* in a **one-system scenario** or in a **multiple-system scenario**. If you use *SAP Dispute Management* in a one-system scenario, this means that you use *SAP Dispute Management* in the same system as *Accounts Receivable*. In a multiple-system scenario, you run *SAP Dispute Management* in a separate system. This communicates with the Accounts Receivable system connected by means of synchronous and asynchronous BAPI calls and dialog calls.

The figure below shows an overview of the technical system landscape for *SAP Dispute Management* in a one-system scenario.



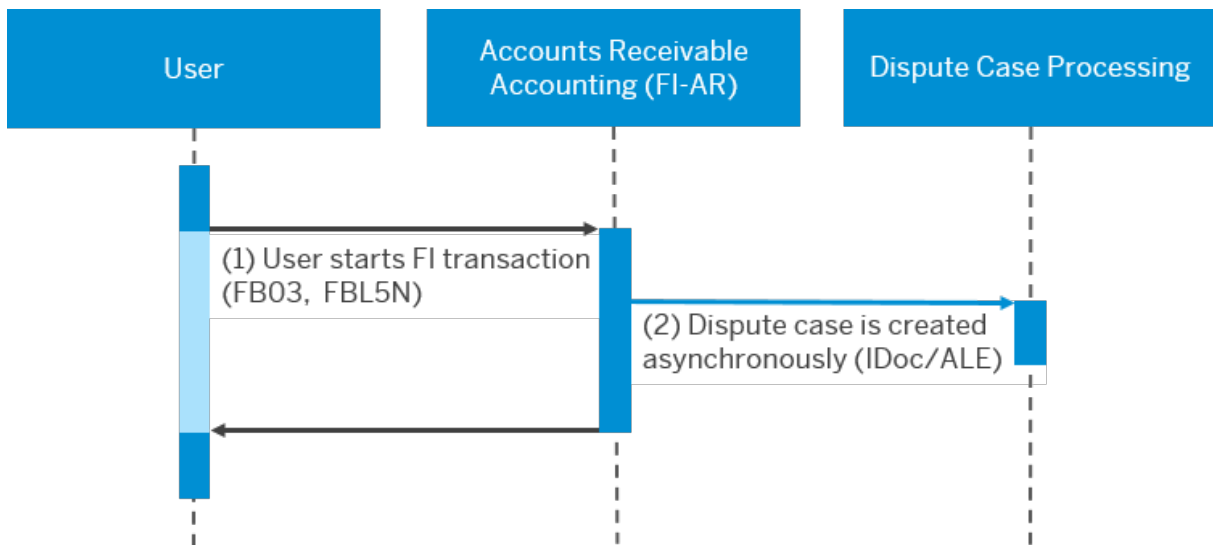
The figure below shows an overview of the technical system landscape for *SAP Dispute Management* in a multiple-system scenario.



For *SAP Dispute Management*, with *Business Package for Dispute Manager* you can also use portal content to use the functions of *SAP Dispute Management* in the portal. For security-relevant information about using the portal content, see the *ABAP Platform Security Guide* for the usage types Enterprise Portal Core (EPC) and Enterprise Portal (EP) in the Portal security guide.

13.2.8.2.2 Security Aspects of Data, Data Flow, and Processes

The figure below shows an example of the data flow that occurs when you create a dispute case in a multiple-system scenario:



The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	User starts FI transaction (for example, FB03 for document display or FBL5N for line item list)	User type: Dialog user
2	Dispute case is created asynchronously (IDoc/ALE)	User type: Technical user or, when the Trusted/Trusting connection is used, dialog user (see also User Administration [page 163])

As already mentioned under [Technical System Landscape \[page 161\]](#), *SAP Dispute Management* uses BAPI calls (IDocs) asynchronously for the data flow between the Accounts Receivable system and the Dispute Case Processing system. The following IDocs are affected:

- Sending system: Accounts Receivable Accounting, receiving system: Dispute Case Processing
 - [AttributesChange](#)
 - [Create](#)
 - [Process](#)
- Sending system: Dispute Case Processing, receiving system: Accounts Receivable Accounting
 - [AttributeSynchronize](#)
 - [StatusChanged](#)
 - [WriteOff](#)

If you are using *SAP Dispute Management* in a one-system scenario, synchronous BAPI calls are used instead.

13.2.8.2.3 User Management

User Administration Tools

The table below shows the user management tools for *SAP DisputeManagement*.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance with AS ABAP (transactions SU01 and PFCG)	For more information, see User and Role Administration of Application Server ABAP in the ABAP Platform documentation.	

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that users who perform their tasks interactively have to change their passwords on a regular basis, but not those users who perform their tasks using background processing.

The user types that are required for *SAP Dispute Management* include:

- Individual users:
 - For each individual user in your system, you need dialog users for the following purposes:
 - To use the system via [SAP GUI for Windows](#)
 - If you use [SAPDisputeManagement](#) in a multiple system scenario and the RFC destinations used use a Trusted/Trusting system relationship, calls to the other system are performed using the current user from the calling system. Therefore, for each user a valid user must also exist in the target system.

- Technical users:
 - Background users can be used for processing in the background.
 - If you use *SAPDisputeManagement* in a multiple system scenario and the RFC destinations concerned are configured such that they do **not** use a Trusted/Trusting system relationship, you need the following technical users for the RFC destinations:
 - Communication users are used for synchronous and asynchronous BAPI calls (IDocs).
 - Dialog users are used for dialog calls that take place remotely in the other system.

For more information about these user types, see under User Types in the Security Guide for *AS ABAP*.

Standard Users

If you use *SAP Dispute Management* in a multiple system scenario and there is **no** Trusted/Trusting system relationship between the systems involved, you have to configure corresponding users for the RFC communication between the systems involved.

Note that in *SAP Dispute Management*, asynchronous BAPI calls, synchronous BAPI calls, and dialog calls take place between the systems involved. There are calls from the Dispute Case Processing system to the system for Accounts Receivable Accounting and vice versa.

The table below shows the users required if you use *SAP Dispute Management* in a multiple system scenario and there is **no** Trusted/Trusting system relationship between the systems involved.

Standard Users

System	User ID	Type	Password	Description
System for Dispute Case Processing	Example: ALERE-MOTE1_COM	Communication users	The user ID and password are stored in the RFC destination for the connection.	These users are used when synchronous or asynchronous BAPI methods are called from the Accounts Receivable system in the Dispute Case Processing system.
System for Dispute Case Processing	Example: ALERE-MOTE1_DIA	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Accounts Receivable Accounting system in the Dispute Case Processing system.

System	User ID	Type	Password	Description
Accounts Receivable Accounting system	Example: ALERE-MOTE2_COM	Communication users	The user ID and password are stored in the RFC destination for the connection.	These users are used when synchronous or asynchronous BAPI methods are called from the Dispute Case Processing system in the Accounts Receivable system.
Accounts Receivable Accounting system	Example:ALERE-MOTE2_DIA	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Dispute Case Processing system in the Accounts Receivable Accounting system.

Create the users and enter them in the corresponding RFC destinations. You can assign user IDs as required. The user IDs above are merely examples.

13.2.8.2.4 Communication Destinations

Use

The following table shows an overview of the communication destinations (RFC) that you need for *SAP Dispute Management* if you use it in a multiple-system scenario. You can use these communication destinations to establish communication between the Financial Accounting system and the Dispute Case Processing system.

You can assign names for your RFC destinations as required. The names of the RFC destinations that are specified in the table are merely examples. The destinations are not delivered in the standard system; you need to create them yourself.

Destination	Description	User, Authorizations
Example: DM2FIN_DIAG	This destination is used for dialog calls that take place from the Dispute Case Processing system to the Accounts Receivable system by means of RFC.	<p>RFC user (dialog) in Accounts Receivable</p> <p>Role: SAP_FIN_FSCM_DM_AR_RFC_DIALOG</p> <p>Contains the authorizations required by a user to call SAP Dispute Management dialog methods using RFC from the Dispute Case Processing system in the Accounts Receivable system.</p> <p>Examples of such methods are including open items in a dispute case and navigating from a dispute case to a linked line item.</p>
Example: DM2FIN_COMM	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Dispute Case Processing system to the Accounts Receivable system.	<p>RFC user (communication) in Accounts Receivable</p> <p>Role: SAP_FIN_FSCM_DM_AR_RFC_COMM</p> <p>Contains the authorizations required by a user to call synchronous and asynchronous SAP Dispute Management BAPI methods from the Dispute Case Processing system in the Accounts Receivable system.</p> <p>Examples of such methods are the automatic write off of dispute cases and automatic notification of Accounts Receivable when confirming and voiding cases.</p>
Example: FIN2DM_DIAG	This destination is used for dialog calls that take place from the Accounts Receivable system to the Dispute Case Processing system by means of RFC.	<p>RFC user (dialog) in Dispute Case Processing</p> <p>Role: SAP_FIN_FSCM_DM_RFC_DIALOG</p> <p>Contains the authorizations for a user with which the DISPLAY method is called in the Dispute Case Processing system from the Accounts Receivable system by RFC. The role contains the authorizations necessary for displaying the dispute case.</p>

Destination	Description	User, Authorizations
Example: FIN2COL_COMM	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Accounts Receivable system to the Dispute Case Processing system.	<p>RFC user (communication) in Dispute Case Processing</p> <p>Role: SAP_FIN_FSCM_DM_RFC_COMM</p> <p>Contains the authorizations required by a user to call synchronous and asynchronous BAPI methods from the Accounts Receivable system in the Dispute Case Processing system.</p> <p>Examples of such methods are creating dispute cases from Accounts Receivable and automatically changing dispute cases using clearing transactions in Accounts Receivable.</p>

Set up RFC destinations for the ALE scenario

When you set up the RFC destinations for the ALE scenario, check whether the option of trusted/trusting system relationship is relevant for you. Using an RFC trusted/trusting system relationship between two SAP systems means that in the case of an RFC (Remote Function Call) from the trusted to the trusting system, **no** password is sent for the logon to the trusting system. You can configure the RFC destinations in such a way that the call in the target system occurs with the current user from the calling system without a password being specified or entered on the logon screen. This has the following advantages, for example:

- When changes to objects or data are logged in the called system, this logging takes place with the current user from the calling system. This makes it easier to track changes that occurred through RFC.
- You can assign individual authorizations to the users in the called system. As such you can differentiate which actions or functions are accessible to the user in the called system irrespective of the user.

With this procedure, you must create the users that are to be allowed to execute using RFC functions in the called system as well. Note that in the ALE scenario of *SAP Dispute Management*, RFC calls take place from the Accounts Receivable system to the Dispute Case Processing system and vice versa. A trust relationship between SAP systems is **not** mutual. This means that you can choose whether one system is to be designated as trusted for the other system and vice versa, or whether you want to define the trust relationship only in one direction.

In Customizing of ALE (*Application Link Enabling*), you can also define different RFC destinations for dialog calls, for BAPI calls, and for sending IDocs. As such you can also define an RFC destination for the dialog calls that use the trusted/trusting system relationship and use the current user from the calling system for the RFC calls in the target system, whilst you define an RFC destination for BAPI calls and for the sending of IDocs that does not use the trusted/trusting system relationship and in which you enter a communication user.

i Note

Note the following if your Accounts Receivable system is known as a trusted system by the Dispute Case Processing system and you want to configure the RFC destination used for sending IDocs so that it uses the

trusted/trusting system relationship and the RFC calls in the target system with the current user from the calling system:

IDocs are sent to the Dispute Case Processing system from the Accounts Receivable system when items are cleared in the Accounts Receivable system, the clearing of items is reset, or partial payments are executed on items for which a promise to pay exists for the corresponding invoice. If the corresponding RFC destination uses the trusted/trusting system relationship, and carries out the call in the target system with the current user from the calling system, this means that the user triggering the clearing, reset of clearing, or partial payment must also be defined in the Dispute Case Processing system. You must therefore create **all** users who carry out clearing, resets of clearing, or partial payments in the Accounts Receivable system, and therefore affect dispute cases, in the Dispute Case Processing system.

13.2.8.2.5 Data Storage Security

Use

Master data, transaction data, and Customizing data of *SAP Dispute Management* are stored in the database of the SAP system.

Access to the database is restricted by the authorization objects of *SAP Dispute Management*.

13.2.8.3 SAP Collections Management

13.2.8.3.1 Technical System Landscape

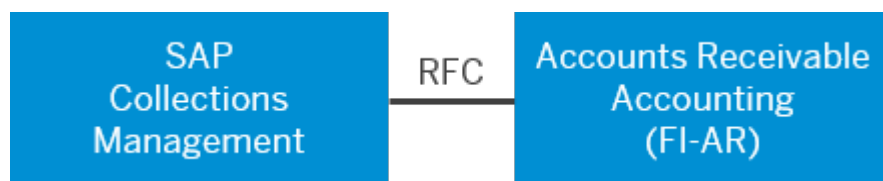
Use

You can use *SAP Collections Management* in a **one-system scenario** or in a **multiple-system scenario**. If you use *SAP Collections Management* in a one-system scenario, this means that you use *Collections Management* in the same system as Accounts Receivable. In a multiple-system scenario, you run *Collections Management* in a separate system. This communicates with the Accounts Receivable system connected by means of synchronous and asynchronous RFC calls and dialog calls.

The figure below shows the technical system landscape in a **one-system scenario**:

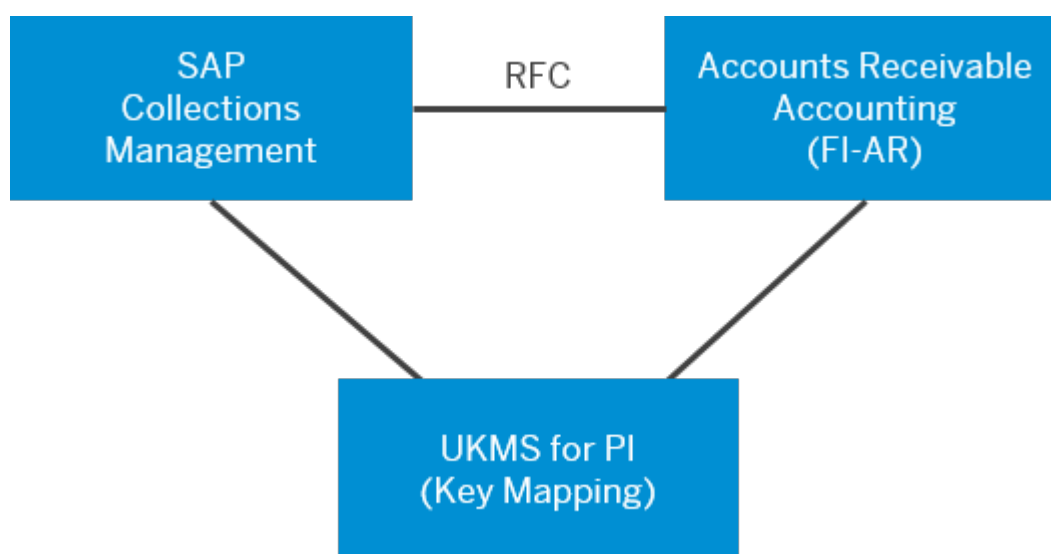


The following figure shows the technical system landscape in a **multiple-system scenario**:



If you connect several FI systems in a multiple-system scenario but have **not** installed a central system for processing customer master data, then you can resolve conflicts when assigning numbers with the connection of *Unified Key Mapping Service* to *SAP Process Integration* (UKMS connection to *SAP Process Integration*).

The figure below shows the technical system landscape in a **multiple-system scenario with several FI systems**:



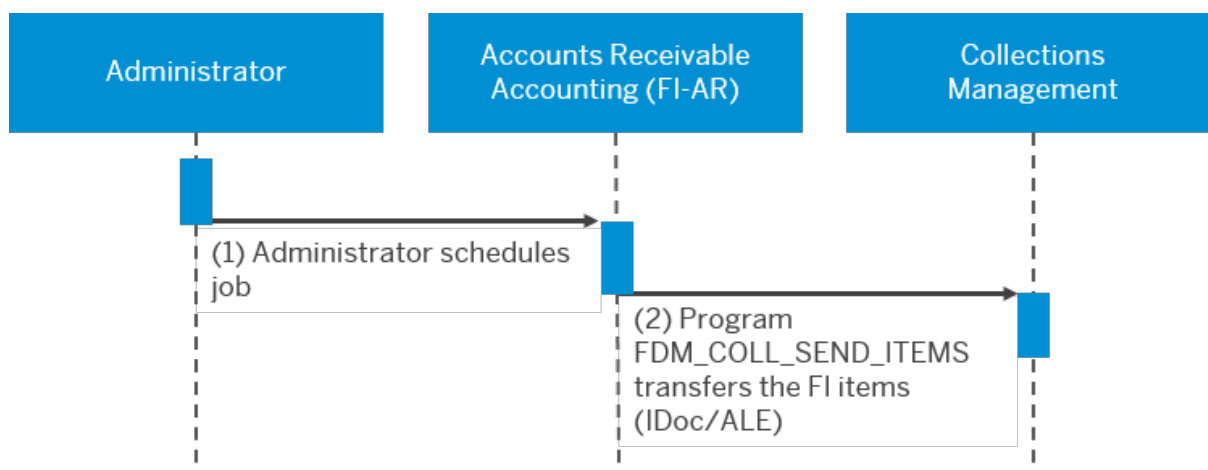
For additional information, go to https://help.sap.com/s4hana_op_2020, enter *Connecting to SAP Process Integration* into the search bar, press , and open the search result with that title.

13.2.8.3.2 Security Aspects of Data, Data Flow, and Processes

The following sections show an overview of the data flow in a multiple-system scenario.

13.2.8.3.2.1 Transfer of Transaction Data

The figure below shows the transfer of transaction data, meaning FI items, from the *Accounts Receivable* (FI-AR) system to the Collections Management system. This is data that the system needs for creating the worklists.

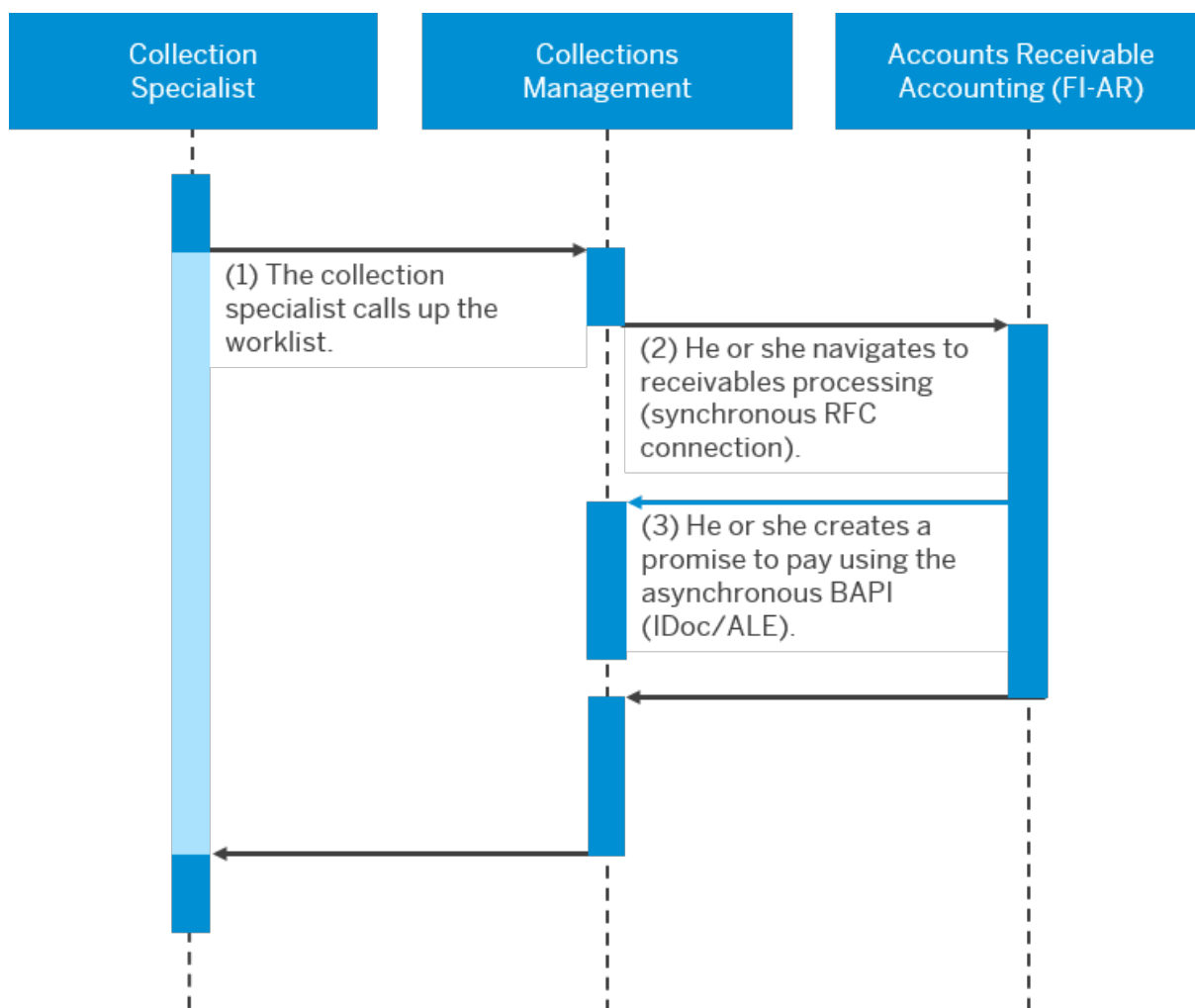


The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	The administrator schedules the job.	User type: Dialog user
2	Program FDM_COLL_SEND_ITEMS transfers the FI items (IDoc/ALE)	User type: Technical user or, when the Trusted/Trusting connection is used, dialog user (see also)

13.2.8.3.2.2 Processing of Items in the Worklist

The figure below shows how a collection specialist processes an item in his worklist, so creating a promise to pay.



The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	The collection specialist call up the worklist (transaction UDM_SPECIALIST)	User type: Dialog user
2	He then navigates to receivables processing (synchronous RFC connection)	User type: Dialog user
3	He creates a promise to pay with asynchronous BAPI (IDoc/ALE)	User type: Technical user or, when the Trusted/Trusting connection is used, dialog user

13.2.8.3.3 User Management

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that users who perform their tasks interactively have to change their passwords on a regular basis, but not those users who perform their tasks using background processing.

The user types that are required for *SAP Collections Management* include:

- Individual users:
 - For each individual user in your system, you need dialog users for the following purposes:
 - To use the system via *SAP GUI for Windows*
 - If you use *SAP Collections Management* in a multiple system scenario and the RFC destinations used use a Trusted/Trusting system relationship, calls to the other system are performed using the current user from the calling system. Therefore, for each user a valid user must also exist in the target system.
- Technical users:
 - Background users can be used for processing in the background.
 - If you use *SAP Collections Management* in a multiple system scenario and the RFC destinations concerned are configured such that they do **not** use a Trusted/Trusting system relationship, you need the following technical users for the RFC destinations:
 - Communication users are used for synchronous and asynchronous BAPI calls (IDocs).
 - Dialog users are used for dialog calls that take place remotely in the other system.

Standard Users

If you use *SAP Collections Management* in a multiple system scenario and there is **no** Trusted/Trusting system relationship between the systems involved, you have to configure corresponding users for the ALE/RFC communication between the systems involved.

Note that in *SAP Collections Management*, asynchronous BAPI calls (IDocs), synchronous BAPI calls, and dialog calls take place between the systems involved. There are calls from the Collections Management system to the system for Accounts Receivable Accounting and vice versa.

The following table shows the standard users required if you use *SAP Collections Management* in a multiple system scenario and there is **no** Trusted/Trusting system relationship between the systems involved.

System	User ID	Type	Password	Description
Collections Management system	Example: ALE-DIAG1	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Accounts Receivable Accounting system in the Collections Management system.
Collections Management system	Example: ALE-COMM1	Communication users	The user ID and password are stored in the RFC destination for the connection.	This user is used for synchronous BAPI calls or asynchronous BAPI calls (IDocs) from the Accounts Receivable Accounting system in the Collections Management system.
Accounts Receivable Accounting system	Example: ALE-DIAG2	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Collections Management system in the Accounts Receivable Accounting system.
Accounts Receivable Accounting system	Example: ALE-COMM2	Communication users	The user ID and password are stored in the RFC destination for the connection.	This user is used for synchronous BAPI calls or asynchronous BAPI calls (IDocs) from the Collections Management system in the Accounts Receivable Accounting system.

Create the users required and enter them in the corresponding RFC destinations. You can assign user IDs as required. The user IDs above are merely examples.

13.2.8.3.4 Communication Destinations

Use

The following table shows an overview of the communication destinations that you need for *SAP Collections Management* if you use it in a multiple-system scenario. You can use these communication destinations to establish communication between the Financial Accounting system and the system that contains SAP Collections Management.

You can assign names for your RFC destinations as required. The names of the RFC destinations that are specified in the table are merely examples. The destinations are not delivered in the standard system; you need to create them yourself.

Destination	Description	User, Authorizations
Example: COL2FIN_DIAG	This destination is used for dialog calls that take place from the Collections Management system to the Accounts Receivable system by means of RFC.	<p>RFC user (dialog) in Receivables Processing</p> <p>Role: SAP_FIN_FSCM_COL_AR_RFC_DIALOG</p> <p>Contains the authorizations for a user with which the navigate to receivables processing from the worklist by means of RFC. The authorizations permit the following activities:</p> <ul style="list-style-type: none"> Display of invoice data Display of payment data Display of invoice history Creation, change, or display of a contact person
Example: COL2FIN_COMM	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Collections Management system to the Accounts Receivable system.	<p>RFC user (communication) in Accounts Receivable</p> <p>Role: SAP_FIN_FSCM_COL_AR_RFC_COMM</p> <p>Contains authorizations for a user with which synchronous and asynchronous BAPI methods are called from the SAP Collections Management system in the Accounts Receivable system.</p> <p>An example of such a method is the automatic notification to Accounts Receivable when promises to pay are confirmed and voided.</p>

Destination	Description	User, Authorizations
Example: FIN2COL_DIAG	This destination is used for dialog calls that take place from the Accounts Receivable system to the Collections Management system by means of RFC.	<p>RFC user (dialog) for collections management functions</p> <p>Role: SAP_FIN_FSCM_COL_RFC_DIALOG</p> <p>Contains authorizations for a user with which dialog methods are called in the SAP Collections Management system from the Financial Accounting system by means of RFC.</p> <p>For example, navigation from receivables processing to the detail display of the promise to pay or dispute case.</p>
Example: FIN2COL_COMM	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Accounts Receivable system to the Collections Management system.	<p>RFC user (communication) for collections management</p> <p>Role: SAP_FIN_FSCM_COL_RFC_COMM</p> <p>Contains authorizations for a user with which synchronous and asynchronous methods are called in the SAP Collections Management system from the Financial Accounting system.</p> <p>For example:</p> <p>Posting of IDocs with data from Financial Accounting</p> <p>Creation of dispute cases, promises to pay, customer contacts, and resubmissions</p> <p>Reading of attributes of dispute cases, promises to pay, customer contacts, and resubmissions for display in receivables processing</p>

Possible additional necessary destinations

If you connect several FI systems in a multiple-system scenario and use the connection of *Unified Key Mapping Service* to *SAP Process Integration* (UKMS connection to *SAP Process Integration*) to resolve conflicts when assigning numbers, you also need to set up the following destinations:

- Calls from the of accounts receivable system to the system of *SAP Process Integration* (PI system)
- Calls from the *Collections Management* system to the PI system

For additional information, see Customizing of *SAP Collections Management* under ► [Basic Settings for Collections Management](#) ► [Business Partners](#) ► [Master Data Distribution for Several FI Systems](#) ►, if you have activated business function *FSCM Functions 2* (FIN_FSCM_CCD_2).

For additional information about the security aspects of the *CRM Middleware* that you can use as a tool for master data replication, see the Security Guide for *SAP Customer Relationship Management*.

Set up RFC destinations for the ALE scenario

When you set up the RFC destinations for the ALE scenario, check whether the option of trusted/trusting system relationship is relevant for you. Using an RFC trusted/trusting system relationship between two SAP systems means that in the case of an RFC (Remote Function Call) from the trusted to the trusting system, no password is sent for the logon to the trusting system. You can configure the RFC destinations in such a way that the call in the target system occurs with the current user from the calling system without a password being specified or entered on the logon screen. This has the following advantages, for example:

When changes to objects or data are logged in the called system, this logging takes place with the current user from the calling system. This makes it easier to track changes that occurred through RFC.

You can assign individual authorizations to the users in the called system. As such you can differentiate which actions or functions are accessible to the user in the called system irrespective of the user.

With this procedure, you must create the users that are to be allowed to execute using RFC functions in the called system as well. Note that in the ALE scenario of *SAP Collections Management*, RFC calls take place from the Accounts Receivable system to the Collections Management system and vice versa. A trust relationship between SAP systems is not mutual. This means that you can choose whether one system is to be designated as trusted for the other system and vice versa, or whether you want to define the trust relationship only in one direction.

In the Customizing of ALE (*Application Link Enabling*), you can also define different RFC destinations for dialog calls, for BAPI calls, and for sending IDocs. As such you can also define an RFC destination for the dialog calls that use the trusted/trusting system relationship and use the current user from the calling system for the RFC calls in the target system, whilst you define an RFC destination for BAPI calls and for the sending of IDocs that does not use the trusted/trusting system relationship and in which you enter a communication user.

i Note

Note the following if your Accounts Receivable system is known as a trusted system by the Collections Management system and you want to configure the RFC destination used for sending IDocs so that it uses the trusted/trusting system relationship and carries out the RFC calls in the target system with the current user from the calling system:

IDocs are sent to the Collections Management system from the Accounts Receivable system when items are cleared in the Accounts Receivable system, the clearing of items is reset, or partial payments are executed on items for which a promise to pay exists for the corresponding invoice. If the corresponding RFC destination uses the trusted/trusting system relationship, and carries out the call in the target system with the current user from the calling system, this means that the user triggering the clearing, reset of clearing, or partial payment must also be defined in the Collections Management system. You must therefore create all users who carry out clearing, resets of clearing, or partial payments in the Accounts Receivable system, and therefore affect promises to pay, in the Collections Management system.

13.2.9 SAP S/4HANA Financial Closing cockpit

13.2.9.1 Authorizations

The *SAP S/4HANA Financial Closing cockpit* uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the AS ABAP Security Guide also apply to the *SAP S/4HANA Financial Closing cockpit*.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF00`) on the AS ABAP and the User Management Engine's user administration console on the AS Java.

For more information about how to create roles, go to the [SAP Help Portal](#) and search for *User and Role Administration of Application Server ABAP*. There, go to ► [Configuration of User and Role Administration](#) ► [Role Administration](#) ►

Authorizations for Business Intelligence (BI) iViews

BI authorizations are maintained separately from the authorizations in the *SAP S/4HANA Financial Closing cockpit*. You need the standard BI authorizations for executing queries.

For more information, go to the [SAP Help Portal](#) and search for *Data Warehouse Management*. There, go to ► [Authorizations](#) ► [Authorizations for Working with Queries](#) ►.

13.2.10 Travel Management

13.2.10.1 Travel Management

Authorizations

Standard Roles in Travel Management (for Web Dynpro ABAP-Based Applications)

Role	Description
SAP_FI_TV_WEB_TRAVELER_2	<p><i>Traveler</i></p> <p>The role contains the authorization profile needed to execute the applications of the <i>Travel and Expenses</i> Employee Self-Service (ESS) in <i>SAP Enterprise Portal</i>.</p>
SAP_FI_TV_WEB_TRAVELER_EXT_TP	<p><i>Traveler</i></p> <p>Users with this role can execute the work center for travelers and the corresponding applications in NWBC. NWBC calls a third-party travel planning solution instead of SAP Travel Planning.</p> <p>The role contains the authorization profile needed to execute the applications of the <i>Travel and Expenses</i> ESS in <i>SAP Enterprise Portal</i>.</p>
SAP_FI_TV_WEB_ESS_TRAVELER_2	<p><i>ESS Single Role for Travelers</i></p> <p>Users with this role can execute the work center for travelers and the corresponding applications in NWBC.</p> <p>This role is integrated into the ESS role for Web Dynpro ABAP-based applications (<i>SAP_EMPLOYEE_ESS_WDA_1</i>).</p>
SAP_FI_TV_WEB_ASSISTANT_2	<p><i>Travel Assistant</i></p> <p>Users with this role can execute the work center for travel assistants and the corresponding applications in NWBC.</p> <p>The role contains the authorization profile needed to execute the applications of the <i>Travel and Expenses</i> ESS in <i>SAP Enterprise Portal</i>.</p>
SAP_FI_TV_WEB_ESS_ASSISTANT_2	<p><i>Travel Assistant</i></p> <p>Users with this role can execute the work center for travel assistants and the corresponding applications in NWBC.</p>
SAP_FI_TV_WEB_APPROVER_2	<p><i>Approving Manager</i></p> <p>Users with this role can execute the work center for approving managers and the corresponding applications in NWBC.</p> <p>This role is integrated into the MSS role for Web Dynpro ABAP-based applications (<i>SAP_MANAGER_MSS_NWBC</i>).</p>

Role	Description
SAP_FI_TV_WEB_POLICY_ADMIN_2	<p><i>Travel Policy Administrator</i></p> <p>Users with this role can execute frequently used Customizing applications for policy management in NWBC.</p>
SAP_FI_TV_TIC_AGENT	<p><i>Travel Interaction Center Agent</i></p> <p>This role authorizes service agents to run the required transactions and Web Dynpro ABAP-based applications in the Travel Management system from within the Travel Interaction Center.</p> <p>The Travel Interaction Center is a Shared Services Center in <i>SAP Customer Relationship Management (SAP CRM)</i>.</p>

Authorization Profiles

The standard system contains the travel profile FI-TV (infotype 0470 of *Human Resources Management (HCM)*). Alternatively, you can create the authorization profile by means of organizational assignment using the HR feature *TRVCP*.

Authorization Objects

For all general functions, *Travel Management* uses the authorization object P_TRAVL.

The transfer of results from expense reports to *accounting* is protected by the authorization object F_TRAVL.

The travel plan status is protected by the authorization object F_TRAVL_S.

Network and Communication Security

In Travel Management, you can set up connections to the following *global distribution systems (GDS)*:

- *Amadeus*
The partner is responsible for the Gateway.
- *Galileo*
The partner is responsible for the Gateway.

Alternatively or in addition, you can use *SAP Process Integration* to set up direct connections to the following travel service providers:

- Flight reservation systems, for example, low-cost carrier providers
Depending on the partner, communication with the Web services is HTTPS or HTTP based.
- Hotel reservation systems such as HRS
Depending on the partner, communication with the Web services is HTTPS or HTTP based. For the communication channel, you can make various security settings. For more information, see the *Configuration Guide*.
- Rail portals such as Deutsche Bahn (BIBE)
Communication with the Web services is HTTPS based.

Alternatively, instead of using SAP Travel Planning, you can use third-party online booking systems (third-party travel planning) such as:

- [GetThere](#)
Communication with the Web services of [GetThere](#) (and of [Sabre](#), if applicable) is HTTPS based. In [SAP Enterprise Portal](#), you can use Single Sign-On (SSO) to automatically log on the SAP Travel Management users to a third-party online booking system.
- [e-Travel](#)
Communication with the Web services of [e-Travel](#) is HTTPS based. In [SAP Enterprise Portal](#), you can use SSO to automatically log on the SAP Travel Management users to a third-party online booking system.

For credit card clearing in [Travel Management](#), you can use [SAP Process Integration](#) to set up direct connections to credit card companies. You agree upon the safeguarding of the connection with the respective partner. For more information, see [SAP Library](#) under ► [Travel Management \(FI-TV\)](#) ► [Travel Expenses \(FI-TV-COS\)](#) ► [Credit Card Clearing](#) ►.

Data Storage Security

[Travel Management](#) transmits credit card information to the named partners. The data in the SAP system **cannot** be accessed.

[Travel Management](#) supports secure handling of credit card data.

To set up connections to third-party systems, such as reservation systems, you might require company IDs and user-specific technical passwords, which you can define in Customizing or in user-specific infotypes. In Customizing, this data is protected by standard authorization objects for Customizing.

[Travel Management](#) imports data from files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). You do this by specifying logical paths and file names in the system that are assigned to the physical paths and file names. The system validates the assignment at runtime and issues an error message if access to a directory is requested that does **not** match any assignment defined.

13.2.10.2 Deletion of Personal Data in FI-TV

Use

The [Travel Management \(FI-TV\)](#) component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

Relevant Application Objects and Available Deletion Functionality

For information, see SAP Note [2028594](#).

Relevant Application and Available WUC functionality

Application	Implemented Solution	Further Information
Travel Expenses (FI-TV-COS)	Where-used check (WUC)	SAP Note 2028595

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for Cross-Application Components under Data Protection.

13.2.11 Incentive and Sales Force Management

Purpose

Incentive and Sales Force Management (ISF) offers a range of security-related functions to handle your security requirements. In addition to the specific *Incentive and Sales Force Management* topics, see also the [SAP Security Guide \[page 182\]](#) that covers the SAP security standard as a whole.

Features

Here you find all of the security topics related to *Incentive and Sales Force Management* and links to the relevant sections in the SAP Security Guide.

[Introduction \[page 182\]](#)

[Before You Start \[page 182\]](#)

[User Management and Authentication \[page 183\]](#)

[Authorization Management in Incentive and Sales Force Management \[page 188\]](#)

[Network and Communication Security \[page 228\]](#)

[Virus Protection \[page 229\]](#)

[Data Protection \[page 229\]](#)

[Revision Security in Incentive and Sales Force Management \[page 234\]](#)

[Procedure Documentation in Incentive and Sales Force Management \[page 235\]](#)

13.2.11.1 Introduction

⚠ Caution

This guide does not replace the administrative or operational guides that are available for the productive operation.

Target Group

- Technology consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all life cycle phases.

The Need for Security

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system must not result in loss of information or processing time. These security requirements equally apply to Incentive and Sales Force Management. We provide this Security Guide to assist you in securing your application.

13.2.11.2 Before You Start

Security Guides Referenced

Incentive and Commission Management is based on the technology of SAP NetWeaver.

Consequently you should refer to the Security Guide of *SAP NetWeaver* on the *SAP Help Portal* under the Internet address [▶ help.sap.com ▶ Documentation ▶ SAP NetWeaver ▶ Release/Language SAP NetWeaver ▶ Security ▶ SAP NetWeaver Security Guide. ▶](#)

To view all of the SAP security guides, see the *SAP Service Marketplace* under the Internet address [service.sap.com/securityguide](#).

Important SAP Notes

SAP Note 138498 contains information on single sign-on solutions.

For further SAP notes on security, see the *SAP Service Marketplace* under the Internet address [▶ service.sap.com/security](https://service.sap.com/security) > *SAP Security Notes* ▶.

Additional information

For more information about specific topics, see the sources in the table below.

Additional Information

Contents	Quick Link to SAP Service Marketplace
Security	service.sap.com/security
Security guides, <i>SAP NetWeaver</i> security guide	service.sap.com/securityguide
SAP NetWeaver documentation	▶ help.sap.com > <i>Documentation</i> > <i>SAPNetWeaver</i> ▶
Related SAP notes	service.sap.com/notes

13.2.11.3 User Management and Authentication

Use

Incentive and Sales Force Management uses the user administration and authentication mechanisms of the *SAP NetWeaver* platform, and in particular the *SAP NetWeaver Application Server*. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver AS Security Guide for ABAP Technology* also apply to ISF.

Setting up users and assigning roles to user master data records are basic prerequisites for starting up an SAP system. Secure authentication protects the system against unauthorized users and the related security risks. ISF takes into account the SAP security standards for user authentication.

i Note

For more information, see

- SAP Help Portal under the Internet address [▶ help.sap.com](https://help.sap.com) > *Documentation* > *SAP NetWeaver* > *Release/LanguageSAP NetWeaver* > *Security* > *User Authentication and Single Sign-On* ▶

- or SAP Service Marketplace under the Internet address [▶ service.sap.com/security](https://service.sap.com/security) > *Security in Detail* > *SAP Security Guides* > *SAP Basis / Web AS Security Guides* ▶

- [User Authentication](#)
- [SAP Authorization Concept](#)

In addition to these guidelines, we include information about user administration and authentication that specifically applies to ISF in the following topics:

User Administration

This section lists the tools to use for user administration, the types of users required, and the standard users that are delivered with ISF.

Integration in Single Sign-On Environments

This section describes how ISF supports single sign-on mechanisms.

13.2.11.3.1 User Administration

User administration in *Incentive and Sales Force Management* uses the mechanisms provided with the [SAP NetWeaver Application Server for ABAP](#), for example tools, user types, and password policies.

For an overview of how these mechanisms affect ISF see the sections below.

In addition, we provide a list of the standard users required for operating ISF.

User Administration Tools

The following table displays the tools of the user administration in ISF.

User Management Tools

Tool	Detailed Description
User and role maintenance with Application Server ABAP (Transactions SU01 and PFCG)	For more information, go to the product page for SAP S/4HANA , choose your release and then ► Product Assistance ► Enterprise Technology ► ABAP Platform ► Administering the ABAP Platform ► Administration Concepts and Tools ► Solution Lifecycle Management ► Identity and Access Management ►.
Central User Administration (CUA) for the maintenance of multiple ABAP-based systems	Administration of users in a central system. A SAP system group consists of several SAP system with several clients. The same users are frequently created in each client and roles assigned. The objective of Central User Administration is to complete these tasks in a central system and pass on the data to the systems in the SAP system group.

Tool	Detailed Description
User Management Engine (UME)	<p>Administration console for maintenance of users, roles, and authorizations in Java-based systems and in the Enterprise Portal.</p> <p>The UME also provides persistence options, such as ABAP Engine.</p>

Note

For more information on the tools that SAP provides for user management with [SAP NetWeaver](#), see SAP Service Marketplace at [▶ service.sap.com/securityguide ▶ SAP NetWeaver Security Guide ▶ User Administration and Authentication ▶](#).

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run, for example:

- Individual users:
 - Dialog users
Dialog users are used for SAP GUI for Windows.
 - Internet users for Web applications
Here, the same policies as for dialog users also apply for Internet connections.
- Technical users:
 - Service users
Service users are dialog users who are available for a large set of anonymous users (for example, for anonymous system access via an ITS service).
 - Communication users
Communication users are used for dialog-free communication between systems.
 - Background users
Background users can be used for processing in the background.

For additional information on user types, see [User Types](#) in the Security Guide for [SAP NetWeaver](#).

Standard Users

The table below shows the standard users that are necessary for operating ISF.

System	User ID	Type	Password	Description
<i>SAP NetWeaver Application Server</i>	<sapsid>adm	SAP system administrator	Mandatory	SAP NetWeaver installation guide
<i>SAP NetWeaver Application Server</i>	SAP Service <sapsid>	SAP system service administrator	Mandatory	SAP NetWeaver installation guide
<i>SAP NetWeaver Application Server</i>	SAP Standard ABAP user (SAP*, DDIC, EARLY-WATCH, SAPCPIC)	See <i>SAP NetWeaver Security Guide</i>	See <i>SAP NetWeaver Security Guide</i>	<p>▶ service.sap.com/securityguide ▶ <i>SAP NetWeaver Security Guide</i> ▶ <i>Security Guides for the SAP NetWeaver Products</i> ▶ <i>SAP NetWeaver Application Server Security Guide</i> ▶ <i>SAP NetWeaver Application Server Security Guide for ABAP Technology</i> ▶ <i>User Authentication</i> ▶ <i>Protecting Standard Users</i> ▶</p> <p>These users are used in applications that use Web Dynpro.</p>
<i>SAP NetWeaver Application Server</i>	SAP Standard SAP NetWeaver AS for Java users	See <i>SAP NetWeaver Security Guide</i>	See <i>SAP NetWeaver Security Guide</i>	<p>▶ service.sap.com/securityguide ▶ <i>SAP NetWeaver Security Guide</i> ▶ <i>Security Guides for the SAP NetWeaver Products</i> ▶ <i>SAP NetWeaver Application Server Security Guide</i> ▶ <i>SAP NetWeaver Application Server Security Guide for Java Technology</i> ▶ <i>Users and User Management</i> ▶ <i>Standard Users and Groups</i> ▶.</p> <p>These users are used in applications that use Web Dynpro.</p>

System	User ID	Type	Password	Description
SAP ECC	SAP Users	Dialog users	Mandatory	The number of users depends on the area of operation and the business data to be processed.

Note

For more information about standard users in *SAP NetWeaver*, see *SAP Help Portal* at help.sap.com [Documentation](#) [SAP NetWeaver](#) [Release xx/Language](#) [Security](#) [Identity Management](#) [Users and Roles \(BC-SEC-USR\)](#) [User Maintenance](#) [Logon and Password Security in the SAP System](#) [Password Rules](#).

For information about user types, see *SAP Service Marketplace* at service.sap.com/securityguide [SAP NetWeaver Security Guide](#) [User Administration and Authentication](#) [User Management](#) and then *User Types*.

13.2.11.3.2 Integration in Single Sign-On Environments

Incentive and Sales Force Management supports the single sign-on mechanisms (SSO mechanisms) of the SAP NetWeaver Application Server. Therefore, the security recommendations and guidelines for user administration and authentication as described in the Security Guide for *SAP NetWeaver Application Server* also apply to *Incentive and Sales Force Management*.

The supported mechanisms are listed below.

Secure Network Communications (SNC)

SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.

For more information, see **SAP Service Marketplace** at service.sap.com/securityguide [SAP NetWeaver Security Guide](#) [Security Guides for the SAP NetWeaver Products](#) [SAP NetWeaver Application Server Security Guide](#) [SAP NetWeaver AS Security Guide for ABAP Technology](#) [User Authentication](#) [Authentication and Single Sign-On](#) [Secure Network Communications \(SNC\)](#).

SAP Logon Tickets

ISF supports the use of logon tickets for SSO when using a Web browser as the front-end client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The

ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.

For more information, see the [SAP Web Application Server](#) under [SAP Logon Tickets](#).

Client Certificates

As an alternative to user authentication using a user ID and passwords, users using a Web browser as a front-end client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

For more information, see [Client Certificates](#) in the [SAP NetWeaver Application Server](#) security guide.

13.2.11.4 Authorization Management in Incentive and Sales Force Management

Use

The authorization concept comprises the structure and functions of authorization assignment and authorization checks in the SAP system.

Having authorization means that you can execute a certain action in the SAP system.

Each authorization refers to an authorization object and defines one or more values for each authorization field contained in the authorization object. Authorizations are summarized in profiles, which are entered in the user's master data.

Integration

In the environment of [Incentive and Sales Force Management](#), the two main areas that you should protect against unauthorized access by implementing an authorization concept are the commission agreements and the commission database. For more information on agreements, go to the product assistance for [SAP S/4HANA](#), choose your release and then [Product Assistance](#) [Enterprise Business Applications](#) [Finance](#) [Incentive and Sales Force Management](#) [Incentive and Commission Management](#) [Master Data](#) [Commission Contracts](#) [Agreements](#).

You can also use authorization objects to control the credentials to execute certain actions.

Prerequisites

Before you can assign authorization profiles in *Incentive and Sales Force Management* , you must have system administrator authorization for your system.

Features

To be able to work with an application (ICM or CRD), the user needs authorization for each application.

Within the application itself, the functions and menu options that users can select might depend on different user profiles that are assigned to the user.

All menu options are displayed in the ISF menu. The authorization check does not take place until the user tries to call a transaction via a menu option. If the user does not have authorization for the transaction in question, the system issues a corresponding error message.

Authorizations in ISF are classed as quantifying , qualifying , or [structural \[page 220\]](#) authorizations.

Quantifying Authorization Groups

You can group quantifying authorizations into authorization groups.

Qualifying Authorization Profiles

You control qualifying authorizations with the help of commission-specific authorization profiles .

Structural Authorizations

You map structural authorizations by creating appropriate links in Organizational Management.

Company-specific specifications govern the assignment of authorizations, in other words, who is given which authorization for which object. This means that authorizations can be derived from the position of the person in the company hierarchy.

❖ Example

Commission contract partner A can only view their own data and that of their subordinates.

Commission contract partner B can only see their own data.

Commission contract partner C can only see data from their subordinates.

13.2.11.4.1 Authorization profile

Use

Authorization profiles give users access to the system. They contain authorizations that are identified by the name of an authorization object and the name of an authorization. If the system administrator enters a profile in the user master record, then the user is assigned all the authorizations contained in the profile.

Prerequisite

You maintain authorizations for the whole commission application centrally. To do so, you need administrator authorization in your SAP system. In Incentive and Commission Management, there is an authorization profile for every authorization object.

Features

A profile can be a single profile or a collective profile.

- **Single profiles** contain authorizations. Each authorization is identified by the name of an authorization object and the name of the authorization that was created for the object.
- **Collective profiles** contain other profiles. A collective profile gives the user all single or collective profiles contained therein. To get all the superuser authorizations, select the composite profile **SAP_ICM_C_SUSER**.

i Note

For additional information on the authorization profile, see the SAP Library under mySAP Technology Components ->SAP WEB Application Server-> Security (BC-SEC) -> Users and Roles (BC-SEC-USR).

13.2.11.4.1.1 Authorization Control

Use

Authorizations in *Incentive and Sales Force Management* are controlled by the authorization profiles documented below: Each authorization refers to an authorization object and defines one or more values for each authorization field contained in the authorization object.

Certain permitted activities are assigned to each authorization object. For additional information, see Permitted Activities for each Authorization Object .

Prerequisites

To set the required authorizations in ISF, choose from the SAP Easy Access Menu **Tools** > **Administration** > **User Maintenance** > **Information System** > **Authorization Objects** > **Authorization Objects by Complex Search Criteria**.

Features

Authorization Objects in ISF

Authorization Object	Description	Field
E_CACS_ACC	Authorization for settlement	ACTVTCACS_APPL
E_CACS_ADM	Authorization for administrator	ACTVTCACS_APPL
E_CACS_ALV	Save authorization for global ALV layouts	CACS_APPL
E_CACS_APP	Application authorization	CACS_APPL
E_CACS_BDL	Authorization for contract bundling	ACTVTCACS_APPL
E_CACS_BK	Post commission case	ACTVTCACS_APPLBUS_OBJ_TY
E_CACS_BR	Authorization object for Business Rule Editor	ACTVTCACS_APPL
E_CACS_CHG	Authorization for follow-up and additional postings	ACTVTCACS_APPL
E_CACS_CSD	Authorization for user interface dispatcher transactions	TCDCACS_APPL
E_CACS_CTR	Authorization for commission contracts	CACS_APPLACTVTCACS_GPART CACS_CTRID
E_CACS_DOC	Post document	ACTVTCACS_APPL DOC_TYPE
E_CACS_EDT	Edit	CACS_APPL
E_CACS_FGB	Commissions: Field group contract bundle	CACS_FDG_B
E_CACS_FGC	Commissions: Field group commission contract	CACS_FDG_C
E_CACS_GEN	Authorization for generator	ACTVTCACS_APPL
E_CACS_HRG	HR Customizing	ACTVT
E_CACS_MAS	Mass processing	ACTVTCACS_APPL
E_CACS_OBJ	Authorization for object data changes in commission case	CACS_APPLBUS_OBJ_TY

Authorization Object	Description	Field
E_CACS_REV	Authorization for releasing and returning for review	ACTVTCACS_APPL
E_CACS_SEG	Authorization for segment assignment	CACS_APPLACTVT CACS_SEGID CACS_SEGTY
E_CACS_SFA	Display/change other account	ACTVTCACS_APPL
E_CACS_SFC	Display/change other commission contract	ACTVTCACS_APPL
E_CACS_SLC	Also permits a change to organizational unit manager	ACTVTCACS_APPL
E_CACS_SMA	Display own account	ACTVTCACS_APPL
E_CACS_SMC	Display/change own commission contract	ACTVTCACS_APPL
K_KA_RPT	Interactive drilldown reports	ACTVTCEAPPL CEREPIID TABLE
K_KA_RCS	Interactive drilldown reporting line/column structures	ACTVTCEAPPL CEFORM TABLE
B_BUPA_ATT	Business partner: Authorization types	ACTVTAUTHTYP AUVAL1 AUVAL2
B_BUPA_GRP	Business partner: Authorization groups	ACTVTBEGRU
B_BUPA_FDG	Business partner: Field groups	FLDGRACTVT
B_BUPA_RLT	Business partner: BP roles	ACTVTRLTYP
B_CCARD	Payment cards	ACTVT
B_BUPA_ALL	Business partner: All authorizations	ACTVT

Authorization Object	Description	Field
S_WFAR_OBJ	SAP ArchiveLink: Authorizations for accessing documents	OAARCHIV OAOBJEKTE OADOKUMENT ACTVT
S_WFAR_PRI	SAP ArchiveLink: Authorization for accessing print lists	OAARCHIV OAOBJEKTE OADOKUMENT ACTVT PROGRAM
S_PROJECT	Project management: Authorization for working with projects	PROJECT_ID APPL_COMP ACTVT PROJ_CONF
S_DEVELOP	ABAP/4 Development Workbench	DEVCLASS OBJTYPE OBJNAME P_GROUP ACTVT
S_PROJECTS	Super-user authorization in management	APPL_COMP PRCLASS ACTVT
S_MWB_FCOD	Permitted function codes for Manager's Desktop	MWBFCODE
S_TABU_DIS	Table maintenance (using standard tools such as SM30)	DICBERCLS ACTVT
V_KONG_VWE	Condition generating program: Authorization for use/application	KVEWE KAPPL ACTVT

Authorization Object	Description	Field
V_KOND_VEA	Condition maintenance: Authorization for use/application/condition type/table	KVEWE KAPPL KSCHL KOTABNR ACTVT
V_VVISCS_ALL	All authorizations for commission system	Contains authorization fields for the objects B_BUPA_ALL and E_CACS_ALL
PLOG	Personnel planning and development	PLVAROTYPE INFOTYP SUBTYPISTATPPFCODE

13.2.11.4.1.2 Permitted Activities for each Authorization Object

Use

This overview lists all the activities that are possible for each authorization profile.

Prerequisite

To make set corresponding authorizations in Commission Management, choose from the SAP Easy Access Menu ► [Tools](#) ► [Administration](#) ► [User Maintenance](#) ► [Information System](#) ► [Profile](#) .

Features

Authorization Object	Permitted actions
E_CACS_ADM	01 Add or Create
	02 Change
	03 Display
	04 Print, Process messages
	05 Lock
	06 Deletion
	07 Activate, Generate
	08 Display change documents
	09 Price display
	10 Post
	11 Number range: Change status
	12 Maintain/generate change documents
	13 Initialize number statuses
	14 Field selection: Generate screen
	15 Field selection: Assign table
	16 Execute
	17 Maintain number range object
	18 Deliveries from collective processing
	19 Bills from collective processing
	20 Transport without translation
	21 Transport
	22 Enter, include, assign
	23 Maintain
	24 Archive
	25 Restore
	26 Change customer's account group
	27 Display totals records
	28 Display single items
	29 Display saved data
	30 Determine

Authorization Object**Permitted actions**

- 31 Confirm
 - 32 Save
 - 33 Read
 - 34 Write
 - 35 Output
 - 36 Extended maintenance
 - 37 Accept
 - 38 Exercise
 - 39 Check
 - 40 Create in database
 - 41 Delete in database
 - 42 Convert in database
 - 43 Release
 - 44 Mark
 - 45 Permit
 - 47 Lend
 - 48 Simulate
 - 49 Request
 - 50 Postpone
 - 51 Initialize
 - 52 Change application start
 - 53 Display application start
 - 54 Display archive application
 - 55 Change archive application
 - 56 Display archive
 - 57 Store archive
 - 58 Display transfer
 - 59 Distribute
 - 60 Import
 - 61 Export
 - 62 Create ledger
 - 63 Activate
-

Authorization Object**Permitted actions**

64 Generate
65 Reorganize
66 Update
67 Translate
68 Model
69 Reject
70 Manage, administration
71 Evaluate
72 Plan
73 Write digital signature
74 Take back approval
75 Accept
76 Enter
77 Park
78 Assign
81 Schedule
82 Supplement
83 Counterconfirm
84 Settle
85 Reverse
88 Exercise
90 Transfer
91 Reactivate
913 Calculate
95 Unlock
97 Fix
98 Mark for release
99 Create invoice lists
A1 Defer
A2 Pay out
A3 Change status
A4 Resubmit

Authorization Object**Permitted actions**

A5 Display reports
A6 Read with filter
A7 Write with filter
A8 Process mass data
A9 Send
B1 Display permitted values
B2 Close from technical point of view
B3 Derive
B4 Deactivate
B5 Display history
B6 Create file
BD Object maintenance not in own system
BE IMG projection
C1 Maintenance of payment cards
C2 Display of payment cards
C3 Maintenance of manual authorization
C4 Close lot
C8 Confirm change
D1 Copy
DL Download
DP Delete planning
E0 Save extract
E6 Delete own extracts
E7 Delete external extracts
FP Change customer field selection
IA Process inactive
KA Activate notice of termination
KS Reverse notice of termination
LO All functions
L1 Features stage 1
L2 Features stage 2

Authorization Object	Permitted actions
	O1 Overbook O2 Overbooking always possible P1 Display list P2 Change date/room P3 Change released dates P4 Release plan U2 Carry out business volume comparison U3 Change business volume comparison U4 Add business volume data UL Upload VP Process VIP
E_CACS_CHG	02 Change 03 Display
E_CACS_GEN	02 Change 03 Display 64 Generate

Authorization Object	Permitted actions
E_CACS_ACC	01 Add or Create 02 Change 03 Display 04 Print, Process messages 05 Lock 06 Deletion 07 Activate, Generate 08 Display change documents 09 Price display 10 Post 11 Number range: Change status 12 Maintain/generate change documents 13 Initialize number statuses 14 Field selection: Generate screen 15 Field selection: Assign table 16 Execute 17 Maintain number range object 18 Deliveries from collective processing 19 Bills from collective processing 20 Transport without translation 21 Transport 22 Enter, include, assign 23 Maintain 24 Archive 25 Restore 26 Change customer's account group 27 Display totals records 28 Display single items 29 Display saved data 30 Determine 31 Confirm

Authorization Object**Permitted actions**

- 32 Save
 - 33 Read
 - 34 Write
 - 35 Output
 - 36 Extended maintenance
 - 37 Accept
 - 38 Exercise
 - 39 Check
 - 40 Create in database
 - 41 Delete in database
 - 42 Convert in database
 - 43 Release
 - 44 Mark
 - 45 Permit
 - 47 Lend
 - 48 Simulate
 - 49 Request
 - 50 Postpone
 - 51 Initialize
 - 52 Change application start
 - 53 Display application start
 - 54 Display archive application
 - 55 Change archive application
 - 56 Display archive
 - 57 Store archive
 - 58 Display transfer
 - 59 Distribute
 - 60 Import
 - 61 Export
 - 62 Create ledger
 - 63 Activate
 - 64 Generate
-

Authorization Object**Permitted actions**

65 Reorganize

66 Update

67 Translate

68 Model

69 Reject

70 Manage, administration

71 Evaluate

72 Plan

73 Write digital signature

74 Take back approval

75 Accept

76 Enter

77 Park

78 Assign

81 Schedule

82 Supplement

83 Counterconfirm

84 Settle

85 Reverse

88 Exercise

90 Transfer

91 Reactivate

93 Calculate

95 Unlock

97 Fix

98 Mark for release

99 Create invoice lists

A1 Defer

A2 Pay out

A3 Change status

A4 Resubmit

A5 Display reports

Authorization Object**Permitted actions**

A6 Read with filter
A7 Write with filter
A8 Process mass data
A9 Send
B1 Display permitted values
B2 Close from technical point of view
B3 Derive
B4 Deactivate
B5 Display history
B6 Create file
BD Object maintenance not in own system
BE IMG projection
C1 Maintenance of payment cards
C2 Display of payment cards
C3 Maintenance of manual authorization
C4 Close lot
C8 Confirm change
D1 Copy
DL Download
DP Delete planning
E0 Save extract
E6 Delete own extracts
E7 Delete external extracts
FP Change customer field selection
IA Process inactive
KA Activate notice of termination
KS Reverse notice of termination
L0 All functions
L1 Features stage 1
L2 Features stage 2
O1 Overbook

Authorization Object	Permitted actions
	O2 Overbooking always possible P1 Display list P2 Change date/room P3 Change released dates P4 Release plan U2 Carry out business volume comparison U3 Change business volume comparison U4 Add business volume data UL Upload VP Process VIP
E_CACS_REV	See: E_CACS_ACC
E_CACS_EDT	23 Maintain
E_CACS_SLC	See: E_CACS_ACC
E_CACS_MAS	23 Maintain
E_CACS_BK	01 Add or Create 02 Change 03 Display 85 Reverse
E_CACS_SMC	04 Display
E_CACS_SMA	03 Display
E_CACS_SFC	03 Display
E_CACS_SFA	03 Display
E_CACS_DOC	See: E_CACS_ACC

Authorization Object	Permitted actions
K_KA_RPT	01 Add or Create
	02 Change
	03 Display
	04 Print, Process messages
	16 Execute
	21 Transport
	28 Display single items
	29 Display saved data
	32 Save
	60 Import
	61 Export
	65 Reorganize
	66 Update
	L0 All functions
L1 Features stage 1	
L2 Features stage 2	
K_KA_RCS	01 Add or Create
	02 Change
	03 Display
	21 Transport
	60 Import
	65 Reorganize
B_BUPA_ATT	01 Add or Create
	02 Change
	03 Display
B_BUPA_GRP	01 Add or Create
	02 Change
	03 Display
B_BUPA_FDG	02 Change
	03 Display

Authorization Object	Permitted actions
B_BUPA_RLT	01 Add or Create 02 Change 03 Display
B_CCARD	01 Add or Create 02 Change 03 Display
S_PROJECT	02 Change 03 Display 23 Maintain
S_PROJECTS	70 Manage, administration
V_KONG_VWE	01 Add or Create 02 Change 03 Display
V_KOND_VEA	01 Add or Create 02 Change 03 Display
S_DEVELOP	01 Add or Create 02 Change 03 Display 06 Deletion 07 Activate, Generate 16 Execute 40 Create in database 41 Delete in database 42 Convert in database 71 Manage, administration

13.2.11.4.2 Authorization Types

Use

The authorization types control in detail which actions (such as *Change commission contract*) a commission manager or a commission contract partner may perform in *Incentive and Sales Force Management*.

Features

A differentiation is made between quantifying and qualifying authorization types.

Authorization type	Controls the following:
Quantifying authorization	<ul style="list-style-type: none">• Amounts, quantities, and values in the condition technique
Qualifying authorization	<ul style="list-style-type: none">• Menu and screen options of individual transactions• Authorization for business transactions (in part, already regulated by deactivation of menu options) such as Create, Change, Display• Making Customizing settings
Structural authorization [page 220]	Taking into account structural considerations

13.2.11.4.2.1 Qualifying Authorizations

Use

With qualifying authorizations, the screen structure of individual transactions controls whether a user (depending on the role defined) can only select certain menu options (such as *Create*, *Change*, *Display*, and so on), and/or whether the user may only carry out certain activities within these menu options.

Integration

The qualifying authorization controls which actions each user is allowed to execute in *Incentive and Sales Force Management*.

A **commission manager** generally needs a more complex authorization profile than, for example, a **commission contract partner**, who normally executes fewer activities in the system than a commission clerk.

You must check that the commission manager actually does have authorization to change and display data. Commission clerks can also initiate the calculation of commission rates. They require additional authorizations for this activity.

Features

At the start of each transaction, the system checks the qualifying authorization for various authorization objects.

If the user does not have authorized access, the system issues a warning and the transaction is terminated.

Qualifying authorizations are used in ISF in the processes and activities described below.

SAP EP

The following reference roles are available in SAP EP:

ICM Analyst

The authorization object <E_CACS_STD> checks if the ICM analyst is authorized to edit standard commission contracts.

You can restrict these authorizations depending on the way tasks are assigned in your company.

In addition, the authorization object <E_CACS_BR> checks if the ICM Analyst is authorized to maintain business rules.

ICM Participant

The only authorization query that the system makes is the role assignment of the user management and authentication mechanisms of the SAP NetWeaver platform.

Credentials Manager

The authorization object <E_CRD_PRNT> checks if the credentials manager is authorized to print correspondence.

The authorization object <E_CRD_AS> checks if the credentials manager is authorized to make credential assignments.

SAP Easy Access Menu

The following authorizations are available for the SAP Easy Access menu:

Commission Case

The commission case is divided up into the activities *Create*, *Change*, *Display*, *Undo* and *Reactivate*. These activities have an activity indicator that is queried in the authorization check (1 = Create, 2 = Change, 3 = Display, 85 = Undo). Authorization object <E_CACS_BK> checks these activities.

You can include processing modes (0 - Simulation, 1 - Buffering, 4 - Parking, 6 - To Be Checked, 7 - Reserved for Update (CALC_DATE) and 9 - Final Entry (Post) in the authorization check within the individual processes.

► *Commission Case* ► *Create* ►

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Post commission case: <E_CACS_BK>

► *Commission Case* ► *Change* ►

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Post commission case: <E_CACS_BK>

► *Commission Case* ► *Display* ►

The system checks the following authorization object:

Authorization object <E_CACS_SFC> only permits the *Display* activity.

► *Commission Case* ► *Undo* ►

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Post commission case: <E_CACS_BK>

Release and reverse: <E_CACS_REV>

See Change menu option

► *Commission Case* ► *Reactivate* ►

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Post commission case: <E_CACS_BK>

Pending Cases (General)

A commission manager who has editing authorization also has display authorization.

The same authorizations are required to edit commission cases and pending cases.

► *Pending Cases* ► *Display* ►

The system checks the following authorization object:

Authorization object <E_CACS_SFC> only permits the *Display* activity.

► *Pending Cases* ► *Edit* ►

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Post commission case: <E_CACS_BK>

Document Posting (General)

A user who should have authorization to post documents must have profile <E_CACS_DOCP>.

This profile contains authorization object <E_CACS_DOC>.

If the data for the FI document is to be checked in the target system, the system calls function module **CACS00_TRANSFER_FI_PREPARE**. A user needs the following authorization to execute this function module in the target system:

```
CALL FUNCTION ,AUTHORITY_CHECK_RFC'
```

```
EXPORTING
```

```
USERID = sy-uname
```

```
FUNCTIONGROUP = ,ACC4'
```

```
EXCEPTIONS
```

```
RFC_NO_AUTHORITY = 1
```

Master Data (General)

You maintain master data with the Business Data Toolset (BDT). This includes predefined authorization checks.

The checks are called up between the initial screen and the first data screen, or before the user saves data for the first time. Different authorization types and fields have been defined. Within this authorization, you can define which user may process which fields. Authorization types and related fields are grouped into authorization objects. Within these authorization objects, you can also define activities, such as [Create](#), [Change](#).

Customer-specific field groups have to be checked by customer-specific programs. Nevertheless, existing function modules can still be called to carry out the authorization check.

► [Master Data](#) ► [Commission Contract Partner \(General\)](#) ►

⇒ [Create](#)

⇒ [Change](#)

⇒ [Display](#)

A commission manager who has authorization to edit objects is also automatically authorized to display them.

The system checks the following authorization objects:

Authorization types: <B_BUPA_ATT>

Field groups: <B_BUPA_FDG>

Authorization groups: <B_BUPA_GRP>

Role of commission contract partner: <B_BUPA_RLT>

(The authorization looks for the role of commission contract partner. Payment cards: <B_CCARD>)

► *Master Data* ► *Contract* ▾

⇒ *Create*

⇒ *Change*

⇒ *Display*

The authorization to perform activities on a commission contract is divided into three views that are controlled by their authorization objects.

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Activity for other contracts: <E_CACS_SFC

(The contracts that do not belong to the user currently logged on to the system.)

Activity for your own contracts: <E_CACS_SMC>

(The contracts that belong to the user currently logged on to the system.)

Activity for commission contracts of business partners in managerial positions: <E_CACS_SLC >

The following authorization objects:

<E_CACS_SMC>

<E_CACS_SFC>

<E_CACS_SLC>

are searched for the respective activity:

(01 *Create* , 02 *Change* , 03 *Display*).

In the case of authorization for editing other contracts, the system checks whether the user is a business partner who also has the role of commission clerk. If this is the case, the system takes the PD-Org structure to read all subordinate organizational units and contracts below the organizational unit to which the business partner is assigned as commission clerk.

In the case of authorization for processing own contracts, the system checks the user's own contracts. For a user to be able to view his or her own contracts, the system user must be entered as a business partner in the role of commission contract partner (and also the *User* field). The system user is then able to maintain and display all of the contracts determined on the basis of the above criteria. Users can also maintain and display all the contracts that they themselves have " *parked* " (contracts with "parked" status).

You can, however, get around the structural authorization by assigning authorizations to the object **E_CACS_CTR** .

► *Master Data* ► *Portfolio Assignment* ▾

The system checks the following authorization objects:

Administration in PFO: <E_PFO_ADM>

(Checks the authorizations for administrative activities in portfolio assignment).

Mass activities in PFO: <E_PFO_MAS>

Checks whether the user can start EDT.

Objects in PFO: <E_PFO_OBJ>

Checks whether a user is authorized to access the following programs:

PFO_SEG: Display of segments in PFO

PFO_GZO: Display of business object assignment role

PFO_SZO: Display of assignment role for assignment object

► [Master Data](#) ► [Organizational Plan](#) ►

Assignment: commission contract -PD-Org

When you are working in a commission contract and actively save it, the system checks whether you are authorized to assign a position.

The system checks which organizational unit the clerk is assigned to (user ID and link 290 between organizational unit and position), and whether the organizational unit to be assigned is in the clerk's area of validity.

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Activity for other contracts: <E_CACS_SFC

Activity for your own contracts: <E_CACS_SMC>

Activity for commission contracts of business partners with managerial positions: <E_CACS_SLC >

Personnel planning and development, and structure authorizations: <PLOG> PD

Info Center

⇒ [My Workplace](#)

The system checks the following authorizations as to whether the user who has logged in is a commission clerk:

Authorization object: <S_MWB_FCOD>

Authorization profile: <S_MDT_ALL>

Info Center

⇒ [My Remuneration](#)

No qualifying authorizations objects implemented.

► [Info Center](#) ► [Reports](#) ► [Line Items](#) ►

⇒ [Valuation](#)

⇒ [Remuneration & Liability](#)

⇒ [Settlement](#)

A check is made as to whether the user only sees those contracts for which he/she has authorization, in other words, his/her own contract and those assigned to the user. The system calls data service module **CACS_ORG_PERMISSIONS_ASK** "[Check OU and CContract for Clerk](#)".

If the selection teasers or display fields include field **CTRTBU-ID** , data service module **CACS_READ_DATA** looks for the user's own contract or for authorization to view other contracts.

As with the commission contract, authorization must be given through authorization object **<E_CACS_SMG>**.

Profile **<E_CACS_REP>** also exists. This profile controls authorization for reporting. It includes the following objects: **<K_KA_RPT>**

with the following activities:

01 Add or Generate, 02 Change, 03 Display, 04 Print, Edit Messages, .16 Execute, 21 Transport, 28 Display Line Items, 29 Display Saved Data, 32 Save, 60 Import, 61 Export 65 Reorganize, 66 Update, LO All Functions, L1 Scope of Functions Stage1, L2 Scope of Functions Stage 2 and **<K_KA_RCS>**

with the following activities:

01 Add or Generate, 02 Change, 03 Display, 21 Transport, 60 Import, 65 Reorganize.

In background (batch) processing, the system must save the user ID with the reports that are created. The same authorization checks are made as with online processing.

The reports that are created can be saved. When a user calls a saved document, the system does not check whether the user is permitted to view the data. You should therefore create different reports for each authorization group.

You have to define a *Superuser* role (user with extensive authorization) before you can set up reports.

► [Info Center](#) ► [Reports](#) ► [Totals](#) ►

⇒ [Valuation](#)

⇒ [Remuneration & Liability](#)

⇒ [Settlement](#)

See [Info Center](#) → [Line Items](#)

If the position or the number of the organization unit is part of the ID, the system must check whether the clerk has authorization for the position or organizational unit.

There are two variants:

- Authorization for the organizational unit
- Different reports for each type of organizational unit

► [Info Center](#) ► [Remuneration Inquiry](#) ►

The system checks the following authorization objects:

Application authorization: **<E_CACS_APP>**

Post document: **<E_CACS_DOC>**

Display/change other commission contract: **<E_CACS_SFC>**

Info Center

→ [Display of Settlement Lock](#)

The following authorization object is used: E_CACS_DOC

Administration

►► [Periodic Processing](#) ► [Data Transfer](#) ►

There is no specific authorization check for data transfer. The check depends on the particular process, regardless whether this occurs as a dialog or by EDT.

AdministrationPeriodic ProcessingClosing

⇒ [Flat Rates, Guarantees](#)

⇒ [Guarantee Offsetting](#)

⇒ [Additional Commission Cases](#)

→ [Accruals Notification](#)

The following authorization objects are used:

Authorization for mass processing: **E_CACS_MAS**

Authorization for settlement: <**E_CACS_ACC**>

AdministrationPeriodic Processing

⇒ [Settlement Schedule Run](#)

The following authorization objects are used:

Authorization for mass processing: **E_CACS_MAS**

Authorization for settlement: <**E_CACS_ACC**>

AdministrationPeriodic Processing

⇒ [Settlement](#)

The following authorization objects are used:

Authorization for mass processing: **E_CACS_MAS**

Authorization for settlement: <**E_CACS_ACC**>

AdministrationPeriodic ProcessingCorrespondence

⇒ [Mass Printing](#)

⇒ [History](#)

The following authorization objects are used:

Authorization for mass processing: **E_CACS_MAS**

AdministrationPeriodic Processing

⇒ [Commission Contracts](#)

The system checks the following authorization objects:

See ►► [Master Data](#) ► [End Contracts](#) ►

Administration

⇒ [Current Administration](#)

⇒ [Edit Period Rules](#)

The system checks the following authorization objects:

Administration functions in Change & Transport System: <S_CTS_ADMI>

Table maintenance: <S_TABU_DIS>

AdministrationCurrent Administration

⇒ *Standard Commission Contract*

The system checks the following authorization objects:

Administration functions in Change & Transport System: <S_CTS_ADMI>

Table maintenance: <S_TABU_DIS>

AdministrationCurrent Administration

⇒ *Edit Target Rules*

The system checks the following authorization object:

Target agreements: Authorization to process rules: <E_CACS_TRU>

AdministrationCurrent Administration

⇒ *Lock Agent for Settlement*

The system checks the following authorization object:

Table maintenance: <S_TABU_DIS>

AdministrationCurrent Administration

⇒ *Mass Updating*

Mass data processing is conducted here.

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

Authorization for mass processing: <E_CACS_MAS>

AdministrationCurrent Administration

⇒ *Retroactive Case Processing*

The system checks the following authorization object:

Checks the creation and processing of RCP worklists. <E_CACS_RCP>

The *Activity* and *Commission Application* fields are checked.

AdministrationCurrent Administration

⇒ *Object Transfer*

The system checks the following authorization object:

FOA: Authorization object for accessing Framework for Object Assignment

<E_CACS_OAA>

AdministrationCurrent Administration

⇒ *Unlock Payment*

The system checks the following authorization objects:

Authorization for settlement: <E_CACS_ACC>

Authorization for mass processing: <E_CACS_MAS>

Administration → **Current Administration**

→ *Maintenance of Settlement Lock*

The following authorization object is used: <E_CACS_DOC>

▶ *Administration* ▶ *System Administration* ▶ *Commission Clerk* ▶

⇒ *Create*

⇒ *Authorize*

⇒ *Change*

⇒ *Display*

The authorization must check the role of commission contract partner.

Authorization object <B_BUPA_RLT> must be assigned to users to enable them to process commission clerk master data.

Own check of field group user ID and B_BUPA_FDC.

▶ *Administration* ▶ *System Administration* ▶ *Resetting* ▶

The system checks the following authorization object:

(Authorization for mass processing): <E_CACS_MAS>

Administration → **System Administration** → **Resetting**

⇒ *Data Transfer*

⇒ *Flat Rates, Guarantees*

⇒ *Additional Commission Case*

⇒ *Settlement*

⇒ *Settlement Schedule Run*

→ *Accruals Reversal*

The system checks the following authorization object:

(Authorization for mass processing): <E_CACS_MAS>

Administration → **System Administration** → **Archiving**

⇒ *Commission Cases*

⇒ *Commission Documents*

⇒ *Commission Contracts*

The system checks the following authorization object:

(Authorization for mass processing) <E_CACS_MAS>

AdministrationSystem Administration

⇒ *Parallel Processing*

There is no specific authorization check for parallel processing. The check depends on the particular process.

AdministrationSystem Administration

⇒ *Logs*

No qualifying authorizations objects implemented

AdministrationSystem Administration

⇒ *Area Menus*

A check runs on transaction CACSBDT.

Different authorizations are required for *Display* and *Change* .

⚠ Caution

Only experienced BDT experts should have authorization for this menu option, because this is the menu used to change program flow, screen structure of input screens, and so on.

AdministrationSystem Administration

⇒ *Customizing* (General)

Users with authorization for Customizing also have display and change authorizations.

S_PROJECT: Controls activities related to Customizing projects (*Create*, *Change* and so on).

S_PROJECTS: Superuser authorization in project management.

Authorization object <S_TABU_DIS> handles authorization for views. This object controls whether a clerk can process the views used in Customizing.

Authorization object <E_CACS_APPL> can handle views that are not generated. The system issues a query when you try to start the application.

▶ *Administration* ▶ *System Administration* ▶ *Test* ▶

⇒ *Compare Commission Case*

⇒ *CATT*

No qualifying authorizations objects implemented.

Administration

⇒ *System administration*

⇒ *Individual Settings*

The system checks the following authorization object:

(Authorization for mass processing): <E_CACS_MAS>

Other Qualifying Authorizations

Condition Technique

The system checks the following authorization objects:

Application authorization: <E_CACS_APPL>

The following SD authorization objects are required:

Authorization for condition types and conditions maintenance: <V_KONH_VKS>

Condition generation: Authorization for usage/application. <V_KONG_VWE>

Generator

The generator looks for the following authorization objects:

Administration: <E_CACS_ADM>

Application authorization: <E_CACS_APPL>

Authorization for generator: <E_CACS_GEN>

In the current version the system queries activity 2. A user with authorization for this menu option can also work in change and display mode.

Authorization for namespace conversion

Authorizes user to convert data as a consequence of the namespace change: <E_CACS_NSC> .

The definition of the conversion is not affected by this.

Defined fields CACS_APPL:

Limits the conversion to a specified commission application.

Organizational Management Drilldown

The following authorization objects are used:

Application authorization: <E_CACS_APPL>

Activity for other contracts: <E_CACS_SFC

Activity for your own contracts: <E_CACS_SMC>

Activity for commission contracts of business partners with managerial positions: <E_CACS_SLC >

PD: Personnel planning and development, and structure authorizations: <PLOG>

Financial Accounting

The user requires authorization for the FI area to create documents (for Accounts Receivable/Accounts Payable accounting).

→ Recommendation

SAP recommends that you use the profile generator (transaction **PFCG**) to create authorization profiles).

Business Rule Editor

The system checks authorization object <E_CACS_BR> for the following:

1. Maintenance of rule characteristics for the standard commission contract
2. Individualization of the business rules in the commission contract
3. Binding of business rule data objects for valuation and remuneration

13.2.11.4.2.1.1 Authorization Maintenance Transactions in ISF

The following transactions are required for authorization maintenance in Incentive and Sales Force Management:

Transaction	Description
PFCG	The SU02 transaction has been replaced by the PFCG transaction for Release 4.64 (role maintenance). The roles greatly simplify the creation of authorizations and profiles using the profile generator.
SU25	Copying check indicator standard proposals for authorization objects and authorization field values
SU24	Maintenance of default values
SU01	User maintenance (assignment of profiles)
SU20	Definition of authorization fields
SU21	List of the object classes for creating authorization objects.
SU53	Display of authorization values of individual users

13.2.11.4.2.2 Quantifying Authorizations

Use

By using quantifying authorizations you can impose a control so that commission manager can only enter values up to a certain amount. If a quantifying authorization is overstepped, the commission case receives the status "pending".

Integration

A commission manager is always assigned to a certain authorization group. This group contains the fields required for the quantifying authorization from various tables, along with their values and currencies. Function module CACS_CHECK_QUAN_AUTH reads these values, and compares them with the values entered.

Features

There are four different areas that are relevant for the quantifying authorization:

Commission Contract

In the commission contract, a quantifying authorization was developed for areas:

Flat-rate remuneration

Settlement/payment

Guarantee

The system checks the following fields AMNT, RES_MAX_AMNT, RES_RATE, THRESH_AMNT in tables CACS_REMARU, CACS_RESRULE and CACS_WARRU.

Commission Case/Document Posting

In the commission case, only the fields DREM_CONAMNT, REM_CONAMNT and REM_RATE in table CACS00_LIN are checked.

Document Posting

The total of the remuneration difference amounts/quantities is queried here.

Condition Technique

Absolute, relative, and percentage amounts are checked in the condition technique.

These values are entered in the performance-related remuneration.

Field KBETR_T in structure CACS_S_COND_TC_LINE_BDT is checked.

13.2.11.4.2.3 Structural Authorizations

Use

Following a defined evaluation path, the structural authorization helps you to define those organizational units in a root object that can be displayed to a user.

Features

Always create the validity of commission manager, based on staffing assignments, as being the actual validity periods. For example, if a commission manager is responsible for the regional office in Washington from 1 July 1998 to 31 December 2001, enter these precise dates. During this period the commission manager is responsible for all contracts and cases in his/her organizational structure, even for those that arose or ended before 1 July 1998, provided that at the effective validity end date they are/were still assigned to the organizational unit for which the commission manager currently has authorization (position validity of commission manager).

Incentive and Sales Force Management checks whether the current version of the commission contract is within the responsibility of the commission manager. If you have a pending version of a contract that is correctly assigned to a position or organizational unit, the pending version of the contract is chosen, otherwise the latest active version (in other words, the version with the latest technical validity commencement). The following date is taken for access to the link between the commission contract and PD-ORG (in each case on the basis of the status selected):

- The *processing date*, insofar as "effective from" is < processing date =< "effective to"
- The *"effective from"* date if the processing date is < effective from
- The *"effective to"* date if the processing date is > effective to.

The system selects the staff assignment to a position or organizational unit that is valid on this particular date. The organizational structure (including commission manager position) is evaluated on the basis of the time conditions set in Customizing (standard Customizing; processing date (current date) to an unlimited time in the future). If the commission contract is assigned to the commission manager position under the terms of the time conditions named, this commission manager then has structural authorization.

If the staff assignment ends when the contract legally ends, information on the organizational structure for contract-related processes, which may continue to run after the legal termination, is no longer available. For example, in the settlement process it is no longer possible to get the cost center from PD-ORG. This would lead to error messages after the legal end.

For structural authorization this means that the only solution is to search for the occupied position or organizational unit at an earlier point in time. In the meantime the commission contract could have been assigned to a position or organizational unit in another branch of the organizational structure. Evaluations/statistics that use the organizational structure would not include early cancellation cases processed after the legal termination of the contract, because the staff assignment has already ended.

Contracts that are not assigned to commission managers can be viewed and processed by any commission manager, provided that the commission manager in question has authorization to display and process. In terms of structural authorization this means that all commission commission managers are authorized to view and process commission contracts that are not assigned to the organizational structure.

Activities

You maintain the structural authorizations in the Customizing for Incentive and Commission Management under ► [Authorizations](#) ► [Structural Authorizations](#). ►

For further information, see Maintenance of Structural Authorizations .

13.2.11.4.2.3.1 Editing Structural Authorizations

Use

Authorization profiles are used to control the specific authorizations for personnel planning and development.

Features

You have the following options:

- Maintenance of Structural Profiles
- Assigning Structural Authorization Profiles
- Save user data in the SAP Memory:
Defines the users for which the structural authorization data should be saved in the SAP memory. The main purpose of this function is to avoid performance problems with users that have large authorization profiles.

Activities

You define the structural authorizations in Customizing for *Incentive and Sales Force Management* under [► General Tools ► Authorizations ► Structural Authorization. ►](#)

Define the following data:

Table T77UA "User Authorization"

Attribute	Type	
Key		
MANDT	PK	Client
UNAME	PK	User name
PROFL	PK	Authorization profile
BEGDA	PK	Validity start
Attribute		
ENDDA		Validity end

GEN_FLAG

General flag

Table T77PS "Authorization Profile Texts"

Attribute	Type	
Key		
MANDT	PK	Client
LANGU	PK	Language key
PROFL	PK	Authorization profile
Attribute		
TEXTB		Authorization profile (description)

13.2.11.4.2.3.1.1 Defining Structural Profiles

Features

You can define authorizations for the following areas:

- Planning variants
- Object types
- Object IDs

You can also use the following parameters and functions when defining authorization profiles:

Evaluation paths

By entering a certain evaluation path, you stipulate that a user can only access objects along this evaluation path. If you use an evaluation path, you must make an entry in the object ID field.

Status vector

You can use a status vector to stipulate that a user can only access objects whose link infotypes have a certain status (planned or active, for example).

Level of display

You can use the level of display to stipulate up to which hierarchy level a user can access a structure.

Period

You use this parameter to define the profile that is dependent on the validity period of the structure. For example, if you choose entry D (current day), the structural authorization only applies to the structure valid on the current day. If no date is stated, there is no restriction on the validity period of structures.

Function module

The system uses function modules to determine the root object dynamically at runtime. In this case, you should not fill the object ID field with data, but you must specify the planning variant and object type. The advantage of using function modules is that if you define one single authorization profile, the system creates a user-specific profile on the basis of the dynamic determination of the root object at runtime.

There are two standard function modules:

RH_GET_MANAGER_ASSIGNMENT (determine organizational units for managers)

The root object determined using this function module is the organizational unit to which the user is assigned as manager on the basis of his/her position and the A012 link (is manager of). This function module works on a key date basis. This means that the only organizational units determined as being the root object for a user are those to which he/she is assigned as manager on the date or period selected.

RH_GET_ORG_ASSIGNMENT (organizational assignment)

The root object determined using this function module is the organizational unit to which the user is assigned for organizational purposes.

In addition, you can define profiles that contain a maintenance authorization. To do so, select the *Maintenance* processing type. This means that you can also execute function codes that have the *Maintenance* flag in table T77FC.

Overall authorization arises from the basic authorization and the restriction imposed by structural authorization.

13.2.11.4.2.3.1.2 Assigning Structural Authorizations

Use

You assign the users a specific authorization profile, time-dependently.

Prerequisites

In the previous activity, you defined in the authorization profiles which of the specific authorizations are relevant for the personnel planning and development.

Features

Users are assigned a specific authorization profile that is time-dependent.

You enter the names of generally authorized users in personnel planning and development to whom you need to assign application-specific authorization profiles.

i Note

Users not explicitly mentioned are treated the same as the "SAP" user.

Activities

1. Choose **New Entries**.
2. Enter the user name.
3. Assign the user to the corresponding authorization profile. Enter the authorizations that should be contained in the PD profile. You can make as many entries as you wish. Enter the corresponding authorization key directly or select the authorization profile using the input help (F4).
4. Enter the beginning and end data to define the period in which the authorization profile is valid.

Result

You have assigned the users a specific authorization profile, time-dependently.

13.2.11.4.2.4 Example: Creating a Commission Manager and Assigning Authorizations

Use

A commission manager is responsible for processing commission cases, for which he or she requires the relevant authorizations. In Incentive and Sales Force Management (ISF), both the SAP Authorization Concept as well as the SAP ICM Authorization Concept are used. To check the authorizations of a commission manager, the following relationships have to be established:

1. Between Organizational Management and ISF
2. Between the BP role: commission manager and the SAP user name

Prerequisites

An organizational structure with positions or organizational units for commission contract partners must exist for ISF.

Procedure

1. To create a commission manager, in the main menu of ISF choose ► [Administration](#) ► [System Administration](#) ► [Commission Manager](#) ► [Create](#). Select a business partner category that you wish to create in the BP role: Commission Manager. The Create in BP Role field defaults to [Commission Manager \(New\)](#).

2. Tab page *Address*
Enter the relevant address data.
3. Tab page *Identification*
Enter the SAP user. This establishes the relationship between the commission manager and the SAP user.

Result

You have created a commission manager.

13.2.11.4.2.4.1 Assigning Commission Managers Structural Authorizations

Use

Organization Management allows you to include the commission manager as the owner of a position in the company hierarchy. This fulfills the requirement of assigning the commission manager (quantitative and qualitative) authorizations. The commission manager may only process those commission contracts that are lower in the organizational structure.

Prerequisites

A relationship must have been established between the BP role *commission manager* and the user name (SAP user name). You do this by specifying the USER ID (SAP user name) in the master data of the business partner. See [Example: Creating a Commission Manager and Assigning Authorizations \[page 225\]](#).

Procedure

1. To assign a commission manager a position, in the main menu of ISF choose ► *Master Data* ► *Organizational Plan* ►.
2. ►► *Organization and Staff Assignment* ► (transaction PPOME) or
3. ►► *General Structures* ► (transaction PPSM)
4. For more information, go to the product page for [ABAP Platform and SAP NetWeaver](#), choose your release and then ► *Application Server ABAP - Infrastructure* ► *Other Services* ► *Services for Business Users* ► *Organizational Management* ► *Expert Mode* ► *Organizational Management* ► *Expert Mode* ► *Organizational Management* ►.
5. Under *General Structures*, in the *Object type* and *Object ID* fields enter the data for your organizational unit.

6. Enter the key *CACS_GP* in the *Evaluation Path* field and choose *Enter*.
7. The evaluation path *CACS_GP* shows the chain of relationships ► *Organizational Unit* ► *Position* ► *Person* ►.
8. You can now assign one or more organizational units in the organizational structure to the positions with the *relationship 290 – has administrator*.
9. Now assign the position with the *relationship - 008 holder* to the required commission manager(s).

→ Recommendation

We recommend creating the positions of *commission manager* in a node of the organizational structure that is separate from the organizational units to avoid undesirable side-effects from other functions that are based on Organizational Management.

Result

You have assigned a commission manager structural authorizations. The assigned commission manager can now process all commission contracts of organizational units that are lower in the hierarchy. For more information see Structural Authorization.

13.2.11.4.2.4.2 Assigning Commission Managers Qualifying and Quantifying Authorizations

Use

A commission manager requires qualifying and quantifying authorizations to be able to carry out his or her work in ISF.

Prerequisites

You have created a commission manager and assigned him or her in Organizational Management to an organizational unit, thus establishing the required structural authorizations.

Assigning Commission Managers Qualifying Authorizations

Qualifying authorizations are assigned with the standard SAP authorization concept in ISF.

You access the authorization objects in the initial screen under ► *Tools* ► *Administration* ► *UserMaintenance* ► *Information System* ► *Authorization Objects*. ►

For further information, see the User Information System section of **User and Roles (BC-SEC-USR)** .

→ Recommendation

To create qualifying authorizations, we recommend using the roles of the “PFCG” profile generator.

You access the roles with transaction PFCG.

For further information, see the Role Maintenance section of **User and Roles (BC-SEC-USR)** .

You will find sample standard roles in the commission system under transaction PFCG:

- Single Roles:SAP_ICM_S_*
- Composite Roles:SAP_ICM_C_*

Assigning Commission Managers Quantifying Authorizations

You can assign commission managers quantifying authorizations as well as qualifying ones. In so doing, you restrict the qualifying authorizations to a greater degree.For more information, see Quantifying Authorizations .

Result

You have now assigned the commission manager all the relevant authorizations.

13.2.11.5 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for Incentive and Sales Force Management is based on the topology used by the SAP NetWeaver platform . Therefore, the security guidelines and recommendations described in the SAP NetWeaver security guide also apply to ICM.Details that particularly apply to ICM are described in the following sections:

Communication Channel Security

ISF uses RFC technology and communicates with any number of external systems such as CRM or an (external) policy management system.

The settlement data can be transferred to SAP systems (FI-AP; FI-AR; HR-PY; FS-CD) as well as non-SAP systems.

Network Security

See the product page for [ABAP Platform and SAP NetWeaver](#), choose your release and then ► [Securing the ABAP Platform](#) ► [User Authentication and Single Sign-On](#) ► [Authentication and Infrastructure](#) ► [AS ABAP Authentication Infrastructure](#) ► [Secure Network Communications \(SNC\)](#) ►.

Communication Destinations

The communication destinations are **not** part of the standard delivery of ISF.

13.2.11.6 Virus Protection

Use

If the application saves or transfers data that could contain viruses, you must ensure that there is an interface to a virus scanner.

i Note

For more information on virus protection, see the SAP Service Marketplace under ► service.sap.com/security ► [Security in Detail](#) ► [SAP Security Guides](#) ► [SAP WebAS Security Guide \(aka SAP Security Guide\)](#) ► in the SAP Security Guide, VOLUME II under [Special Topics: Virus Protection and SAP GUI Integrity Checks](#).

13.2.11.7 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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 given system landscape and the applicable legal requirements.

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.

Glossary

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Business 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	Deletion of personal data so that the data is no longer usable.
Retention period	The time period during which data must be available.
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.

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

- Access control: Authentication features as described in section [User Management and Authentication \[page 183\]](#)
- **Authorizations:** Authorization concept as described in section [Authorization Management in Incentive and Sales Force Management \[page 188\]](#)
- **Read access logging:** as described in section [Read Access Logging \[page 233\]](#).
- **Transmission control:** as described in section [Network and Communication Security \[page 228\]](#)
- **Input control:** Change logging is described in the application-specific documentation
- Availability control as described in:
 - Section [Data Storage Security](#)
 - SAP NetWeaver Database Administration documentation
 - SAP Business Continuity documentation in the [SAP NetWeaver Application Help](#) under [Function-Oriented View](#) > [Solution Life Cycle Management](#) > [SAP Business Continuity](#)
 - Separation by purpose: Is subject to the organizational model implemented and must be applied as part of the authorization concept.

⚠ Caution

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate

usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped in Customizing for *Cross-Application Components* under *Data Protection*. Additional industry-specific, scenario-specific or application-specific configuration might be required.

For information about the application-specific configuration, see the application-specific Customizing in SPRO.

13.2.11.7.1 Deletion of Personal Data

The *Incentives and Commissions Management (ICM)* application might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. The *Incentives and Commissions Management (ICM)* solution uses SAP ILM to support the deletion of personal data as described in the following sections. SAP delivers an end of purpose check for the Business Partner created in the *Incentives and Commissions Management (ICM)* application.

All applications register either an end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the business partner or a WUC. For information about the Customizing of blocking and deletion for *Incentives and Commissions Management (ICM)*, see *Configuration: Simplified Blocking and Deletion*.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases.

- **Phase one:** The relevant data is actively used.
- **Phase two:** The relevant data is actively available in the system.
- **Phase three:** The relevant data needs to be retained for other reasons.
For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change a business object that contains blocked data.
- **Create:** It is not possible to create a business object that contains blocked data.

- **Copy/Follow-Up:** It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- **Search:** It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see [Process Flow and Configuration: Simplified Blocking and Deletion](#).

Integration with Other Solutions

In the majority of cases, different installed applications run interdependently.

An example of an application that uses central master data is an SAP for Healthcare (IS-H) application that uses the purchase order data stored in Financial Accounting (FI) or Controlling (CO).

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented solution (EoP)	Further information
EA-APPL	EoP for BP: Function module CACS_ILM_EOP_BP EoP for customer: Class CL_CACS_EOP_CHECK_CUST, method CVP_IF_APPL_EOP_CHECK~CHECK_P ARTNERS EoP for Vendors: Class CL_CACS_EOP_CHECK_VEND, method CVP_IF_APPL_EOP_CHECK~CHECK_P ARTNERS	EoP checks if the purpose of BP, Customer/Vendor with respect to ICM application is over.

Process Flow

1. Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
 - Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA).
 - Run transaction IRMPOL and maintain the required retention policies for the ILM objects of ICM
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.

3. To determine which customer/vendor have reached end of purpose and can be blocked, you do the following:
 - Run transaction BUPA_PRE_EOP to execute the end of purpose check function for the central business partner.
 4. To unblock blocked customer/vendor data, you do the following:
 - Request unblocking of blocked data by using the transaction BUP_REQ_UNBLK.
 - If you have the needed authorization for unblocking business partner data, you can unblock the requested data by running the transaction BUPA_PRE_EOP for the central business partner data.
 5. You delete data by using the transaction *ILM_DESTRUCTION* for the ILM objects of *FSCM Collection Management*.
1. Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
 - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and vendor master in SAP S/4HANA (ILM objects: FI_ACCPAYB, FI_ACCRECV, FI_ACCKNVK).
 2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
 3. To determine which customer/vendor have reached end of purpose and can be blocked, you do the following:
 - Run transaction CVP_PRE_EOP to execute the end of purpose check function for the customer master and vendor master in SAP S/4HANA.).
 4. To unblock blocked customer/vendor data, you do the following:
 - If you have the needed authorization for unblocking business partner data, you can unblock the requested data by running the transaction CVP_UNBLOCK_MD for customer master data and vendor master data in SAP S/4HANA.

For information about how to configure blocking and deletion for *Incentive and Commission Management*, see *Configuration: Simplified Blocking and Deletion*.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for Cross-Application Components under Data Protection.

- Define the settings for authorization management in under ► *Data Protection* ► *Authorization Management* ►. For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for Cross-Application Components under ► *Data Protection* ► *Blocking and Unblocking* ► *Business Partner* ►.

13.2.11.7.2 Read Access Logging

If no trace or log is stored that records which business users have accessed data, it is difficult to track the person(s) responsible for any data leaks to the outside world. The Read Access Logging (RAL) component

can be used to monitor and log read access to data and provide information such as which business users accessed personal data, for example, of a business partner, and in which time frame.

In RAL, you can configure which read-access information to log and under which conditions.

For more information about *RAL, Read Access Logging (RAL)* in the documentation for *SAP NetWeaver* on the SAP Help Portal under <http://help.sap.com>.

13.2.11.8 Revision Security in Incentive and Sales Force Management

Use

Through integration of *Incentive and Sales Force Management* with other SAP components, revision security is achieved in different ways, depending on the SAP component.

Features

Archiving

Incentive and Sales Force Management ensures that master data and transaction data cannot be deleted by using the menu, reports, and so on. This is only possible when using the standard SAP archiving tool.

i Note

For additional information on data archiving, go to the product page for [SAP S/4HANA](#), choose your release and then *Product Assistance*:

- ▶ [Enterprise Technology](#) ▶ [ABAP Platform](#) ▶ [Adminstrating the ABAP Platform](#) ▶ [Administration Concepts and Tools](#) ▶ [Solution Lifecycle Management](#) ▶ [Data Archiving](#) ▶
- ▶ [Enterprise Business Applications](#) ▶ [Finance](#) ▶ [Incentive and Sales Force Management](#) ▶ [Incentive and Commission Management](#) ▶ [Services and Tools](#) ▶ [Tools for Implementing Individual Process Steps](#) ▶ [Archiving in Incentive and Commission Management](#) ▶

Period and Version Management in Incentive and Sales Force Management

The two-dimensional period management ensures revision security for the master data and Customizing data on which the period management is based. This means that the transaction data is automatically secure in terms of revision. For additional information, see the SAP Library under Period and Version Management.

HR Master Data

For information on revision security of HR master data, see the SAP Library under ▶ [Personnel Management](#) ▶ [Personnel Administration](#) ▶ [Procedures in Personnel Administration](#) ▶ [Time Constraints in HR Master Data](#) ▶.

Change Document

Change documents are not used in *Incentive and Sales Force Management* since all relevant activities are logged using the period management tool.

For the business partner (in the roles of commission contract partner, commission manager, and commission recipient), changes are logged using change documents and these can be viewed at any time.

Condition Technique

In *Incentive and Sales Force Management*, revision security is ensured in the condition technique using two-dimensional period management. For additional information, see *Period Management in the Condition Technique*.

(External Data Transfer) Generates a Run Log

The run log contains information on EDT-specific activities in general (log level, number of records processed, information on the runtime, and so on).

The *Incentive and Commission Management* business function can also include process-specific information for each processed commission case in the EDT run log.

This is done using the following function modules:

CACS_MSGEDT

CACSBATCHDISP

Using the Basis Application Log (BAL)

The process logs all activities in the basis application log.

You can specify the level of detail in the log by setting suitable parameters/setting certain parameter IDs:

CACS_MSGDISP

CACS_MSGSTORE

CACS_MSGEDT

CACS_BATCHDISP

13.2.11.9 Procedure Documentation in Incentive and Sales Force Management

Use

Incentive and Sales Force Management offers a range of possibilities for establishing security mechanisms in the system but nonetheless it is not possible to cover all of the security-relevant and organization-specific aspects completely with ISF. In particular, it is down to you to make sure that all security-related requirements are covered with suitable procedure documentation.

→ Recommendation

For example, if a commission manager has access to personal data, the company must have a data protection statement to make sure that the data is not passed on.

13.3 Human Resources

13.3.1 User Management

Use

User management for Human Resources uses the mechanisms provided by *SAP NetWeaver Application Server* (ABAP, Java, or ABAP and Java), for example, tools, user types, and password policies. See the sections below for an overview of how these mechanisms apply to Human Resources. In addition, there is a list of the standard users that are necessary for operating Human Resources.

User Administration Tools

The table below shows the tools for user management in Human Resources.

Tool	Description
User and role maintenance with AS ABAP (transactions SU01 and PFCG)	For more information, look for <i>User Administration and Identity Management in ABAP Systems</i> in the documentation of SAP NetWeaver at http://help.sap.com/netweaver .
User Management Engine	This tool is used for user management of HR portal roles (business packages). For more information, go to https://help.sap.com/s4hana_op_2020 , enter <i>User Management Engine</i> into the search bar, press Enter , and open the search result with that title.

User Types

It is often necessary to specify different security policies for different types of users. For example, it may be necessary that individual users who perform tasks interactively have to change their passwords on a regular basis, but not users who run background processing jobs.

The specific user types that are required for human resources include:

- Individual users
 - Administrator

- Personnel Administration
- Benefits Administration
- Manager
 - Personnel Administration
 - Benefits Administration
 - Compensation Administration
 - Training and Event Management
- Specialists for
 - Personnel Administration
 - Talent Management
 - Benefits Administration
 - Compensation Administration
 - Training and Event Management

- Technical users

Technical users are required for the following business processes:

- WF-BATCH user
If you want to use the workflow functions for the different *Personnel Management* functions, you must create a WF-BATCH system user in the standard system.
- Distribution of master data through ALE technology. For more information, see the documentation for the report RHALEINI (*HR: ALE Distribution of HR Master Data*).
- *Compensation Management* (PA-CM): For the integration with the *Award* function, the technical user requires authorization for the following functions:
 - Call RFC function module HRCM_RFC_LTI_ACCRUALDATA_GET (*Determine awards data for accumulating accruals*)
 - Read the *Award* infotype (0382), authorization object P_ORGIN
- *Budget Management* (PA-PM)
 - You use background processing to create commitments in accounting with a RFC connection. Depending on the process and the system landscape used, it may be necessary to set up a user for the background processing. You can use your own user (an additional logon is required) or set up a special commitment engine user.

For more information about these user types, see the Security Guide for *SAP NetWeaver Application Server ABAP* under <http://help.sap.com/netweaver>.

13.3.2 Authorizations

The authorizations topic plays a fundamental role in the area of Human Resources since access to personnel data must be carefully protected. In SAP Human Resources, there is a two-part concept for setting up authorizations. You should familiarize yourself with this concept if you use Human Resources components.

Human Resources uses the authorization concept provided by **ABAP platform**. Therefore, the security recommendations and guidelines for authorizations detailed in the *ABAP Platform Security Guide* also apply to **Human Resources**.

i Note

Furthermore, Human Resources has specific **structural authorizations** for which the organizational assignment is checked to see whether a user may perform an activity.

For detailed information about authorizations in **Human Resources**, go to https://help.sap.com/s4hana_op_2020, enter *Authorizations for Human Resources* into the search bar, press , and open the search result with that title.

The **ABAP platform** authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF00`) on the **Application Server ABAP**.

Standard Roles

The table below shows the standard roles that are used by the Personnel Management components listed under "Description".

i Note

The standard roles for Human Resources components that are described in a separate chapter of this Security Guide are also in the "Authorizations" section. The same applies to the self-service components [Employee Self-Service \[page 340\]](#) and [Manager Self-Service \[page 355\]](#) that are also described under

▶ [Cross-Application Components](#) ▶ [Self-Services](#) ▶ in this Security Guide.

Standard Roles

Role	Description
SAP_HR_BN*	Roles for the PA-BN (<i>Benefits</i>) component
SAP_HR_CM*	Roles for the PA-CM (<i>Compensation Management</i>) component
SAP_HR_CP*	Roles for the PA-CM-CP (<i>Personnel Cost Planning</i>) component
SAP_HR_OS*	Roles for the PA-OS (<i>Organizational Structure</i>) component
SAP_HR_PA_xx_*	Roles for the international versions and country versions of the PA-PA (<i>Personnel Administration</i>) component
SAP_HR_PA_PF_xx_*	Roles for the PA-PF (<i>Pension Schemes</i>) component
SAP_HR_PD*	Roles for the PA-PD (<i>Personnel Development</i>) component
SAP_HR_RC*	Roles for the PA-RC (<i>Recruitment</i>) component

Role	Description
SAP_HR_REPORTING	Role for the Human Resources Analyst <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p>i Note</p> <p>This role is obsolete. We recommend that you no longer use this role.</p> </div>
SAP_ASR_ADMINISTRATOR	Enhancement of the role SAP_HR_PA_XX_* for the HR administrators that use the functions of the component PA-AS (<i>HR Administrative Services</i>)

For the roles marked with an asterisk (*), several roles exist for each of the components. For roles with xx, where xx represents the SAP country key, various roles exist for each of the country versions.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by *Human Resources*.

i Note

For more information about the authorization objects for Human Resources, see https://help.sap.com/s4hana_op_2020 under [Product Assistance](#) > [Enterprise Business Applications](#) > [Human Resources](#) > [HR Tools](#) > [Authorizations for Human Resources](#) > [Technical Aspects](#) > [Authorization Objects](#).

Most Important Standard Authorization Objects

Authorization Object	Name	Description
P_ORGIN	HR master data	Used to check the authorization for accessing HR infotypes. The checks take place when HR infotypes are edited or read.
P_ORGINCON	HR master data with context	This authorization object consists of the same fields as the authorization object P_ORGIN, and also includes the field PROFIL (structural profile). A check using this object enables user-specific contexts to be mapped in HR master data.

Authorization Object	Name	Description
P_ORGXX	HR master data – extended check	You can use this object to determine that other fields are also to be checked. You can determine whether this check is to be performed in addition to or as an alternative to the <i>HR Master Data</i> authorization check.
P_P_ORGXXCON	HR master data - extended check with context	This authorization object consists of the same fields as the authorization object P_ORGXX, and also includes the field PROFIL (structural profile). A check using this object enables user-specific contexts to be mapped in HR master data
P_TCODE	HR: Transaction Code	This authorization object checks some specific SAP Human Resources transactions.
PLOG	Personnel planning	Determines for which types of information processing a user has authorization.
PLOG_CON	Personnel planning with context	This authorization object consists of the same fields as the object PLOG, and also includes the field PROFIL (structural profile). The check using this object enables user-specific contexts to be mapped.

Authorization Object	Name	Description
P_ASRCONT	Authorization for process content	The Authorization for Process Content object is used by the authorization check for <i>HR Administrative Services</i> . It checks the authorization for access to various process contents and also runs through the authorization objects that you have specified in Customizing in the table T77S0 (see note below). For more information, see https://help.sap.com/s4hana_op_2020 under ▶ <i>Product Assistance</i> > <i>Enterprise Business Applications</i> > <i>Human Resources</i> > <i>Shared Services</i> > <i>HR Administrative Services (PA-AS)</i> > <i>HCM Processes and Forms</i> and section <i>Authorization Concept of HCM Processes and Forms</i> .
P_DEL_PERN	Deletion of personnel numbers in live systems	This authorization object is used in the report RPUDELPP and facilitates the deletion of personnel numbers in live systems. It is used by two roles, one for requesting the deletion and one for performing the deletion. These roles need to be assigned to two different users (double verification principle).
P_EICAU	Authorization for activity in the Employee Interaction Center	This authorization object checks the authorization for editing EIC activities. For more information, see https://help.sap.com/s4hana_op_2020 under ▶ <i>Product Assistance</i> > <i>Enterprise Business Applications</i> > <i>Human Resources</i> > <i>Shared Services</i> > <i>Employee Interaction Center (EIC)</i> > <i>General Settings</i> and section <i>Authorization Concept for Employee Interaction Center (EIC)</i> .

i Note

In Customizing for certain authorization objects, you can specify whether they are to be checked. The table T77S0 in the *Group for Semantic Short Text for PD Plan* AUTSW groups all central switches and settings for the *Human Resources* authorization check. Note that changes to the settings severely affect your authorization concept.

For more information about changing the main authorization switch, see Customizing for *Personnel Administration* and choose ► *Tools* ► *Authorization Management* ►.

13.3.3 Security-Relevant Logging and Tracing

Change documents are created for the infotypes of SAP Human Resources, on the basis of which you can trace changes to infotype data. For more information, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Human Resources* ► *HR Tools* ► in the following sections:

- *Creating Change Documents for Personnel Administration Infotypes*
- *Creation of Change Documents for Personnel Planning Infotypes*

13.3.4 Core HR and Payroll

13.3.4.1 Core HR

About This Chapter

This section of the Security Guide provides an overview of security-relevant information for *Core HR*.

Overview of the Main Sections of This Chapter

The following sections contain the security-relevant information that is specific to Personnel Management:

- *Important SAP Notes*
This section lists the most important SAP Notes for the security of Personnel Management.
- *Authorizations*
This section provides an overview of the authorization concept used for Personnel Management.
- *Communication Channel Security*
This section provides an overview of the communication paths used by Personnel Management and provides information on how you can best protect them.
- *Communication Destinations*
This section provides an overview of the communication destination for the components of Personnel Management and the country-specific components of Personnel Administration.
- *Data Storage Security*
This section provides an overview of the critical data used by Personnel Management, as well as the security mechanisms used.

- [Security for Additional Applications](#)
This section contains information about temporary sequential (TemSe) data storage, which only temporarily stores data from country-specific reports from Personnel Administration.
- [Other Security-Relevant Information](#)
This section contains information about security-relevant Customizing for infotype records and indicates the reports that perform database statistics and consistency checks without checking the user's authorizations.
- Chapter with the security-relevant information for the component [HCM Processes and Forms](#)

13.3.4.1.1 Authorizations

Use

The Personnel Management components use the two-part authorization concept from SAP Human Resources. For more information, see section [Authorizations](#) in the SAP S/4HANA Security Guide for [Human Resources](#) section.

Standard Roles

The table below shows the standard roles that are used by the Personnel Management components.

Role	Description
SAP_HR_OS*	Roles for the PA-OS (Organizational Structure) component
SAP_HR_PA_XX_*	Roles for the international versions and country versions of the component PA-PA (Personnel Administration)

i Note

For the roles marked with an asterisk (*), several roles exist for each of the components. For roles with "xx", where "xx" represents the SAP country key, various roles exist for each of the country versions.

Standard Authorization Objects

The Personnel Management components use the standard authorization objects from SAP Human Resources. For more information about the authorization objects for Human Resources, see SAP Library for SAP S/4HANA on SAP Help Portal at [► Human Resources ► HR Tools ► Authorizations for Human Resources ► Technical Aspects ► Authorization Objects ►](#).

13.3.4.1.2 Communication Channel Security

Use

The table below shows the communication channels used by *Personnel Management*, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Interface Toolbox (Transaction PU12)	ALE	Master data, <i>Benefits</i> data, organizational data as defined by the user	
SAP BW	Extractor program	Master data, organizational data, <i>Personnel Development</i> data	
SAP CO (for distributed systems)	RFC	Cost centers, orders, and so on	Authorizations for CO objects are required here
External files	ASCII	<i>Personnel Administration</i> data	Applicable only for country versions Australia and New Zealand
MS Word	Report interface with SAP NetWeaver		Office Integration
Connection of PDF-based print forms to the archive	HTTP(S)	Person-related data (for example, employee photo)	

DIAG and RFC connections can be protected using *Secure Network Communications* (SNC). The Secure Sockets Layer protocol (SSL protocol) protects HTTP connections.

Note

If you convert the protocol from HTTP to HTTPS and use PDF-based print forms, see SAP Note 1461447.

For more information, see the SAP NetWeaver Security Guide under *Transport Layer Security*.

13.3.4.1.3 Communication Destinations

Use

Specific communication destinations are available for the *Personnel Management* components and *Personnel Administration* country-specific components.

Features

The function group HRPDV_SERVICES contains the following Remote Function Calls (RFCs) for displaying and updating the position attributes. The communication user requires authorization for the authorization object S_RFC to execute Remote Function Calls.

Function Group	Function Module	Description
HRPDV_SERVICES	HRPDV_GET_ROOT_OBJECT	Gets the root object for the user
	HRPDV_ORG_PATHROOTS	Root object specification
	HRPDV_CREATE_POSITION	Creates a new position in the organizational unit
	HRPDV_GET_POSITION_ATTR	Gets the corresponding position attributes
	HRPDV_UPDATE_POSITION_ATTR	Updates the corresponding position attributes
	HRPDV_COPY_POSITION	Copies an existing position and the corresponding attributes several times
	HRPDV_DELIMIT_POSITION	Delimits an existing position
	HRPDV_POSITION_SEARCH	Enables a search for positions based on <i>Object and Data Provider</i> (OADP)
	HRPDV_GET_TIME_CONSTRAINTS	Gets the time constraints information of the corresponding position infotypes and relationships
	HRPDV_TRANSFER_EMPLOYEE	Enables the conversion of an employee from one position to another or creates an additional personnel assignment for the employee
HRPDV_GET_POSITION_F4_HELPS	Returns the input help values for the infotype fields <i>Account Assignment</i> and <i>Employee Subgroup</i>	

Benefits (PA-BN)

When evaluating retirement benefits for employees, service-related data is sent to an external system using IDocs. The Benefits system places the IDocs in a special port. External systems can collect the IDocs from this port. The external systems evaluate the retirement benefits based on the transferred data and then send them with an inbound IDoc back to the SAP system.

There are no special functions from the Benefits system side to protect this data.

Compensation Management (PA-CM)

The self-service scenario *Salary Benchmarking* (HRCMP0053) exchanges data with external benchmarking providers. You communicate synchronously and online using HTTPS protocol (HyperText Transfer Protocol with SSL).

Personnel Administration

- HR Administrative Services
HR Administrative Services can transfer personal data from *SAP E-Recruiting* and return data to *SAP E-Recruiting*. For more information, see the Security Guide for *SAP E-Recruiting* under *Communication Destinations*.
- Pension Fund (PA-PF)
 - You can create files with *SAP List Viewer* (ALV) and TemSe (*Temporary Sequential Objects*).
 - There is no encryption of data in the standard SAP system.

13.3.4.1.4 Data Storage Security

The infotypes in *Personnel Management* contain particularly sensitive data. This data is protected by central authorization objects.

i Note

For more information about authorization objects, see section *Authorizations* in the SAP S/4HANA security guide for *Human Resources*.

Examples of infotypes containing particularly sensitive data:

- International infotypes for *Personnel Administration* (PA-PA)
 - *Personal Data* (0002)
 - *Basic Pay* (0008)
 - *Bank Details* (0009)
 - *Family Member/Dependents* (0021)
- *Personnel Development* (PA-PD)
 - *Qualifications*
 - *Appraisals*
- *Personnel Cost Planning and Simulation* (PA-CP)
 - *Planning of Personnel Costs* (0666), contains salary-based information
- *Management of Global Employees* (PA-GE)
 - *Compensation Package Offer* (0706)

Other sensitive Personnel Management data

- Budget Management
The Budget Management component accesses the salary data of employees and displays data from the Controlling (CO) and Funds Management (FI-FM) components. The standard authorization concept for *Human Resources*, *Controlling*, and *Funds Management* is used for these processes. The following authorization objects are also available to protect the data:
 - P_ENCTYPE (*HR: PBC - Financing*): Determines which funds reservation types a user can access and which activities the user is allowed to perform.
 - P_ENGINE (*HR: Authorization for Automatic Commitment Creation*): Determines which activities a user is allowed to perform when creating commitments.
- Pension Fund (PA-PF)
Access to salary data, pensions, and benefits entitlements is protected by the following authorization objects:
 - P_ORIGIN (*HR: Master Data*)
 - P_CH_CHK (*HR-CH: Pension Fund: Account Access*)
 - P_NL_PKEV(*Bevoegdheidsobject voor PF-gebeurtenissen*)
- Personnel Cost Planning (PA-CM-CP and PA-CP)
The old *Personnel Cost Planning* (PA-CM-CP) and the new *Personnel Cost Planning and Simulation* (PA-CP) components both save salary-relevant information to the clusters of the database PCL5. You can control access rights using the authorization object P_TCODE (*HR: Transaction Code*).
- Employee Interaction Center (PA-EIC)
The *EIC Authentication* infotype (0816) enables question and response pairs to be saved that an agent of *Employee Interaction Center* then uses to identify a calling employee. You can only maintain the infotype with the *Authentication for EIC* Employee Self-Service.
- HR Administrative Services (PA-AS)
The personnel file and all process instances are saved with intermediate statuses and history to the *Case Management* databases.

13.3.4.1.5 Security for Additional Applications

Personnel Administration country-specific components use several reports that store security-relevant and sensitive data. This data includes employee data relating to salary, tax, social insurance, pension contributions, and garnishments.

The data is stored in temporary sequential (TemSe) files and used when printing legal forms, statistics, and business reports. Access to TemSe is controlled by the authorization object S_TMS_ACT. Data encryption is not necessary here. For a list of all reports and programs using TemSe, see the *Personnel Administration* documentation for your country version.

You can also download data directly from the front-end server (for example, PC/terminal) or application server without first storing the data records in the TemSe. To do so, you copy the data to a data carrier that you can then send to the authorities.

13.3.4.16 Other Security-Relevant Information

Use

Other security-relevant Customizing for infotype records

With the field *Access Auth.* (Access Authorization) in table V_T582A (*Infotype attributes (Customizing)*), you can control access to an infotype record depending on whether the record belongs to the area of responsibility of a person responsible on the current date. For more information, see Customizing for *Personnel Management* under ► *Personnel Administration* ► *Customizing Procedures* ► *Infotypes* ► *Infotypes* ▾. Note in particular the help for the *Access Authorization* field.

Technical utilities without integrated authorization check

The following technical utilities read data without the user's authorizations being checked. You should therefore only assign relevant report authorizations to roles containing system administrator functions.

- Reports with the prefix RHDBST*: Database statistics
- Reports with the prefix RHCHECK*: Consistency checks for *Organizational Management* and *Personnel Development* data.

If required, you can use the following reports (developed for SAP internal use) for testing purposes. However, SAP does not accept any responsibility for these reports:

- Report RPCHKCONSISTENCY: (*Consistency check for HR master data*)
- Report RPUSCNTC (*Find Inconsistencies in Time Constraints*)

13.3.4.17 HCM Processes and Forms

About this Document

This chapter provides an overview of the security-relevant information that applies to *HCM Processes and Forms* (PA-AS).

Overview of the Main Sections of This Chapter

The *HCM Processes and Forms* chapter comprises the following sections:

- *Before You Start*
This section contains references to other Security Guides that build the foundation for the *HCM Processes and Forms* chapter and a list of the most important SAP Notes for *HCM Processes and Forms* regarding security.

- [Authorizations](#)
This section provides an overview of the authorization concept that applies to *HCM Processes and Forms*.
- [Internet Communication Framework Security](#)
This section provides an overview of the Internet Communication Framework (ICF) services that are used by *HCM Processes and Forms*.
- [Security for Additional Applications](#)
This section provides information on a Business Add-In (BAI) that can be used for the attachment handling of *HCM Processes and Forms*.
- [Other Security-Relevant Information](#)
This section provides information on the possibility of protecting the Customizing views of *HR Administrative Services* by using a grouping option for the authorization check to prevent users without authorization from maintaining person-related data.

13.3.4.1.7.1 Authorizations

Use

HCM Processes and Forms uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to *HCM Processes and Forms*.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF09`) on the AS ABAP.

i Note

For more information about how to create roles, see section [Role Administration](#) in the SAP Library for *SAP S/4HANA Identity Management*.

Role and Authorization Concept for HCM Processes and Forms

The authorization concept for *HCM Processes and Forms* is described under the section [Authorization Concept of HCM Processes and Forms](#) in the SAP Library for *SAP S/4HANA HCM Processes and Forms*.

Standard Roles

The table below shows the standard roles that are used for *HCM Processes and Forms* authorizations.

Standard Roles for HCM Processes and Forms

Role	Name	Description
SAP_ASR_HRADMIN_SR_HCM_CI_3	HR Administrator: NWBC Role	This single role contains the authorizations for the HR Administrator role.
SAP_ASR_EMPLOYEE_SR_HCM_CI_3	ESS Single Role for HCM PF Services	This single role contains the authorizations for the Employee role in Employee Self-Service (WDA).
SAP_ASR_EMPLOYEE	HR Administrative Services : Employee	This single role contains the authorizations for the Employee role in the <i>Business Package for Employee Self-Service</i> (up to and including 1.4.1).
SAP_ASR_MANAGER	HR Administrative Services : Manager	This single role contains the authorizations for the Manager role.

Note

The Employee and Manager roles use *HCM Processes and Forms*. For security-relevant information regarding these components, see the sections *Employee Self Service* and *Manager Self Service* under *Self Services* in the S/4 HANA Security Guide.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by *HCM Processes and Forms*:

Authorization Object	Name	Comment
S_RFC	Authorization Check for RFC Access	
S_SCMG_CAS	Case Management: Case	These authorization objects manage access to the <i>Process Object</i> of <i>HCM Processes and Forms</i> .
S_SCMG_FLN	Case Management: Authorization by Field	
S_SRMGS_CT	Records Management: Authorizations for Document Content	These authorization objects manage access to the digital Personnel File in the HR Administrator Role.
S_SRMGS_DC	Records Management: Authorization for Documents	
S_SRMGS_PR	Records Management: Authorizations for Attributes	

Authorization Object	Name	Comment
S_SRMSY_CL	SAP Records Management : General Authorization Object	
S_TCODE	Transaction Code Check at Transaction Start	
P_ASRCNT	Authorization for Process Content	This authorization object manages the rights to start and execute processes with <i>HCM Processes and Forms</i> .

13.3.4.1.7.2 Internet Communication Framework Security

Use

You should only activate those services that are needed for the applications running in your system. For *HCM Processes and Forms*, the following services are needed which you can find under the path `default_host/sap/bc/webdynpro/sap/`:

- `asr_form_display`
- `asr_keyword_search`
- `asr_launchpad`
- `asr_mass_start_process`
- `asr_OBJECT_SEARCH`
- `asr_pa_pd_processes_display`
- `ars_personnel_file`
- `asr_processes_display`
- `ASR_PROCESS_EXECUTE_FPM`
- `asr_process_select`
- `ars_profiles_show`
- `asr_srch_pd_process`

Activities

Use the transaction `SICF` to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

More Information

For more information, see [Activating and Deactivating ICF Services](#) in the SAP NetWeaver Library documentation.

13.3.4.1.7.3 Security for Additional Applications

For the uploading of attachments in [HCM Processes and Forms](#) you can use Business Add-In (BAI) HRASR00ATTACHMENT_HANDLING for defining the file types allowed and the maximum size of attachments. For more information, see the BAI documentation in the SAP S/4HANA system.

13.3.4.1.7.4 Other Security-Relevant Information

Authorizations for the Implementation Guide for HR Administrative Services

The views in the Implementation Guide for HR Administrative Services are protected separately by a grouping for the authorization check to prevent users without authorization maintaining person-related data. Under the field name DICBERCLS ([Authorization Group](#)), you can set the following in the authorization object S_TABU_DIS:

- Switch PASC: Authorization check for all views of HR Administrative Services in which no Customizing settings were made that affect authorization checks for the users of HR Administrative Services.
- Switch PASA: Additional authorization check for the views that may affect the authorization check for users of HR Administrative Services.

13.3.4.1.8 Personnel & Organization

About This Chapter

This chapter of the Security Guide provides an overview of the security-relevant information for [Personnel & Organization](#) (PA-PAO).

Role and Authorization Concept for Personnel & Organization

The [Personnel & Organization](#) component uses the following authorization concepts:

- **ABAP Platform authorization concept** (based on assigning authorizations to users based on roles)
For this purpose, the roles mentioned in section [Standard Roles](#) are available as a template. You can copy the standard roles to the customer name space and adjust them to suit your requirements. You use the profile generator (transaction PFCG) to maintain roles.

- Structural Authorizations (HCM-specific authorization concept)
You configure structural authorizations in Customizing for *Personnel & Organization* by choosing the following path: ► *Security* ► *Authorizations* ► *Structural Authorizations* ►.
For more information about the structural authorization check, see *Structural Authorization Check* (in SAP Library for SAP S/4HANA under ► *Human Resources* ► *HR Tools* ► *Authorizations for Human Resources* ►).

Standard Roles

The following standard single roles are available for the *Personnel & Organization* component: *Single Roles for Personnel & Organization*.

Gateway Information

For security information for Gateway, please see:

[Security Settings in the SAP Gateway](#)

The SAP Gateway Foundation Security Guide

Go to https://help.sap.com/s4hana_op_2020, enter *SAP Gateway Foundation Security Guide* into the search bar, press , and open the search result with that title.

13.3.4.2 Payroll (PY)

About This Chapter

This section of the Security Guide provides an overview of security-relevant information for *Payroll* (PY).

Overview of the Main Sections of This Chapter

The chapter “Payroll” comprises the following main sections:

- *Important SAP Notes*
This section lists the most important SAP Notes with regard to the security of Payroll.
- *User Management*
This section provides an overview of the user types required for Payroll.
- *Authorizations*
This section provides an overview of the authorization concept used for Payroll.
Note also the section *Authorizations* for Human Resources overall.
- *Communication Channel Security*
This section provides an overview of the communication paths used by Payroll.
- *Data Storage Security*
This section provides an overview of the critical data used by Payroll, as well as the security mechanisms used.
- *Security for Third-Party Applications or Additional Applications*
This section contains security information that applies for additional applications that are used together with Payroll (for example, the Interface Toolbox or B2A: Communication with Authorities).



- Country-Specific Features
This section contains additional security-relevant information for some country versions.

i Note

The information in the chapter “Payroll (PY)” applies for **all** country versions of Payroll. The country-specific sections only contain **additional** country-specific information, if any exists.

13.3.4.2.1 Important SAP Notes

The following table lists the most important SAP Notes with regard to the security of Payroll.

Title	SAP Note	Comment
Analyzing HR authorizations	902000 	Contains general information about authorizations in the attachments
Q&A: How to customize Payroll Accounting postings in Rel.4.x	116523 	Explains that the display authorizations for posting to Accounting are controlled using the report authorizations (that is, there are no table authorizations)

13.3.4.2.2 User Management

Definition

User management for *Payroll* uses the mechanisms provided by the *SAP Web Application Server* (ABAP), for example, tools, user types, and password policies. For an overview of how these mechanisms apply for *Payroll* , see the sections below. In addition, there is a list of the standard users that are necessary for operating *Payroll* .

User Management Tools

The table below shows the tools to use for user management with *Payroll* .

User Management Tools

Tool	Detailed Description	Prerequisites
User and Role Maintenance (transaction PFCG)	You can use the Role Maintenance transaction PFCG to generate profiles for your <i>Payroll</i> users.	

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

The user types required for *Payroll* include:

- Individual users
 - Administration user
 - Payroll manager
 - Payroll specialist
- Technical users
 - Payroll procedure administrator
 - ALE user for posting payroll results to Accounting

For more information about these user types, see the SAP Web AS ABAP Security Guide under *User Types*.

13.3.4.2.3 Authorizations

Role Concept and Authorization Concept for Payroll

Payroll uses the authorization concept provided by Application Server ABAP, which is based on the assignment of authorizations to users using roles.

The roles named as “standard roles” are available as templates. You can copy the standard roles into the customer-specific namespace and adjust them to suit your requirements. To maintain roles, you use the Profile Generator (transaction PFCG).

Standard Roles

The following table shows examples of standard roles that are used by the *Payroll* component.

Standard Roles

Role	Description
SAP_HR_PY_xx_PAYROLL-ADM	Payroll administrator <xx>
SAP_HR_PY_xx_PAYROLL-MANAGER	Payroll manager <xx>
SAP_HR_PY_xx_PAYROLL-PROC-ADM	Payroll procedure administrator <xx>
SAP_HR_PY_xx_PAYROLL-SPEC	Payroll specialist <xx>
SAP_HR_PY_xx_*	Roles for mapping country-specific tasks within Payroll
SAP_HR_PY_PAYROLL-LOAN-ADM	Loan accounting administrator

xx stands for the country key. For the roles marked with an asterisk (*), additional roles exist for each of the countries.

Standard Authorization Objects

Payroll uses the authorization objects that are usually available for Human Resources. For more information, see *Authorizations*.

The following table shows the security-relevant authorization objects that are also used by Payroll.

Standard Authorization Objects

Authorization Objects	Name	Description	Additional Information
P_PBSPWE	Process Workbench Engine (PWE) authorization	Authorizations for the Process Workbench Engine(PWE)	
P_PCLX	HR: Cluster	Check when accessing HR files on the PCLx (x = 1, 2, 3, 4) databases	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources > Technical Aspects > Authorization Objects > P_PCLX (HR: Cluster) >
P_PCR	HR: Personnel control record	Authorization check for the personnel control record (transaction PA03)	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources > Technical Aspects > Authorization Objects > P_PCR (HR: Personnel Control Record) >
P_PE01	HR: Authorization for personnel calculation schemes	Authorization check for personnel calculation schemes	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources > Technical Aspects > Authorization Objects > P_PE01 (HR: Authorization for Personnel Calculation Schemas) >

Authorization Objects	Name	Description	Additional Information
P_PE02	HR: Authorization for personnel calculation rule	Authorization check for personnel calculation rules	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶ P_PE02 (HR: Authorization for Personnel Calculation Rule) ▶
P_PYEVD0C	HR: Posting document	Protection of actions on payroll posting documents	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶ P_PYEVD0C (HR: Posting Document) ▶
P_PYEVRUN	HR: Posting run	Control of actions that are possible for posting runs	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶ P_PYEVRUN (HR: Posting Run) ▶
P_OCWBENCH	HR: Activities in the Off-Cycle Workbench	Used for the authorization check in the Off-Cycle Workbench.	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶ P_OCWBENCH (HR: Activities in the Off-Cycle Workbench) ▶

Authorization Objects	Name	Description	Additional Information
S_TMS_ACT	Actions on TemSe objects	The authorization determines who may execute which operations on which TemSe objects	SAP Library for SAP S/4HANA under ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶ S_TMS_ACT (TemSe: Actions on TemSe Objects) ▶

For documentation about authorization objects, see SAP Library for SAP S/4HANA and choose [▶ Human Resources ▶ HR Tools ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶](#).

Authorizations for Posting Data to Accounting

The authorization check for posting data to Accounting is performed using report authorizations. This means that the different level of detail of the data comes from calling different reports and can be restricted using corresponding report authorizations.

When posting data to Accounting, the following authorization checks are made:

- Report RPCIPA00
 - Authorization object S_Program, based on report RPCIPA00
 - Authorization object P_PYEVRUN, based on:
 - Run type PP
 - Run information (simulation, productive)
 - Activity (display)
- Report RPCIPS00
 - Authorization object S_Program, based on report RPCIPS00
 - Authorization object P_PYEVD0C, based on:
 - Company code of document
 - Activity (display of contents of posting document)
- Report RPCIPD00
 - Authorization object S_Program, based on report RPCIPD00
 - Authorization object P_PYEVD0C, based on:
 - Company code of document
 - Activity (display of detailed posting information with data related to personnel number)

For more information, see SAP Note 1235291.

13.3.4.2.4 Communication Channel Security

Use

The table below shows the communication channels used by *Payroll*, the protocol used for the connection, and the type of data transferred.

Communication Paths

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Interface Toolbox (Transaction PU12)	ALE, local files	Determined by the user	Salary data, HR master data
Display posting runs (transaction PCP0)	ALE	Data for cost accounting	Salary data (accumulated in part)
Display documents from Accounting	ALE	Documents from Accounting	
Data medium files (creation in Accounting)	Local files	Files for transfer of bank transfers to the banks	Salary data
Display original document for an external wage component in infotype <i>External Wage Components</i> (0579)	RFC	Documents from Accounting	Additional salary data from external systems

RFC connections can be protected using Secure Network Communications (SNC). For more information, see the SAP NetWeaver Security Guide under Transport Layer Security.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

In addition, there is also an authorization check for calling the RFC-capable function module itself (CALL FUNCTION 'AUTHORITY_CHECK_RFC'). For more information, see SAP NetWeaver Library and choose RFC Programming in ABAP.

For more information about the security of ALE connections, see ABAP Platform Security Guide ALE.

13.3.4.2.5 Data Storage Security

Data Storage

The payroll results are saved as compressed to an INDX-like table. In the standard system, access is protected using the read and write authorizations for the infotypes and the authorizations for the required cluster.

The Payroll data and the posting to Accounting are saved to the databases of Application Server ABAP. Payroll uses the standard security concept of AS ABAP for this.

The payroll results in the table `PCL2` are protected using the authorization object `P_PCLX`.

The posting data is stored in the table `PPOIX` and other transparent tables. Access to the posting data is regulated using the report authorizations. For more information, see [Authorizations](#) under [Payroll](#).

⚠ Caution

Data stored in database tables can be displayed using the transactions `SE16` or `SE16N` even **without** an application-specific authorization check. To prevent this, you remove the authorizations for these transactions in productive systems or adjust them accordingly.

For more information, see [Authorization Checks](#) and the Application Server ABAP Security Guide.

Using Logical Paths and File Names to Protect Access to the File System

Payroll saves data in files in the local file system. Therefore, it is important to assign explicit access to the corresponding files in the file system without access to other directories or files (also called directory traversal). This is achieved by entering logical paths and file names in the system that are assigned to the physical paths and file names. This assignment is validated at runtime. If access to a directory is requested that does not correspond to a stored assignment, an error occurs.

The following lists show the logical file names and paths that are used by Payroll, and the reports for which these file names and paths are valid:

Logical File Names and Path Names Used in Payroll

The following logical file names and logical file paths were created using transaction `FILE` to facilitate the validation of physical file names:

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_XX_DIR_RPUFCP01	RPUFCP01	HR_XX_DIR_RPUFCP01

In addition, country-specific logical file names and file paths were created for some country versions. For more information, see the following sections of the Security Guide:

- Country-Specific Features: Canada
- Country-Specific Features: Germany
- Country-Specific Features: Great Britain
- Country-Specific Features: Non-Profit Organizations
- Country-Specific Features: Singapore
- Country-Specific Features: USA
- Country-Specific Features: Other Countries

Activating Validation of Logical Paths and File Names

These logical paths and file names are specified in the system for the corresponding reports. Due to downward compatibility reasons, the validation is deactivated by default at runtime. To activate the validation at runtime,

you maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-dependent). To determine which paths are used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see the following:

- [Logical File Names](#)
- [Protecting Access to the File System](#)
- [Security Audit Log](#)

13.3.4.2.6 Security for Additional Applications

Display of Documents Using Remote Function Call (RFC)

Posting Data to Accounting

Administrators for Accounting can use the transaction `PCPO` (*Display posting runs*) to display posting documents for Human Resources by choosing **► Goto ► Document Overview ► Goto ► Accounting Documents ►**. The administrator requires a user for Human Resources that has the corresponding report authorizations for posting data to Accounting (see *Authorizations* under *Payroll*). You can also deactivate this option by removing the corresponding ALE function module.

Conversely, the authorization check for displaying documents from Accounting must be made from the HR system to Accounting.

External Wage Components

From the *External Wage Components* infotype (0579), users can display the original document for an external wage component. The document is displayed using the function module `HR_PCIF_SHOW_RECEIPT`, which calls an RFC-capable function module in the external system. This function module then has to perform its own checks.

The function module `BAPI_WAGE_COMP_EXT_GET_LIST` is used to display a list of data of the *External Wage Components* infotype (0579). This uses the function module `HR_CHECK_AUTHORITY_INFITY` for the authorization check.

For the detailed view, the function module `BAPI_WAGECOMPEXT_GETDETAIL` is used. This uses the function module `HR_READ_INFOTYPE` for the authorization check.

For more information, see SAP Note 318789.

Interface Toolbox and Outsourcing

The interface toolbox (transaction `PU12`) uses the cluster `IF`. It uses the following authorization objects:

- `P_PCLX`
- `P_PCR`
- `S_TMS_ACT`

- P_PBSPWE

Outsourcing uses ALE and local files with file access using transaction AL11. This is controlled using user exits in the interface toolbox.

In the standard system, Outsourcing uses the logical system FILEPORT. You can use the transaction WE21 to define customer-specific logical systems.

The XML conversion to IDOC is made using the function module OUT_IDOC_XML_TRANSFORM of the function group HROT and the function group IDOC_XML1 (RSIDOCWF). The function module GUI_DOWNLOAD (function group SFES) is also called for the conversion.

Communication with Authorities

For more information, see [B2A: Communication with Authorities](#) .

Payroll Control Center

For more information, see [Payroll Control Center](#) .

TemSe Files

The country versions for Payroll use reports in which sensitive data is displayed. For example, this data can be from the following sensitive areas:

- Salary
- Tax
- Social insurance
- Pension contributions
- Court orders

This data is saved in temporary sequential (TemSe) files. The TemSe process is used for the following purposes:

- To create and output statutory forms, statistics, and analyses
- To download data for the front end server or application server directly, without storing the data as TemSe objects beforehand. The data can then be transferred from the front end server or application server to a data medium that can be transferred to the authorities.
- For posting data to Accounting

⚠ Caution

We recommend you **no longer** use the TemSe process for posting data to Accounting. If you run Accounting and Human Resources in separate systems, we recommend instead that you use Application Link Enabling (ALE). For more information, see SAP Notes 560301, 121614, and 125164.

You can control access to the TemSe objects within the SAP S/4HANA system using the authorization object S_TMS_ACT ([TemSe: Actions on TemSe Objects](#)). Data encryption is not necessary here.

You can find information about the TemSe objects for your country version in the [Payroll](#) documentation for your country version.

13.3.4.2.6.1 B2A: Communication with Authorities

This section of the Security Guide provides an overview of security-relevant information for [B2A: Communication with Authorities](#). [B2A: Communication with Authorities](#) is based on SAP S/4HANA Central Component and Human Resources. Therefore, the corresponding sections in the Security Guide also apply for [B2A: Communication with Authorities](#).

[B2A: Communication with Authorities](#) is used by the following country versions:

- Switzerland
For more information, see [Country-Specific Features: Switzerland](#)
- Germany
For more information, see [B2A: Communication with Authorities \(PY-DE-BA\)](#).
- Great Britain
For more information, see [Country-Specific Features: Great Britain](#)

Underlying Security Guides

Security Guide of Scenario, Application, or Component	Path
Secure Store and Forward (SSF)	SAP NetWeaver Developers' Guide in SAP NetWeaver Library under Secure Store and Forward Mechanism (SSF)
SAP Business Connector (BC)	SAP Business Connector Security Guide
SAP NetWeaver Exchange Infrastructure/Process Integration (XI/PI)	SAP Process Integration (PI) Security Guides

Important SAP Notes

Currently, there are no security-relevant SAP Notes for B2A.

Authorizations

For more information, see [Authorizations](#).

13.3.4.2.6.1.1 Authorizations

Use

B2A: Communication with Authorities uses the authorization concept provided by AS ABAP. Therefore, the security recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to *B2A: Communication with Authorities*.

Roles and Authorization Concept for B2A: Communication with Authorities

Standard Roles

Currently, there are no application-specific roles available.

Standard Authorization Objects

The following table shows the authorization objects relevant for security used by *B2A: Communication with Authorities*.

Standard Authorization Objects

Authorization Object	Field	Value	Description
P_B2A (<i>HR-B2A: B2A Manager</i>)	MOLGA	Country Grouping: Unique identifier for a country, for example, 01 for Germany	You use this authorization object to determine the authorization check for B2A Manager. You need to maintain this authorization object only if you use B2A Manager.
	B2A_WERKS		Authorization Check – Personnel Area
	B2A_BTRTL		Authorization Check – Personnel Subarea
	SAGRP		Area – identifies an application in Human Resources
	DOCTY		Document Type – includes documents of the same type within an area within the framework of the B2A functions

Authorization Object	Field	Value	Description
	B2A_ACTIO		<ul style="list-style-type: none"> • S – Send Messages • D – Detail View for Messages • R – Reorganize Messages • L – Delete Messages • Z – Convert Status of Messages

13.3.4.2.7 Country/Region-Specific Features

The following chapters contain information on country/region-specific features.

13.3.4.2.7.1 Country/Region-Specific Features: Australia

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the country version for Australia (PY-AU, PA-PA-AU), this affects the tax file number (TFN number) in the infotype *TFN Australia* (0227), for example.

More Information

[Payroll \(PY\)](#)

13.3.4.2.7.2 Country/Region-Specific Features: Austria

Overview of security-relevant information for payroll and personnel administration for the local version for Austria.

Authorizations

Standard Authorization Objects

The local version for Austria uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Austria.

For more information, see the following:

- [Authorization](#) (Personnel Management)
- [Authorization](#) (Payroll)

The following table shows the security-relevant objects that are also used in the local version for Austria:

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_AT_BW	BEWID	Statement Identifier Identifies exactly one statement within Statements	This object determines the authorization check within Statements for Austrian Payroll.
	BSUBJ	Functional Area ID for Statements Logical subdivision of statements according to individual topics Values 31-33	
	BACT	<ul style="list-style-type: none"> • E = Creation of Statements • A = Asynchronous Archiving • S = Fast Data Entry/Ad-hoc Query • D = Create Data Records • V = Administrative Archived Statements • Z = Display Archived Statements 	

For the documentation for the authorization objects, see SAP Library for S/4HANA and choose [Human Resources](#) > [HR Tools](#) > [Authorizations for Human Resources](#) > [Technical Aspects](#) > [Authorization Objects](#).

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Austria](#) (PY-AT).

Logical File Names Used in Payroll Austria

The following logical file names were created to help with the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_AT_DATASET_GWB	RPCGWBA2	HR_AT_DATASETS
HR_AT_DATASET_KSB	RPCKSBA0_B2A	HR_AT_DATASETS
HR_AT_ELDA_KSB_1	RPCKSBA0_B2A	HR_AT_DATASETS_ELDA1
HR_AT_ELDA_KSB_2	RPCKSBA0_B2A	HR_AT_DATASETS_ELDA2
HR_AT_PDF_A1_IN	RPCUA1A0_B2A	HR_AT_PDF_A1_IN
HR_AT_PDF_A1_OUT	RPCUA1A0_B2A	HR_AT_PDF_A1_OUT
HR_AT_DATASET_ELDA	<ul style="list-style-type: none">• RPUELDA0• RPUELDA2	HR_AT_DATASETS
HR_AT_DATASET_KSJ	RPUKSJA1	HR_AT_DATASETS
HR_AT_DATASET_SVC	RPUSVCA0	HR_AT_DATASETS_ELDA_SVC_UP
HR_AT_DATASET_SVC_DONE	RPUSVCA0	HR_AT_DATASETS_ELDA_SVC_DONE
HR_AT_DATASET_SVC_ERROR	RPUSVCA0	HR_AT_DATASETS_ELDA_SVC_ERROR
HR_AT_DATASET_GMVS	RPUGVTA0PBS	HR_AT_DATASETS

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Austria, sensitive data includes the social insurance number (SI number) in infotypes *Social Insurance A* (0044) and *Family/Related Persons* (0021)

More Information

See [Payroll \(PY\)](#) in the S/4HANA Security Guide for Human Resources.

13.3.4.2.7.3 Country/Region-Specific Features: Belgium

Overview of security-relevant information for payroll and personnel administration for the local version for Belgium.

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for *Payroll Belgium* (PY-BE).

Logical File Names Used in Payroll Belgium

The following logical file names were created to help with the validation of physical file names:

Logical File Names and Reports Used in Payroll Belgium

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_BE_B2A_AL01	<ul style="list-style-type: none"> RPCSRDB0 RPUSRDB0_MONI 	HR_BE_B2A_AL01
HR_BE_B2A_UN05	<ul style="list-style-type: none"> RPCSRDB0 RPUSRDB0_MONI 	HR_BE_B2A_UN05
HR_BE_B2A_BOWA	<ul style="list-style-type: none"> RPCBWAB0 	HR_BE_B2A_BOWA
HR_BE_B2A_BOWM	<ul style="list-style-type: none"> RPCBWMB0 	HR_BE_B2A_BOWM
HR_BE_B2A_DIMN	<ul style="list-style-type: none"> RPCDIGB0 	HR_BE_B2A_DIMN
HR_BE_B2A_DMFA	<ul style="list-style-type: none"> RPCDMFB0 	HR_BE_B2A_DMFA
HR_BE_B2A_DMUP	<ul style="list-style-type: none"> RPCDUPB0 	HR_BE_B2A_DMUP
HR_BE_B2A_FO_IN	<ul style="list-style-type: none"> RPUSIFB0 	HR_BE_B2A_FO_IN
HR_BE_B2A_FO_OUT	<ul style="list-style-type: none"> RPUSIFB0 	HR_BE_B2A_FO_OUT
HR_BE_B2A_SMFA	<ul style="list-style-type: none"> RPCDMFB0 	HR_BE_B2A_DMFA
HR_BE_B2A_SMPS	<ul style="list-style-type: none"> RPCDMFB0 	HR_BE_B2A_DMFA
HR_BE_UPLOAD_FILE_DMFA	<ul style="list-style-type: none"> RPCDMFB0 	HR_BE_B2A_DMFA
HR_BE_B2A_PY2P	<ul style="list-style-type: none"> RPCDPPB0 	HR_BE_B2A_PY2P

More Information




See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources.

13.3.4.2.7.4 Country/Region-Specific Features: Brazil

Overview of security-relevant information for payroll and personnel administration for the local version for Brazil.

Important SAP Notes

The following table presents the most important SAP Notes regarding security for the local version for Brazil (PA-PA-BR, PY-BR, PY-BR-PS).

Title	SAP Note	Comment
Preparation for INL/3UP Integration of Payroll Posting with Finance in S/4HANA Cloud - HCM Localization for Brazil	2885311 	
eSocial - SOA Manager - configuration of web service for communication to eSocial production environment	2585709 	
eSocial - SOA Manager - configuration of web service for communication to eSocial restricted production environment - web service delivery phase	2514483 	

Authorizations

The local version for Brazil uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Brazil.

Standard Authorization Objects

The local version for Brazil uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

The following table shows the security-relevant authorization objects that are also used in the local version for Brazil.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_EFD_COMP	Company Code (BUKRS)		eSocial: Authorization per company, personnel area/subarea
	Personnel Area (PERSA)		
	Personnel Subarea (BTRTL)		
P_EFD_DELE	Activity (ACTVT)		eSocial: author.ctrl.report employee events and re-proc.batch
P_EFD_EVTY	eSocial event type (EFD_EVTYPE)		eSocial: Authorization for actions by event type
	Activity (ACTVT)		

Communication Channel Security

The following table shows the communication paths that the local version for Brazil uses, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
SOA Manager for eSocial	HTTPS	Employee data and payment data for Brazil	Employee data
Company information from FI module	WebService e RFC (FI)	Company information	
eSocial external monitor	RFC	Employee and payment data for Brazil	Employee data

You can use Secure Network Communications (SNC) to protect RFC connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.75 Country/Region-Specific Features: Bulgaria

Overview of security-relevant information for payroll and personnel administration for the local version for Bulgaria.

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Bulgaria, this includes the unique personal ID (EGN) in the infotypes *Personal Data* (0002) and *Family Member/Dependents*(0021).

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.76 Country/Region-Specific Features: Canada

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#) under *Payroll*.

The following contains specific information about the logical file names and path names for *Payroll Canada* (PY-CA).

Logical File Names Used in Payroll Canada

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names
HR_CA_DIR_CRA_XML_FILE_NAME_APPV	RPCYERK3_XML
HR_CA_DIR_CRA_XML_FILE_NAME_FEND	RPCYERK3_XML
HR_CA_DIR_CRA_XML_SCH_NAME_FEND	RPCYERK3_XML
HR_CA_DIR_MRQ_XML_FILE_NAME_APPV	RPCYERK3_MRQ_XML
HR_CA_DIR_MRQ_XML_FILE_NAME_FEND	RPCYERK3_MRQ_XML

Logical File Name	Reports That Use These Logical File Names
HR_CA_DIR_MRQ_XML_SCH_NAME_APPV	RPCYERK3_MRQ_XML
HR_CA_DIR_MRQ_XML_SCH_NAME_FEND	RPCYERK3_MRQ_XML
HR_CA_DIR_ROE_FILE_NAME	RPCROEK0_DISPLAY_XML
HR_CA_DIR_ROE_FILE_NAME	RPCROEK0_XMPORTER
HR_CA_DIR_XML_FILE_NAME_FEND	RPCXMLK0_VALIDATE
HR_CA_DIR_XML_SCH_NAME_FEND	RPCXMLK0_VALIDATE

Logical Path Names Used in Payroll Canada

The logical file names listed above all use the logical file path `HR_CA_FILE_PATH`.

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Canada, this includes the social insurance number (SNI number) in the infotype *Personal Data* (0002).

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.77 Country/Region-Specific Features: Croatia

Overview of security-relevant information for payroll and personnel administration for the local version for Croatia.

Authorizations

The local version for Croatia uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Croatia.

Standard Authorization Objects

The local version for Croatia uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

The following table shows the security-relevant authorization objects that are also used in the local version for Croatia.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_HR_EROIB	P58_EROIB (OIB company - Tax ID number)		PY-HR: Authorization check for company OIB number
P_HR_RTEEX	REPID (ABAP Program Name)		Croatia: Export Runtime Environment

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Croatia](#) (PY-HR).

Logical File Names Used in Payroll Croatia

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
	HHRCEEB2	HR_HR_PDF

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Croatia, this includes the OIB number in the infotype [Personal Data - Croatia](#) (0562).

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.78 Country/Region-Specific Features: Czech Republic

Overview of security-relevant information for payroll and personnel administration for the local version for Czech Republic

Authorizations

The local version for Czech Republic uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Czech Republic.

Standard Authorization Objects

The local version for Czech Republic uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

The following table shows the security-relevant authorization objects that are also used in the local version for Czech Republic.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_CZ_HI_ID	P18_HIAREA (Usage area - authorization) P18_HI_ID (Insurance contribution payer)		Authorization for the insurance contribution payer (HI)
P_CZ_SI_ID	P18_SIAREA (Usage area - authorization) P18_SI_ID (Insurance contribution payer)		Authorization for variable symbol
P_CZ_RTEEX	REPID (ABAP Program Name)		Czech Republic: Export runtime of the report environment
P_CZ_SOFID	P18_S_OFID (Service office ID)		Service office - public sector
P_CZ_TX_ID	P18_TXAREA(Usage area - authorization) P18_TAX_ID(DIC)		Authorization for DIC
P_CZ_USRIC	P18_TRX_UN(ISPV TREXIMA name) P18_TRX_IC(TREXIMA ICO)		Authorization object for ISPV TREXIMA in B2A

Communication Channel Security

The following table shows the communication paths that the local version for Czech Republic uses, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
ONZ	Internal communication between HR back-end system and CPI: HTTP(S) External communication between CPI and authority: HTTP(S)	Personnel Data	Personnel Data
ELDP	Internal communication between HR back-end system and CPI: HTTP(S) External communication between CPI and authority: HTTP(S)	Personnel Data	Personnel Data
NEMPRI	Internal communication between HR back-end system and CPI: HTTP(S) External communication between CPI and authority: HTTP(S)	Personnel Data	Personnel Data
eNeschopenka	Internal communication between HR back-end system and CPI: HTTP(S) External communication between CPI and authority: HTTP(S)	Personnel Data	Personnel Data
HZUPN	Internal communication between HR back-end system and CPI: HTTP(S) External communication between CPI and authority: HTTP(S)	Personnel Data	Personnel Data

You can use Secure Network Communications (SNC) to protect RFC connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under Transport Layer Security.

Communication Destinations

You can communicate using the 'Field of Study' API. The communication channel is encrypted with 128 Bit SSL. Data is transferred using the protocol HTTPS.

The following table presents an overview of the communication destinations that the local version for Czech Republic uses.

Communication Destinations

Destination	Provided	Type	Description
HR_CZ_OBORY_VZDELANI	No	HTTPS	Field of Study

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Czech Republic](#) (PY-CZ).

Logical File Names Used in Payroll Czech Republic

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_CZ_DIR_DOWNLOAD	RPUTRXT0 RPCZPLT0 RPCZIPT0 RPCTRXT0 RPCREGT2S RPCPEFT1 RPCPEFT0 RPCELDT2TM RPCELDT2S RPCELDT2P RPCELDT2M_09 RPCELDT2MCL_DDP RPCELDT2MCL_09 RPCELDT2MCL RPCELDT2M RPAISPTV	HR_CZ_DIR_DOWNLOAD
HR_CZ_DIR_UPLOAD	RPDOWNT0	HR_CZ_DIR_UPLOAD
HR_CZ_PVS_NEMPRI_FILE_NAME_APP SERV	RPCDNPT9	HR_CZ_PVS_NEMPRI_APPSERV

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_CZ_PVS_NEMPRI_FILE_NAME_FRO NTEND	RPCDNPT9	HR_CZ_PVS_NEMPRI_FRONTEND
HR_CZ_RPCTAXT0_XML_FILE_NAME_A PPSERV	RPCTAXT0 RPCRZNT0	HR_CZ_RPCTAXT0_XML_APPSERV
HR_CZ_RPCTAXT0_XML_FILE_NAME_F RONTEND	RPCTAXT0 RPCRZNT0	HR_CZ_RPCTAXT0_XML_FRONTEND

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Czech Republic, this includes the Birth ID Number in the infotype *Personal Data* (0002).

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.9 Country/Region-Specific Features: Denmark

Authorizations

The country version for Denmark (PA-PA-DK, PY-DK) uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the country version for Denmark.

Standard Authorization Objects

The country version for Denmark uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)

The following table shows the security-relevant authorization objects that are also used in the country version for Denmark.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_DK_PBS	PBSFIRMA	HR_DK (Company Used for PBS)	Authorization check for PBS companies (see P_DK_PBS (HR-DK: Authorization check for access to PBS company))

For the documentation for the authorization object P_DK_PBS, see SAP Library for SAP S/4HANA and choose [► Human Resources](#) > [HR Tools](#) > [Authorizations for Human Resources](#) > [Technical Aspects](#) > [Authorization Objects](#) .

More Information

See [Payroll \(PY\)](#) under SAP S/4HANA Security Guide for Human Resources

13.3.4.2.7.10 Country/Region-Specific Features: Egypt

Overview of security-relevant information for payroll and personnel administration for the local version for Egypt (PA-PA-EG, PY-EG).

Authorizations

The local version for Egypt uses the standard authorization concept of SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to this local version.

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Egypt, this includes the social security number (SINUM) in the **Social Insurance Egypt** (3390) infotype.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

13.3.4.2.7.11 Country/Region-Specific Features: Finland

Overview of security-relevant information for payroll and personnel administration for the local version for Finland.

Communication Destinations

You can exchange data with local servers or terminals for the VET and EEO reports for the local version for Finland. You can use this function to download files from the application server to a presentation server. You then receive the text files required by the authorities with the output format `.txt`. This output format complies with the law.

The data is **not** encrypted in the standard system. It is your decision as to the level of encryption that you want to use if you want to send the data to the Federal Commission or Department of Labor.

The following table presents an overview of the communication destinations that the local version for Finland uses.

Communication Destinations

Destination	Provided	Type	Description
National Incomes Register	For local version for Finland	Personnel data, Income, Company, Details	

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for *Payroll Finland* (PY-FI).

Logical File Names Used in Payroll Finland

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_FI_HPA_QTA	HFILHPA0_FI_DATA	
HR_FI_HPA_ACCR	HFILHPA0_FI_DATA	
HR_FI_DIR_DOWNLOAD	HFISTBC0_SUBR HFISTWC0_FORMS HFUTMS0	

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Finland, this includes the social security number (SSN number) in the infotype *Personal Data* (0002).

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.12 Country/Region-Specific Features: France

Overview of security-relevant information for payroll and personnel administration for the local version for France.

Communication Channel Security

The following channel shows the communication paths that the local version for France uses. Protocols used for the connection, as well as the types of data that are transferred, are also listed.

Communication Paths and Their Protocols

Communication Paths	Protocols Used	Type of Data Transferred
Social declaration GIP-MDS (net-entreprises.fr)	HTTPS	Event and monthly DSN declaration. Anomalies detected by GIP-MDS
BPIJ (ameli.fr)	HTTPS	The amount of IJSS calculated by the administration for your employees
AER (Pole-Emploi.fr)	HTTPS	Official statement signaling the end of a contract and given to the employee
CIBTP (cibtp.fr)	HTTPS	The vacation leave amount calculated by the paid leave fund

Communication Destinations

- Use this function to download files from the application server to a presentation server. You then receive the .txt files required by the authorities with the output format .txt, or .zip.

- Use this function to upload files from the Administration's servers to the application server. You receive files from the Administration with either one of these output formats: `.txt`, `.xml`, or `.pdf`. They include the result of the data checks performed by the authorities and the official forms.

The following table presents an overview of the communication destinations that the local version for France uses.

Communication Destinations

Destination	Provided	Type	Description
Social declaration GIP-MDS (net-entreprises.fr)	For local version France	Consumer Proxy	Service consumer: <ul style="list-style-type: none"> • CO_HRPAYFR_WSP3112_CRMHTTP_OPS • CO_HRPAYFR_WSP3113_CRMHTTP_OPS • CO_HRPAYFR_WSP3114_CRMHTTP_OPS • CO_HRPAYFR_WSV01_05_GIPHTTP_MD • CO_HRPAYFR_WSV01_06_GIPHTTP_MD • CO_HRPAYFR_WSV01_07_GIPHTTP_MD • CO_HRPAYFR_WSV01_08_GIPHTTP_MD • CO_HRPAYFR_WSV01_09_GIPHTTP_MD • CO_HRPAYFR_WSV202213NEOHTTP_GI • CO_HRPAYFR_WSV202214NEOHTTP_GI • CO_HRPAYFR_WSV202311NEOHTTP_GI • CO_HRPAYFR_WSV202312NEOHTTP_GI
BPIJ (ameli.fr)	For local version France	Consumer Proxy	Service consumer: <ul style="list-style-type: none"> • CO_HRPAYFR_WSV0203_BPIJWWW_02 • CO_HRPAYFR_WSV0204_BPIJWWW_02
AER (Pole-Emploi.fr)	For local version France	.PDF file	The PDF file is linked to the employee from the B2A status handler and infotype <i>B2A Follow-up</i> (3331).

Destination	Provided	Type	Description
CIBTP (cibtp.fr)	For local version France	Consumer Proxy	Service consumer: <ul style="list-style-type: none"> CO_HRPAYFR_WSV02_01_GIPHTTP_MD CO_HRPAYFR_WSV02_02_GIPHTTP_MD CO_HRPAYFR_WSV02_03_GIPHTTP_MD

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for *Payroll France* (PY-FR).

Logical File Names Used in Payroll France

The following logical file names were created to help with the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names
HR_FR_AER_FILE	<ul style="list-style-type: none"> RPUDSNF1
HR_FR_DSN_DSN_START_XLS	<ul style="list-style-type: none"> RPCDSNF0 RPCDSNF0_REM_HOURS RPCDSNF0_REM_HOURS_LAG RPUDSN_PP_SETUP_F0
HR_FR_DSN_DSN_VAL_FILENAME	<ul style="list-style-type: none"> RPCDSNF0 RPUDSNF1
HR_FR_DSN_DSN_VAL_FILENAME_PASRAU	<ul style="list-style-type: none"> RPCDSNF0 RPUDSNF1
HR_FR_DSN_WEB_RESPONSE	<ul style="list-style-type: none"> RPUDSNF1
HR_FR_IT16_MIGRATION_DOWNLOAD	<ul style="list-style-type: none"> RPCI16F0
HR_FR_IT16_MIGRATION_UPLOAD	<ul style="list-style-type: none"> RPCI16F0
HR_FR_PAS_SITUATION_PDF	<ul style="list-style-type: none"> RPLPASF1
HR_FR_RPLPASF0_XLS	<ul style="list-style-type: none"> RPLPASF0

Logical File Name	Reports That Use These Logical File Names
HR_FR_RPUTIRFX_CSV	<ul style="list-style-type: none"> • RPUTIRF0 • RPUTIRF1 • RPUTIRF2
HR_FR_DSN_DSN_ANO_XLS	<ul style="list-style-type: none"> • RPUDSNF1

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for France, sensitive data includes the social security number (NIR number) in infotype *Personal Data* (0002).

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources.

13.3.4.2.7.13 Country/Region-Specific Features: Germany

Authorizations

The local version for Germany (Payroll and/or Personnel Administration) uses the standard authorization concept used by S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for S/4HANA also apply to the local version for Germany (PY-DE, PA-PA-DE).

Standard Roles

The following table shows the standard roles that the local version for Germany also uses.

Standard Roles

Role	Description
SAP_AUDITOR_TAX_HR	Role HR-DE Audit § 147 AO (Template) for Personnel Administration Germany (PA-PA-DE)

Standard Authorization Objects

The local version for Germany uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

The following table shows the security-relevant authorization objects that are also used in the local version for Germany.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_DBAU_SKV HR: DBAU: Construction Industry Germany - Social Fund Procedure	ACTVT	<ul style="list-style-type: none"> Add or Create Display Delete 	<p>This object is only used in Construction Pay Germany and then only within the framework of the report for the social fund procedure. A check is made as to which reports are to be run by an administrator using which parameters or worksteps.</p> <p>For more information, see SAP Library for S/4HANA under P_DBAU_SKV (HR: DBAU: Construction Pay Germany – Social Fund Procedure)</p>
	REPID	ABAP Report Name: Contains the name of a report in which the authorization object is checked, for example, the evaluation report for the social fund procedure. The authorization granted applies only to this report.	
	RZNUM	Data Center Number for Construction Industry Social Fund Determines the data center numbers to which a granted authorization applies	
	ZVKAS	Social Fund Determines the social funds for which a granted authorization applies	
P_DE_BW HR-DE: SAPScript Statements	BEWID	Statement Identifier Identifies exactly one statement within Statements	<p>This object determines the authorization check within Statements (with SAPScript) for German Payroll.</p> <p>For more information, see SAP Library for S/4HANA under P_DE_BW (HR-DE: Statements SAPScript)</p>

Authorization Object	Field	Value	Description
	BSUBJ	Functional Area ID for Statements Logical subdivision of statements according to individual topics Values 01–04	
	BACT	<ul style="list-style-type: none"> • E = Creation of Statements • A = Asynchronous Archiving • S = Fast Data Entry/Ad-hoc Query • D = Create Data Records • V = Administrative Archived Statements • Z = Display Archived Statements 	

For the documentation for the authorization objects, see SAP Library for S/4HANA and choose [Human Resources](#) > [HR Tools](#) > [Authorizations for Human Resources](#) > [Technical Aspects](#) > [Authorization Objects](#).

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Germany](#) (PY-DE).

Logical File Names Used in Payroll Germany

The following logical file names and logical file paths were created to facilitate the validation of physical file names:

Logical File Names, Reports, and File Paths

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_DE_DIR_B2A_KK_ZERTLIST	RPUSVKD0	HR_DE_B2A_KK_ZERTLIST
HR_DE_DIR_B2A_KK_ZERTREQUEST	RPUSVKD0	HR_DE_B2A_KK_ZERTREQUEST
HR_DE_DIR_B2A_KK_ZERTRESPONSE	RPUSVKD0	HR_DE_B2A_KK_ZERTRESPONSE

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_DE_DIR_RBM_IN	RPCRBMD0_INBOUND	HR_DE_DIR_RBM_IN
HR_DE_DIR_RBM_OUT	RPCZFADD_INBOUND	HR_DE_DIR_RBM_OUT
HR_DE_DIR_RBM_PRO	RPCRBMD0_INBOUND	HR_DE_DIR_RBM_PRO
HR_DE_DIR_RPCAODD0	RPCAOPD0 RPCOADD0	HR_DE_TX_DATENUEBERLASSUNG_PFA D
HR_DE_DIR_RPCEHBD0	RPCEHBD0	HR_DE_DIR_RPCEHBD0
HR_DE_DIR_RPCEHCD1	RPCEHCD1	HR_DE_DIR_RPCEHCD1
HR_DE_DIR_RPCEHFD0	RPCEHFD0	HR_DE_DIR_RPCEHFD0
HR_DE_DIR_RPCSVGD0	RPCSVGD0	HR_DE_DIR_RPCSVGD0
HR_DE_DIR_RPLEHAD3	RPLEHAD3	HR_DE_DIR_RPLEHAD3
HR_DE_DIR_RPSKGOD0	RPSKGOD0	HR_DE_DIR_RPSKGOD0
HR_DE_DIR_RSPSDD0	RSPSDD0	HR_DE_DIR_RSPSDD0
HR_DE_DIR_RPURZBD0	RPURZBD0	HR_DE_DIR_RPURZBD0
HR_DE_DIR_RPUTXCD0	RPUTXCD0	HR_DE_TX_RPUTXED0_PFAD
HR_DE_DIR_RPUTXED0	RPUTXED0	HR_DE_TX_RPUTXED0_PFAD
HR_DE_DIR_RPUVEODD	RPUVEODD	HR_DE_DIR_RPUVEODD
HR_DE_DIR_RPUWEDDA	RPUWEDDA	HR_DE_DIR_RPUWEDDA
HR_DE_DIR_RPUZVCD2	RPUZVCD2	HR_DE_PBSZV2006_NOTIFS
HR_DE_DIR_RPUZVTD2	RPUZVTD2	HR_DE_PBSZV2006_NOTIFS
HR_DE_DIR_RPXKHS0	RPXKHS0	HR_DE_DIR_RPXKHS0
HR_DE_DIR_ZFA_INCOMING	RPCZFADD_INBOUND	HR_DE_DIR_ZFA_INCOMING
HR_DE_DIR_ZFA_OUTGOING	RPCZFADD_INBOUND	HR_DE_DIR_ZFA_OUTGOING
HR_DE_DIR_ZFA_PROCESSED	RPCZFADD_INBOUND	HR_DE_DIR_ZFA_PROCESSED
HR_DE_B2A_KK_PSE	RPUSVHD1	HR_DE_B2A_KK_PSE_PSE
HR_DE_DIR_RPSHSTD0	RPSHSTD0	HR_DE_DIR_RPSHSTD0
HR_DE_DIR_RSPAYDE_KHSTAT	RSPAYDE_KHSTAT	HR_DE_DIR_RSPAYDE_KHSTAT

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_DE_DIR_RPSPAYDE_REGISTERZEN SUS	RPSPAYDE_REGISTERZENSUS	HR_DE_DIR_RPSPAYDE_REGISTERZEN SUS
HR_DE_DIR_RPSVEOD0	RPSVEOD0	HR_DE_DIR_RPSVEOD0
HR_DE_DIR_RPUAGODD	RPUAGODD	HR_DE_DIR_RPUAGODD
HR_DE_DIR_RPLEHBD0	RPLEHBD0	HR_DE_DIR_RPLEHBD0
HR_DE_DIR_RP_HRPAYDE_EHVM	RP_PAYDE_EHVM_CREATE_FILES	HR_DE_DIR_RP_HRPAYDE_EHVM
HR_DE_DIR_Z4	RPCZ4VD0	HR_DE_DIR_Z4_PATH
HR_DE_HOME_ECATT_ANY	Verzeichnis für automatisierte Tests (z.B. eCATT)	HR_DE_HOME_ECATT_ANY
HR_DE_HOME_ECATT_FURTHER	Drittes Verzeichnis für automatisierte Tests (z.B. eCATT)	HR_DE_HOME_ECATT_FURTHER
HR_DE_HOME_ECATT_OTHER	Zweites Verzeichnis für automatisierte Tests (z.B. eCATT)	HR_DE_HOME_ECATT_OTHER
HR_DE_KGBA_XML	RPC_PAYDE_KGBA_XML	HR_DE_KGBA_XML
HR_DE_KGID_IN	RPCKGVD0_IN	HR_DE_KGID_IN
HR_DE_KGID_OUT	RPCKGVD0_OUT	HR_DE_KGID_OUT
HR_DE_KGID_PRO	RPCKGVD0_IN	HR_DE_KGID_PRO
HR_DE_PBSZV2006_NOTIFS_FILENAM E	RPUZVTD2	HR_DE_PBSZV2006_NOTIFS
HR_DE_PBSZV2006_RESPONSES_FILE NAME	RPUZVRD2_IN	HR_DE_PBSZV2006_RESPONSES
HR_DE_RPCEHFD0	RPCEHFD0	HR_DE_DIR_RPCEHFD0
HR_DE_TX_DATENUEBERLASSUNG_DAT EINAME	RPCAOQD0	HR_DE_TX_DATENUEBERLASSUNG_PFA D
HR_DE_TX_RPUTXED0_DATEINAME	RPUTXED0	HR_DE_TX_RPUTXED0_PFAD
HR_DE_ZFA_OUTGOING	RPCZFAD0_OUTBOUND	HR_DE_DIR_ZFA_OUTGOING

Related Information

[Payroll \(PY\) \[page 253\]](#)

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

13.3.4.2.7.13.1 B2A: Communication with Authorities (PY-DE-BA)

This section of the Security Guide provides an overview of security-relevant information for [B2A: Communication with Authorities \(PY-DE-BA\)](#).

References to Cross Chapters

[B2A: Communication with Authorities \(PY-DE-BA\)](#) is based on SAP S/4HANA, Human Resources, or Personnel Management. Therefore, the corresponding Security Guides also apply to [B2A: Communication with Authorities \(PY-DE-BA\)](#). Note in particular the most important sections or specific restrictions that are entered in the following table.

Underlying Security Guides

Security Guide of Scenario, Application, or Component	Path
Secure Store and Forward (SSF)	SAP NetWeaver Developers' Guide in SAP NetWeaver Library under Secure Store and Forward Mechanism (SSF)
SAP Business Connector (BC)	SAP Business Connector Security Guides
SAP Process Integration / SAP Process Orchestration (PI/PO)	SAP Process Integration Security Guides
SAP Cloud Integration (CI)	SAP Cloud Integration Security Guide

Important SAP Notes

Currently, there are no security-relevant SAP Notes for B2A.

Configuration

For information about the general settings for setting up [B2A: Communication with Authorities \(PY-DE-BA\)](#), see Customizing for Payroll under [► Payroll: Germany ► Communication with Authorities \(B2A\) ►](#).

Data Flow and Process

- ELSTER: The data is encrypted and signed before being transferred to the tax authorities.
- eSTATISTIK.core: The data is encrypted (HTTPS) before being transferred to the statistical authorities.
- SI (DEUEV, ...): The data is encrypted and signed before being transferred from the HR system to the health insurance fund or pension insurance fund.
- ZfA/PRN: The data is encrypted (VPN) before being transferred to the authority.

Authorizations

For more information, see [Authorizations](#) under *B2A: Communication with Authorities*.

13.3.4.2.7.13.1.1 Communication Channel Security

Use

The following table shows the communication paths that *B2A: Communication with Authorities* (PY-DE-BA) uses, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
ELSTER	HTTP Internal: HR system -> Middleware (BC or PI/PO): Communication channel RFC Middleware (CI): Communication channel HTTPS External: Middleware (BC, CI, PI/PO) -> Tax authorities: Communication channel HTTPS	Personnel data	Person-related data
eSTATISTIK.core	HTTPS	Personnel data	Person-related data
SI (DEUEV, ...)	HTTP/E-mail	Personnel data	Person-related data
ZfA/PRN	VPN	Personnel data	Person-related data

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under Transport Layer Security.

Communication Destinations

The following table provides an overview of the communication destinations that *B2A: Communication with Authorities* (PY-DE-BA) uses.

Destination	Provided	Type	Description
HR_DE_ELSTER	No	RFC/HTTPS	Transfer of data for EL-STER to middleware (BC, CI, PI/PO)
HR_DE_ECORE	No	HTTPS	Transfer of data for statistical data (Earnings Survey)
HR_DE_GKV, HR_DE_RVBEA, HR_DE_DSVV, HR_DE_DSRV	No	HTTPS	Transfer of data for GKV/DSRV to health insurance
HR_DE_ZFA, HR_DE_RBM_BC	No	RFC	Transfer of data for ZFA to middleware (BC, PI/PO)

Security-Relevant Logging and Tracing

- ELSTER: Tracing for error analysis using BI/BC is possible.
- eSTATISTIK.core: Tracing for error analysis using ICM (transaction: SMICM) is possible.
- SI (DEUEV, ...): Tracing for error analysis using ICM (transaction: SMICM) is possible.
- ZfA/PRN: Tracing for error analysis using ICM (transaction: SMICM) is possible.

13.3.4.2.7.14 Country/Region-Specific Features: Greece

Overview of security-relevant information for payroll and personnel administration for the local version for Greece.

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for *Payroll Greece* (PY-GR).

Logical File Names Used in Payroll Greece

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
	HGRLE2T0	HR_GR_DIR_DOWNLOAD

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Greece, this includes the AFM tax registration number (AFM) in the infotype 3219 and the AMKA Social security number (AMKA) and the IKA Social security number (RGIKA) in the infotype 3220.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.15 Country/Region-Specific Features: Hungary

Overview of security-relevant information for payroll and personnel administration for the local version for Hungary (PY-HU).

Authorizations

The local version for Hungary uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Hungary.

Standard Authorization Objects

The local version for Hungary uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Hungary \(PY-HU\)](#).

Logical File Names Used in Payroll Hungary

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names, Reports, and File Paths

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_HU_DIR_RPC100HX	RPC100H0	HR_HU_DIR_RPC100HX
HR_HU_DIR_RPCBBAHX	RPCBBAH0 RPUBBAH0	HR_HU_DIR_RPCBBAHX
HR_HU_DIR_RPCBBMHX	RPCBBMH0	HR_HU_DIR_RPCBBMHX
HR_HU_DIR_RPCBNKHX	RPCBNKHM RPCBNKH0	HR_HU_DIR_RPCBNKHX

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_HU_DIR_RPCCHQHX	RPCCHQH0	HR_HU_DIR_RPCCHQHX
HR_HU_DIR_RPCCSTHX	RPCCSTH4 RPCCSTH5	HR_HU_DIR_RPCCSTHX
HR_HU_DIR_RPCJFGHX	RPCJFGH3	HR_HU_DIR_RPCJFGHX
HR_HU_DIR_RPCJFMHX	RPCJFMH1	HR_HU_DIR_RPCJFMHX
HR_HU_DIR_RPCLKKHX	RPCLKKH0 RPCLKKH1	HR_HU_DIR_RPCLKKHX
HR_HU_DIR_RPCNEGHX	RPCNEGH2 RPCNEGH3 RPCNEGH4	HR_HU_DIR_RPCNEGHX
HR_HU_DIR_RPCNETHX	RPCNETH2 RPCNETH3	HR_HU_DIR_RPCNETHX
HR_HU_DIR_RPCSVBHX	RPCSVBHN RPCSVBHO RPCSVBHO_HK RPCSVBHO_MB	HR_HU_DIR_RPCSVBHX
HR_HU_DIR_RPCTBZHX	RPCTBZH6	HR_HU_DIR_RPCTBZHX
HR_HU_DIR_RPLM30HX	RPLM30HP RPLM30HQ RPLM30HR RPLM30HR_13 RPLM30HR_15 RPLM30HR_307 RPLM30HR_OLD RPLM30HR_PRE18	HR_HU_DIR_RPLM30HX

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_HU_DIR_RPLVAXHX	RPLVAXH0	HR_HU_DIR_RPLVAXHX
HR_HU_DIR_RPSMKFHX	RPSMKFH2	HR_HU_DIR_RPSMKFHX
HR_HU_DIR_RPUCHRHX	RPUCHRH0	HR_HU_DIR_RPUCHRHX
HR_HU_DIR_RPULKTHX	RPULKTH0	HR_HU_DIR_RPULKTHX
HR_HU_DIR_RPURTAHX	RPURTAH0	HR_HU_DIR_RPURTAHX
HR_HU_DIR_RPUSTDHX	RPUSTDH0	HR_HU_DIR_RPUSTDHX
	RPUSTDH3	

Particularly Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Hungary, this includes the personal tax number in the infotype *Tax H (0163)* and SI ID in the infotype *Contribution H (0164)*.

More Information

See *Payroll (PY)* under SAP S/4HANA Security Guide for Human Resources

13.3.4.2.7.16 Country/Region-Specific Features: Ireland

Overview of security-relevant information for payroll and personnel administration for the local version for Ireland (PY-IE, PA-PA-IE).

Authorizations

The local version for Ireland uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Ireland.

Standard Authorization Objects

The local version for Ireland uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)
- [Authorizations](#) (B2A: Communication with Authorities)

Communication Channel Security

The following table presents the communication paths used by the local version for Ireland (PY-IE, PA-PA-IE) for [B2A: Communication with Authorities](#), the protocol used by the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Smart PAYE	Internal communication between HR back-end system and middleware (CPI): HTTP(S) External communication between CPI and tax authorities: HTTP(S)	Personnel Data	Personal-related Data

HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

i Note

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under Transport Layer Security.

For more information about B2A security, see [B2A: Communication with Authorities](#).

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Ireland \(PY-IE\)](#).

Logical File Names Used in Payroll Ireland

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names, Paths, and Reports

Logical File Name	Logical File Path	Reports That Use These Logical File Names
HR_IE_DIR_CMAP	HR_IE_DIR_CMAP	HIECEOY0
HR_IE_DIR_HIECEELO	HR_IE_DIR_FILEPATH	HIECEELO
HR_IE_DIR_HIECNRR0	HR_IE_DIR_FILEPATH	HIECNRR0
HR_IE_DIR_HIECPAY0	HR_IE_DIR_FILEPATH	HIECPAY0
HR_IE_DIR_HIECRPN0	HR_IE_DIR_FILEPATH	HIECRPN0

Particularly Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Ireland, this includes the PPS number in the infotype *Personal Data* (0002).

More Information


See [Payroll \(PY\)](#) under SAP S/4HANA Security Guide for Human Resources

13.3.4.2.7.17 Country/Region-Specific Features: Italy

Overview of security-relevant information for payroll and personnel administration for the local version for Italy.

Important SAP Notes

The following table presents the most important SAP Notes regarding security for the local version for Italy (PA-PA-IT, PY-IT).

Title	SAP Note	Comment
Change of master data in a productive payroll	385319 	

Authorizations

The local version for Italy uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Italy.

Standard Authorization Objects

The local version for Italy uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)

Country/Region-Specific Authorization Objects

The following table shows the security-relevant authorization objects that are also used in the local version for Italy.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_IT_UERST	P_RESET (Reject posting for social insurance)		Authorization for termination of social insurance (report RPCUED10)
P15_MATRIC	ACTVT (Activity) P15_MODMN (Calculation grouping DM10) P15_INPSC (INPS Indicator)		Authorization for reading, creating, changing, and deleting UniEmens cluster data
PAYIT_CUD	ACTVT (Activity) BUKRS (Company Code) PERSA (Personnel Area) BTRTL (Personnel Subarea) PERSG (Employee Group) PERSK (Employee Subgroup)		Authorization for adding, creating, displaying, and locking Certificazione Unica cluster data

Related Information

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.18 Country/Region-Specific Features: Japan

Overview of security-relevant information for payroll and personnel administration for the local version for Japan (PA-PA-JP, PY-JP).

Authorizations

The local version for Japan uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Japan.

Standard Authorization Objects

The local version for Japan uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

The following table shows the security-relevant authorization objects that are also used in the local version for Japan.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_22_INMAO	P22INMROLE (Role Definition for Individual Number Authorization)		Authorization to Individual Numbers
	P22CPNMFRO (Corporate Number Modifier)		

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Japan, this includes the individual number in the *Individual Numbers JP* (3386) infotype.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.19 Country/Region-Specific Features: Kazakhstan

Overview of security-relevant information for payroll and personnel administration for the local version for Kazakhstan.

Authorizations

The local version for Kazakhstan (PA-PA-KZ, PY-KZ) uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Kazakhstan.

Standard Authorization Objects

The local version for Kazakhstan uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations \[page 243\]](#) (Personnel Management)
- [Authorizations \[page 255\]](#) (Payroll)

The following table shows the security-relevant authorization objects that are also used in the local version for Kazakhstan.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Description
P_KZ_EHRUI	P_RMS_REPT (Report type)	Kazakhstan e-HR: Authorization checks
	P_RMS_REPA (Reporting area)	
	P_EHR_CLCA (Class category for e-HR Kazakhstan)	
	P_EHR_OPER (Operation ID)	
P_RMS_RSE	P_RMS_REPA (Reporting area)	HR-CIS: Authorization for operations with RMS Reporting Session
	P_RMS_REPT (Report type)	
	P_RMS_OPER (Processing level operation)	
P_RMS_SDC0	P_RMS_CTYP (Entity type)	HR-CIS: Authorization for operations with RMS records
	P_RMS_REAA (Reporting unit/area)	
	P_RMS_GREER (Employer)	
	P_RMS_ACTV (Activities with RMS entity)	

Authorization Object	Field	Description
P_RMS_SDD0	P_RMS_DTYP (Entity type)	HR-CIS: Authorization for operations with RMS documents
	P_RMS_REAA (Reporting unit/area)	
	P_RMS_GRER (Employer)	
	P_RMS_ACTV (Activities with RMS entity)	
P_RMS_SDE0	P_RMS_ETYP (Entity type)	HR-CIS: Authorization for operations with RMS reports
	P_RMS_REAA (Reporting unit/area)	
	P_RMS_GRER (Employer)	
	P_RMS_ACTV (Activities with RMS entity)	

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security \[page 259\]](#).

The following contains specific information about the logical file names and path names for *Payroll Kazakhstan* (PY-KZ).

Logical File Names Used in Payroll Kazakhstan

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names
HR_KZ_F200	RPCPAYKZ_F200_DECLR
HR_KZ_TAST	RPCPAYKZ_TAST

Logical Path Names Used in Payroll Kazakhstan

The logical file names listed above all use the logical file path HR_KZ_DATASET.

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Kazakhstan, this includes the social security number (IIN number) in the infotype *Personal Data* (0002).

Related Information

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.20 Country/Region-Specific Features: New Zealand

Overview of security-relevant information for payroll and personnel administration for the local version for New Zealand (PY-NZ, PA-PA-NZ).

Authorizations

The local version for New Zealand uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to this local version.

Standard Authorization Objects

The local version for NZ uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

Further, the following security-relevant authorization objects are used specifically in the local version for NZ:

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_NZ_PDF	P43_ABKRS (Payroll Area) PNZ_ERIRD (Employer/Company Inland Revenue Number)		Authorizations for NZ Payday Filing

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The logical file names and path names created specifically for *Payroll New Zealand* (PY-NZ) to facilitate the validation of physical file names are as follows:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_NZ_EMS_FILENAME	HNZLEMPD0 HNZLPDS0	HR_NZ_EMS_FILEPATH

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for New Zealand (PY-NZ, PA-PA-NZ), this includes the employee IRD number in the infotype *IRD Nbr New Zealand* (IT0309). You can access the number in the following ways:

- Directly using infotype *IRD Nbr New Zealand* (IT0309) with transaction *Maintain HR Master Data* (PA30)
- By choosing the *IRD Number* pushbutton in infotype *Tax New Zealand* (IT0313).

The authorizations required to read or change the IRD number depend on the authorizations in the user profile.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.21 Country/Region-Specific Features: Norway

Overview of security-relevant information for payroll and personnel administration for the local version for Norway.

Authorizations

The local version for Norway (PY-NO, PA-PA-NO) uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Norway.

Standard Authorization Objects

The local version for Norway uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)

The following table shows the security-relevant authorization objects that are also used in the local version for Norway.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_NO_ENTNR	P20_ENTNR (EDAG - Enterprise Nr.)		Norway: Authorization object for Enterprise Number
P_NO_ALTIN	ACTVT(Activity)		Norway: Authorization to send data to Altinn Portal
P_NO_RTEEX	REPID(ABAP Program Name)		Norway: Export Runtime Environment
P_NO_RPRTE	PNO_RPRTEE (HRNO - Reportee Number)		Norway: Authorization object for Reportee
P_NO_TEMSE	BUKRS(Company Code)		Authorization object for downloading Norway Temse Files

Communication Channel Security

The following table shows the communication paths that the local version for Norway uses, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
A-message	Internal communication between HR back-end system and middleware (PI/PO/CPI): HTTP(S) External communication between middleware (PI/PO/CPI) and authority: HTTP(S)	Personnel Data	Personnel Data
Tax Card	Internal communication between HR back-end system and middleware (PI/PO/CPI): HTTP(S) External communication between middleware (PI/PO/CPI) and authority: HTTP(S)	Personnel Data	Personnel Data

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Income Form	Internal communication between HR back-end system and middleware (PI/PO/CPI): HTTP(S) External communication between middleware (PI/PO/CPI) and authority: HTTP(S)	Personnel Data	Personnel Data
Sick Note	Internal communication between HR back-end system and CPI: HTTP(S) External communication between CPI and authority: HTTP(S)	Personnel Data	Personnel Data

You can use Secure Network Communications (SNC) to protect RFC connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under Transport Layer Security.

Communication Destinations

You can communicate using the CPI Gateway. The communication channel is encrypted with 128 Bit SSL. Data is transferred using the HTTPS protocol.

The following table presents an overview of the communication destinations that the local version for Norway uses.

Communication Destinations

Destination	Provided	Type	Description
HR_NO_CPI_EC_REST_API	No	HTTPS	CPI - Enterprise Certificate REST API
HR_NO_CPI_EC_USR_MNG	No	HTTPS	CPI - Enterprise Certificate User Manager

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Norway](#) (PY-NO).

Logical File Names Used in Payroll Norway

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_NO_DIR_DOWNLOAD	RPLTEMV0 RPCATPV0	HR_NO_DIR_DOWNLOAD
HR_NO_DIR_UPLOAD	RPLTEMV0 RPSSTV1	HR_NO_DIR_UPLOAD
HR_NO_LOAN_XML_FILE_NAME_APPSE RVER	RPLLONV0	HR_NO_LOAN_XML_FILE_TO_APPSERV ER
HR_NO_LOAN_XML_FILE_NAME_FRONT END	RPLLONV0	HR_NO_LOAN_XML_FILE_TO_FRONTEN D

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Norway, this includes the PERID in the infotype *Personal Data* (0002).

More Information

See *Payroll (PY)* in the SAP S/4HANA Security Guide for Human Resources.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.22 Country/Region-Specific Features: Romania

Overview of security-relevant information for payroll and personnel administration for the local version for Romania

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Romania](#) (PY-RO).

Logical File Names Used in Payroll Romania

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_RO_DIR_DOWNLOAD	HROCBT20	
HR_RO_CFIS0	HROCFIS1	
HR_RO_CRS10	HROCRS10	

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Romania, this includes the ID number (CNP/NIF) in the infotype [Personal Data](#) (0002), the ID number (CNP/NIF) - Family member in the infotype [Family Member/Dependents](#) (0021) and the Labour Card (01), Identity Card (02), Passport (03), Driving License (04), Residence Permit (07), Fiscal Identification Number (08), Other type RO Ident. Card (09) and CIS Number (ID for Health Houses) (10) in the infotype 0185.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.23 Country/Region-Specific Features: Russia

Overview of security-relevant information for payroll and personnel administration for the local version for Russia.

Authorizations

The local version for Russia (PA-PA-RU, PY-RU) uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Russia.

Standard Authorization Objects

The local version for Russia uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations \[page 243\]](#) (Personnel Management)
- [Authorizations \[page 255\]](#) (Payroll)

The following table shows the security-relevant authorization objects that are also used in the local version for Russia.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Description
P_LN_ENT	P_LN_REPA (Reporting area)	HR-CIS: Authorization for operations with sickness certificate entities
	P_LN_STEP (Step of sickness certificate processing)	
	P_LN_OPER (Sickness certificate entity operation)	
P_RMS_RSE	P_RMS_REPA (Reporting area)	HR-CIS: Authorization for operations with RMS Reporting Session
	P_RMS_REPT (Report type)	
	P_RMS_OPER (Processing level operation)	
P_RMS_SDC0	P_RMS_CTYP (Entity type)	HR-CIS: Authorization for operations with RMS records
	P_RMS_REAA (Reporting unit/area)	
	P_RMS_GRER (Employer)	
	P_RMS_ACTV (Activities with RMS entity)	

Authorization Object	Field	Description
P_RMS_SDD0	P_RMS_DTYP (Entity type) P_RMS_REAA (Reporting unit/area) P_RMS_GRER (Employer) P_RMS_ACTV (Activities with RMS entity)	HR-CIS: Authorization for operations with RMS documents
P_RMS_SDE0	P_RMS_ETYP (Entity type) P_RMS_REAA (Reporting unit/area) P_RMS_GRER (Employer) P_RMS_ACTV (Activities with RMS entity)	HR-CIS: Authorization for operations with RMS reports
P_RU_0294C	AUTHC (Authorization level)	HR-RU: Authorization for checking records of infotype 0294
P_RU_DCS	P_RU_DCSR (Reporting area) ACTVT (Activity)	HR-RU: Authorization for working with DCS
P_RU_PKMN	HR_RU_EVNT (Count parameter) HR_RU_PKID (Package type) HR_RU_REGN (Registration number) HR_RU_USER (Name of processor who changed the object)	Authorization for checking HR_RU_PF DMS – Package Manager

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security \[page 259\]](#).

The following contains specific information about some of the logical file names and path names for *Payroll Russia* (PY-RU).

Logical File Names Used in Payroll Russia

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names, Logical Path Names, and Reports

Logical File Name	Logical Path Names	Reports That Use These Logical File Names
HR_RU_DATASET_P4_FILENAME	HR_RU_DATASET_P4_FILEPATH	HRULP4

Logical File Name	Logical Path Names	Reports That Use These Logical File Names
HR_RU_DATASET_SICC	HR_RU_SICC	RPCPAYRU_SICC
HR_RU_DATASET_SZVM	HR_RU_DATASETS	RPLPADRU_SZVM
HR_RU_DATASET_SZVR	HR_RU_SZVR	RPCPAYRU_SZVR
HR_RU_FIAS	HR_RU_FIAS	RPUPADRU_FIASLOADER
HR_RU_FXML_FILE	HR_RU_FXML	HRULFXML

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Russia, this includes the social security number (SNILS number) in the infotype *Personal Data* (0002).

Related Information

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.24 Country/Region-Specific Features: Saudi Arabia

Overview of security-relevant information for payroll and personnel administration for the local version for Saudi Arabia (PA-PA-SA, PY-SA).

Authorizations

The local version for Saudi Arabia uses the standard authorization concept of SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to this local version.

Standard Authorization Group

The local version for Saudi Arabia uses the security-relevant authorization objects that are available for Personnel Management and Payroll. Authorization group PCSA is provided with this local version.

The following table shows the security-relevant authorization objects that are also used in this local version.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Description
P_SA_VMLIN	P24_VISFUN (<i>HR KSA: Function Codes for Visa Management</i>)	HR: KSA Visa Line
P_SA_VMBLK	<ul style="list-style-type: none">P24_VISFUN (<i>HR KSA: Function Codes for Visa Management</i>)P24_ASTUS (<i>Visa Block Application Status</i>)	HR: KSA Visa Block Request
P_SA_PROM	ACTVT (<i>Activity</i>)	Authorization Object for Promotion Workbench
FISA_ADP	<ul style="list-style-type: none">PERNR (<i>Personnel Number</i>)ACTVT (<i>Activity</i>)	Advance Payment Request - KSA
FISA_EXPO	<ul style="list-style-type: none">BUKRS (<i>Company Code</i>)ACTVT (<i>Activity</i>)	Expenditure Order - KSA
FISA_PYMO	<ul style="list-style-type: none">BUKRS (<i>Company Code</i>)PAYTYPE_SA (<i>Payment Type</i>)ACTVT (<i>Activity</i>)	Payment Order - KSA

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Saudi Arabia, this includes the GOSI number in the **Social Insurance SA** (3252) infotype.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

13.3.4.2.7.25 Country/Region-Specific Features: Singapore

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Singapore](#) (PY-SG).

Logical File Names Used in Payroll Singapore

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names
HR_SG_DIR_NRSFILENAME	RPCNRSR0_XML_ALV

Logical Path Names Used in Payroll Singapore

The logical file names listed above all use the logical file path HR_SG_DIR_NRS.

More Information

See [Payroll \(PY\)](#) in the SAP S/4HANA Security Guide for Human Resources.

13.3.4.2.7.26 Country/Region-Specific Features: Slovakia

Overview of security-relevant information for payroll and personnel administration for the local version for Slovakia.

Authorizations

The local version for Slovakia uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Slovakia.

Standard Authorization Objects

The local version for Slovakia uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

The following table shows the security-relevant authorization objects that are also used in the local version for Slovakia.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_SK_DIC	P31_DIC		HR: Authorization according to VAT number
P_SK_HIPAY	P31_KVGST P31_ZPPLAT		HR: Health insurance statement

Authorization Object	Field	Value	Description
P_SK_PAYER	P31_PAYER		HR: Payer check
P_SK_USRIC	P31_UNAME P31_ICO		HR: Authorization by company reg. number and user name

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Slovakia](#) (PY-SK).

Logical File Names Used in Payroll Slovakia

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_SK_DIR_HSKCDPL1	HSKCDPL1	
HR_SK_DIR_HSKCJVS0	HSKCJVS0	
HR_SK_DIR_HSKCNEL1	HSKCNEL1	
HR_SK_DIR_HSKCPOJ0	HSKCPOJ0	
HR_SK_DIR_HSKCPOJ0	HSKCPOJ0_2013	
HR_SK_DIR_HSKCPRA0	HSKCPRA0	
HR_SK_DIR_HSKCSTL2	HSKCSTL2	
HR_SK_DIR_HSKCTRX0	HSKCTRX0_2013	
HR_SK_DIR_HSKCTRX0	HSKCTRX0_2017	
HR_SK_DIR_HSKCUNP0	HSKCUNP0	
HR_SK_DIR_HSKCUNP0_XML	HSKCUNP0	
HR_SK_DIR_HSKLVDP0	HSKLVDP0	
HR_SK_DIR_HSKLVDP0	HSKLVDP0	
HR_SK_DIR_HSKLVDP0_2006	HSKLVDP0_2006	
HR_SK_DIR_HSKLVDP0	HSKLVDP0_2013	
HR_SK_DIR_HSKLVDP0	HSKLVDP0_2013	
HR_SK_DIR_HSKLVDP0	HSKLVDP0_2017	
HR_SK_DIR_HSKLVDP0	HSKLVDP0_2017	
HR_SK_DIR_HSKLVDP0_XML	HSKLVDP0_XML	

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_SK_DIR_HSKLVDP0_XML	HSKLVDP0_XML_2013	
HR_SK_DIR_HSKLVDP0_XML	HSKLVDP0_XML_2017	
HR_SK_DIR_HSKLVDP9	HSKLVDP9	
HR_SK_DIR_HSKLVDP9	HSKLVDP9_2013	
HR_SK_DIR_HSKLVDP9	HSKLVDP9_2017	
HR_SK_DIR_HSKPSTM0	HSKPSTM1	

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.27 Country/Region-Specific Features: Slovenia

Overview of security-relevant information for payroll and personnel administration for the local version for Slovenia.

Authorizations

The local version for Slovenia uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Slovenia.

Standard Authorization Objects

The local version for Slovenia uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

The following table shows the security-relevant authorization objects that are also used in the local version for Slovenia.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_SI_PDPZ			HR-SI: Authorization for PDPZ reporting

Authorization Object	Field	Value	Description
	P62_ACTVT	M.D.B.	Activity for authorization check M - Data mining, D - Display data, B - B2A file
	P62_TAXNO		Tax number
P_SI_RTEEX			Slovenia: Export Runtime Environment
	REPID		ABAP Program Name

Communication Channel Security

The following table shows the communication paths that the local version for Slovenia uses, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
eNDM	Internal communication between HR back-end system and CPI: HTTP(S) External communication between CPI and authority: HTTP(S)	Personnel Data	Personnel Data

You can use Secure Network Communications (SNC) to protect RFC connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under Transport Layer Security.

Data Flow and Processes

Overview of security aspects involved throughout the most widely-used processes in the local version for Slovenia.

B2A: Communication with Authorities

Report	Area	Document Class
HSICBOL2	SPOT	ENDM

Report	Area	Document Class
HSICMFR1	MF17	M1, M2, M3
HSICPPZ3	PDPZ	OVRY

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for *Payroll Slovenia* (PY-SI).

Logical File Names Used in Payroll Slovenia

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_SI_DIR_APPLSERVER	HSICBEDD	HR_SI_DIR_APPLSERVER
	HSICBL00	
	HSICBT20	
	HSICDOH1	
	HSICEM43	
	HSICRK18	
	HSICRK28	
	HSICMFR1	
	HSICRK1A	
	FUNCTION-POOL HRBASSI_MFORMS	
	HSIC01ZM_XML	
	HSIC0300_XML	
	HSICZAP4	
	HR_SI_DIR_DOWNLOAD	
HSICBL00		
HSICBT20		
HSICDOH1		
HSICEM43		
HSICRK18		
HSICRK28		
HSICMFR1		
HSICRK1A		
FUNCTION-POOL HRBASSI_MFORMS		
HSIC01ZM_XML		
HSIC0300_XML		
HSICZAP4		

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_SI_DIR_FRONTEND	HSICBEDD HSICBL00 HSICBT20 HSICDOH1 HSICEM43 HSICRK18 HSICRK28 HSICMFR1 HSICRK1A FUNCTION-POOL HRBASSI_MFORMS HSIC01ZM_XML HSIC0300_XML HSICZAP4	HR_SI_DIR_FRONTEND

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Slovenia, this includes the personal registration number (EMSO) in the infotype *Personal Data* (0002) and the employee tax number in the infotype 0603.

Other Security-Relevant Information

You can use the interface toolbox (transaction PU12) to update the taxability model. Currently, there are no special authorizations for this. For more information about the interface toolbox, see section *Security for Additional Applications* under *Payroll*.

You have the following options to prevent unauthorized or unintentional updates of the database PCL4:

- You can use the feature UTXSS to activate and deactivate the authorization checks for the tax report.
- You can use the feature UTXSP to specify codes for spool authorizations depending on the tax company and the tax class.

For more information, see the documentation of the features in the SAP S/4HANA system.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.28 Country/Region-Specific Features: Spain

Authorizations

The country version for Spain (PA-PA-ES, PY-ES) uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the country version for Spain.

Standard Authorization Objects

The country version for Spain uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)

The following table shows the security-relevant authorization objects that are also used in the country version for Spain.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_ES_PA_OK	INFTY (Infotype)		Authorization check for the function codes that are permitted for the HR master data of the country version for Spain
	SUBTY (Subtype)		
	PES_SPRPS (Lock indicator for HR master record)		
	PES_FCODE (Function code)		
	ACTVT (Activity)		

More Information

See [Payroll \(PY\)](#) under SAP S/4HANA Security Guide for Human Resources.

13.3.4.2.7.29 Country/Region-Specific Features: Sweden

Overview of security-relevant information for payroll and personnel administration for the local version for Sweden.

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll Sweden](#) (PY-SE).

Logical File Names Used in Payroll Sweden

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_SE_DIR_UPLOAD	RPISIFS0	
HR_SE_DIR_UPLOAD	RPITAXS0	
HR_SE_DIR_DOWNLOAD	RPLRQTS0	
HR_SE_DIR_DOWNLOAD	RPLRQTS1	
HR_SE_DIR_DOWNLOAD	RPLSIFS1	
HR_SE_DIR_DOWNLOAD	RPCEDTS0_XML_SUBROUTINE	
HR_SE_DIR_DOWNLOAD	RPCKU0S1	
HR_SE_KU04	RPCKU1S1	
HR_SE_DIR_DOWNLOAD	RPCKU1S4_XML	
HR_SE_DIR_DOWNLOAD	RPCKU1S4_XML_LCL	
HR_SE_DIR_DOWNLOAD	RPLAMFS2	
HR_SE_DIR_DOWNLOAD	RPLMEFS1	
HR_SE_DIR_DOWNLOAD	RPLSPPS1	
HR_SE_DIR_DOWNLOAD	RPLSPPXML1	
HR_SE_DIR_DOWNLOAD	RPSDWLS0	
HR_SE_DIR_DOWNLOAD	RPSDWLS1	
HR_SE_DIR_DOWNLOAD	RPSDWLS2	
HR_SE_DIR_DOWNLOAD	RPSDWLS3	
HR_SE_DIR_DOWNLOAD	RPSDWLS4	
HR_SE_DIR_DOWNLOAD	RPSDWLS5	

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_SE_DIR_DOWNLOAD	RPSDWLS6	
HR_SE_DIR_DOWNLOAD	RPSDWLS7	
HR_SE_DIR_DOWNLOAD	RPSDWLS8	
HR_SE_DIR_DOWNLOAD	RPSDWLS9	
HR_SE_DIR_DOWNLOAD	RPSDWLSA	
HR_SE_DIR_DOWNLOAD	RPSDWLSB	
HR_SE_DIR_DOWNLOAD	RPSF08S0	

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.30 Country/Region-Specific Features: Switzerland

Overview of security-relevant information for payroll and personnel administration for the local version for Switzerland.

Authorizations

The local version for Switzerland (PA-PA-CH, PY-CH) uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for Switzerland.

Standard Authorization Objects

The local version for Switzerland uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)

The following table shows the security-relevant authorization objects that are also used in the local version for Switzerland.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_CH_PK	KONNR (Individual PF Account Number)		HR-CH: Pension Fund: Account Access (see ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶ P_CH_PK (HR-CH: Pension Fund: Account Access) ▶)
	AUTGR (HR-CH: Authorization group for PF accounts)		
	PKKLV (HR-CH: Pension fund : Authorization level for account access)		

For the documentation for the authorization object P_CH_PK, see SAP Library for SAP S/4HANA and choose [▶ Human Resources ▶ HR Tools ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶](#).

Communication Channel Security

The following table presents the communication paths used by the local version for Switzerland for [B2A: Communication with Authorities](#), the protocol used by the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
ELM (Uniform Wage Notification Procedure)	External communication between HR backend system and distributor/authorities: HTTPS	Personnel data	Personal data

You can use Secure Network Communications (SNC) to protect RFC connections. The Secure Sockets Layer protocol (SSL protocol) protects HTTP connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under [Transport Layer Security](#).

For more information about B2A security, see [B2A: Communication with Authorities](#).

More Information

See [Payroll \(PY\)](#) in the S/4HANA Security Guide for Human Resources.

13.3.4.2.731 Country/Region-Specific Features: The Netherlands

Overview of security-relevant information for payroll and personnel administration for the local version for the Netherlands.

Authorizations

The local version for the Netherlands (PY-NL, PA-PA-NL) uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for the Netherlands.

Standard Authorization Objects

The local version for the Netherlands uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations \[page 243\]](#) (Personnel Management)
- [Authorizations \[page 255\]](#) (Payroll)
- [Authorizations \[page 264\]](#) (B2A: Communication with Authorities)

The following table shows the security-relevant authorization objects that are also used in the local version for the Netherlands.

Country/Region-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_NL_AEDM	JUPER (Legal person) ACTVT (Activity)	The Activity (ACTVT) field has the following values: <ul style="list-style-type: none">• 01 = Add or create• 03 = Display status	HR: Authorization object for Day-one-announcement
P_NL_EIR	PERSA (Personnel Area) PERSG (Employee Group) PERSK (Employee Subgroup) VDSK1 (Organizational Key) ACTVT (Activity)	The Activity (ACTVT) field has the following values: <ul style="list-style-type: none">• 41 = Delete in DB• A3 = Change status• H1 = Deactivate	HR: Authorization object Elec. Illness & Recovery Reporting

Authorization Object	Field	Value	Description
P_NL_LA06	JUPER (Legal person)	For the Wage Return and CAK Return reports, the Activity (ACTVT) field has the following values:	HR: Authorization object for Wage Return, Work Cost Regulation (WCR), Pension Return, and CAK Return reports
	ACTVT (Activity)		
		For the Work Cost Regulation reports, the Activity (ACTVT) field has the following values:	
		For the Pension Return reports, the Activity (ACTVT) field has the following values:	

Communication Channel Security

The following table presents the communication paths used by the local version for the Netherlands (PY-NL, PA-PA-NL), the protocol used by the connection, the type of data transferred, and the data requiring particular protection.

Communication Paths and Their Protocols

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Wage Return	HTTPS	Periodical declarations of personnel and salary-related information	Personal Data

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Pension Return	HTTPS	Periodical declarations of personnel and pension-related information	Personal Data
Electronic Illness Reporting	HTTPS	Event-based declarations of personnel and illness/absence information	Personal Data

You can use Secure Network Communications (SNC) to protect RFC connections.

Note

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see [Transport Layer Security](#) in the ABAP Platform Security Guide.

For more information about B2A security, see [B2A: Communication with Authorities \[page 263\]](#).

Communication Destinations

The following table presents an overview of the communication destinations that the local version for the Netherlands uses.

Communication Destinations

Destination	Provided	Type	Description
Wage Return	For local version the Netherlands	Consumer Proxy	Service consumer: <ul style="list-style-type: none"> CO_HRNL_SBRAANLEVER_SERVICE_V1 CO_HRNL_SBRSTATUSINFORMATIE_SE
Pension Return	For local version the Netherlands	Consumer Proxy	Service consumer: <ul style="list-style-type: none"> CO_HRNL_PR_WS_UPA_MSGUPAWEB_SE
Electronic Illness Reporting	For local version the Netherlands	Consumer Proxy	Service consumer: <ul style="list-style-type: none"> CO_HRNL_SBRAANLEVER_SERVICE_V1 CO_HRNL_SBRSTATUSINFORMATIE_SE

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security \[page 259\]](#).

The following contains specific information about some of the logical file names and path names for *Payroll Netherlands* (PY-NL).

Logical File Names Used in Payroll Netherlands

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names, Logical Path Names, and Reports

Logical File Name	Logical Path Names	Reports That Use These Logical File Names
HR_NL_EDM_DONE	HR_NL_EDM_DONE	<ul style="list-style-type: none"> • RPCEDKNO • RPCEDZNO
HR_NL_EDM_IN	HR_NL_EDM_IN	<ul style="list-style-type: none"> • RPCEDKNO • RPCEDZNO
HR_NL_EDM_IN_DIR	HR_NL_EDM_IN	<ul style="list-style-type: none"> • RPCEDKNO • RPCEDZNO
HR_NL_EDM_OUT	HR_NL_EDM_OUT	<ul style="list-style-type: none"> • RPCEDMNO • RPCEDZNO
HR_NL_LAA_DONE	HR_NL_LAA_DONE	<ul style="list-style-type: none"> • RPCLAKNO • RPCLAZNO
HR_NL_LAA_IN	HR_NL_LAA_IN	<ul style="list-style-type: none"> • RPCLAKNO • RPCLAZNO • RPULATNO
HR_NL_LAA_IN_DIR	HR_NL_LAA_IN	<ul style="list-style-type: none"> • RPCLAKNO • RPCLAZNO
HR_NL_LAA_OUT	HR_NL_LAA_OUT	<ul style="list-style-type: none"> • RPCLACNO • RPCLAZNO
HR_NL_LAA_OUT_NEW	HR_NL_LAA_OUT	<ul style="list-style-type: none"> • RPCLACNO • RPCLAZNO
HR_NL_PRNL_DONE	HR_NL_PRNL_DONE	<ul style="list-style-type: none"> • RPCPRKNO • RPCPRZNO
HR_NL_PRNL_IN	HR_NL_PRNL_IN	<ul style="list-style-type: none"> • RPCPRKNO • RPCPRZNO

Logical File Name	Logical Path Names	Reports That Use These Logical File Names
HR_NL_PRNL_IN_DIR	HR_NL_PRNL_IN	<ul style="list-style-type: none"> RPCPRKN0 RPCPRZNO
HR_NL_PRNL_IN_NEW	HR_NL_PRNL_IN	RPCPRZNO
HR_NL_PRNL_OUT_NEW	HR_NL_PRNL_OUT	RPCPRZNO

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for the Netherlands, this includes the national identification number (BSN number) in the *Personal Data* (0002) infotype.

Related Information

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.32 Country/Region-Specific Features: Turkey

Overview of security-relevant information for payroll and personnel administration for the local version for Turkey.

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for Turkey, this includes the social security no. (SSKNO) and the tax id number (TAXKN) in the infotype 0769 and the id card no. (IDCNO), TR identity no. (MERNI) and the driv. licns. no. (DLNUM) in the infotype 0770.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

[Payroll \(PY\) \[page 253\]](#)

13.3.4.2.7.33 Country/Region-Specific Features: United Arab Emirates

Overview of security-relevant information for payroll and personnel administration for the local version for the United Arab Emirates (PA-PA-AE, PY-AE).

Authorizations

The local version for the United Arab Emirates uses the standard authorization concept of SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to this local version.

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for the United Arab Emirates, this includes the social security number (SINUM) in the **Social Insurance AE** (3251) infotype.

Related Information

[Authorizations \[page 255\]](#)

[Authorizations \[page 243\]](#)

13.3.4.2.7.34 Country/Region-Specific Features: United Kingdom

Overview of security-relevant information for payroll and personnel administration for the local version for the United Kingdom (PY-GB, PA-PA-GB).

Authorizations

The local version for the UK uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the local version for the UK.

Standard Authorization Objects

The local version for the UK uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- [Authorizations](#) (Personnel Management)
- [Authorizations](#) (Payroll)
- [Authorizations](#) (B2A: Communication with Authorities)

Communication Channel Security

The following table presents the communication paths used by the local version for the United Kingdom (PY-GB, PA-PA-GB) for [B2A: Communication with Authorities](#), the protocol used by the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
E-Filing	Internal communication between HR back-end system and middleware: HTTP(S) (SAP Business Connector (BC): TCP/IP or PI*: Proxy) External communication between middleware and tax authorities: HTTP(S)	Personnel Data	Personal Data

* PI = SAP NetWeaver Exchange Infrastructure/Process Integration (XI/PI)

HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

i Note

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under Transport Layer Security.

For more information about B2A security, see [B2A: Communication with Authorities](#).

Communication Destinations

You can communicate with HMRC Gateway. The communication channel is encrypted with 128 Bit SSL. The employees' tax data is transferred via RFC connections and using the protocol HTTPS.

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll United Kingdom \(PY-GB\)](#).

Logical File Names Used in Payroll United Kingdom

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names
HR_GB_DIR_RPCMAPG0	RPCEOYG0
	RPCEOYG0PBS
	RPLRTIGH
	RPURCNG0
	RPURCNG0PBS
HR_GB_DIR_RPCUSSG0	RPCUSSG0
HR_GB_DIR_RPCUSSG1	RPCUSSG1
HR_GB_DIR_RPUASHG0	RPUASHG0
HR_GB_DIR_RPUCLSG0	RPUCLSG0
HR_GB_DIR_RPUHESG1	RPUHESG1
HR_GB_DIR_RPULGPG1	RPULGPG1
HR_GB_DIR_RPULGPG2	RPULGPG2
HR_GB_DIR_RPURCNG0	RPURCNG0
HR_GB_DIR_RPUTCUG0	RPUTCUG0
HR_GB_DIR_RPUTMSG0	RPUTMSG0
HR_GB_DIR_RPUTPSG0	RPUTPSG0
HR_GB_DIR_RPUUSSG0	RPUUSSG0
HR_GB_DIR_RPUUSSG1	RPUUSSG1

Logical Path Names Used in Payroll United Kingdom

The logical file names listed above all use the logical file path `HR_GB_DIR_FILEPATH`.

Particularly Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the local version for the UK, this includes the National Insurance Number (NINO) in the infotype *Personal Data* (0002).

More Information

See *Payroll (PY)* under SAP S/4HANA Security Guide for Human Resources

13.3.4.2.7.35 Country/Region-Specific Features: USA

Overview of security-relevant information for payroll and personnel administration for the country/region version for USA.

Important SAP Notes

The following table presents the most important SAP Notes regarding security for the country/region version for USA (PA-PA-US, PY-US).

Title	SAP Note	Comment
Tax Reporter Transaction and Spool Security	430595	

Authorizations

The country/region version for USA uses the standard authorization concept used by SAP S/4HANA. Therefore, the recommendations and guidelines for authorizations as described for SAP S/4HANA also apply to the country/region version for USA.

Standard Authorization Objects

The country/region version for USA uses the security-relevant authorization objects that are available for Personnel Management and Payroll.

For more information, see the following:

- *Authorizations* (Personnel Management)
- *Authorizations* (Payroll)

The following table shows the security-relevant authorization objects that are also used in the country/region version for USA.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_USTR	ACTVT (Activity)		Authorizations for Tax Report
	PERSA (Personnel Area)		
	BTRTL (Personnel Subarea)		

Communication Channel Security

The following table shows the communication paths that the country/region version for USA uses, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
BSI TaxFactory for tax calculation	RFC	Tax data for the country/region version for USA	
BSI TaxFactory™ SaaS	HTTPS	Tax data for the country/region version for USA	

You can use Secure Network Communications (SNC) to protect RFC connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the ABAP Platform Security Guide under Transport Layer Security.

Communication Destinations

You can exchange data with local servers or terminals for the VET and EEO reports for the country/region version for USA. You can use this function to download files from the application server to a presentation server. You then receive the text files required by the authorities with the output format `.txt`. This output format complies with the law.

The data is **not** encrypted in the standard system. It is your decision as to the level of encryption that you want to use if you want to send the data to the Federal Commission or Department of Labor.

The following table presents an overview of the communication destinations that the country/region version for USA uses.

Communication Destinations

Destination	Provided	Type	Description
BSI	For country/region version for USA	RFC with the function module PAYROLL_TAX_CALC_US	PAYROLL_TAX_CALC_US_50
			PAYROLL_TAX_CALC_US_60
			PAYROLL_TAX_CALC_US_70
BSI TaxFactory™ SaaS	For country/region version for USA	Consumer Proxy	SOA Manager Consumer Proxy CO_HRCUSCL_T11_BSITF11 SERVICE

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll USA](#) (PY-US).

Logical File Names Used in Payroll USA

The following logical file names were created to facilitate the validation of physical file names:

Logical File Names and Reports

Logical File Name	Reports That Use These Logical File Names
HR_US_TR_XML_SCHEMA	RPCTR101_XML

Logical Path Names Used in Payroll USA

The logical file names listed above all use the logical file path HR_US_TR.

Particularly Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the country/region version for USA, this includes the social security number (SSN number) in the infotype [Personal Data](#) (0002).

Other Security-Relevant Information

You can use the interface toolbox (transaction PU12) to update the taxability model. Currently, there are no special authorizations for this. For more information about the interface toolbox, see section [Security for Additional Applications](#) under [Payroll](#).

You have the following options to prevent unauthorized or unintentional updates of the database PCL4:

- You can use the feature UTXSS to activate and deactivate the authorization checks for the tax report.
- You can use the feature UTXSP to specify codes for spool authorizations depending on the tax company and the tax class.

For more information, see the documentation of the features in the SAP S/4HANA system.

More Information

See [Payroll \(PY\)](#) in the S/4HANA Security Guide for Human Resources.

13.3.4.2.7.36 Country/Region-Specific Features: Non-Profit Organizations

Overview of security-relevant information for payroll and personnel administration for the local version for Non-Profit Organizations.

Communication Channel Security

The table below shows the communication paths used by the local version for Non-profit Organizations, the protocol used for the connection, and the type of data transferred for **B2A: Communication with UN Pension Fund Authorities (UNJSPF)**.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Common HR Interface	Internal communication between HR back-end system and middleware: HTTP(S) (SAP Business Connector (BC): TCP/IP or PI*: Proxy) External communication between middleware and tax authorities: HTTP(S)	HR master data containing Personnel Data	Personal Data

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Monthly Financial Interface	Internal communication between HR back-end system and middleware: HTTP(S) (SAP Business Connector (BC): TCP/IP or PI*: Proxy) External communication between middleware and tax authorities: HTTP(S)	Financial Data containing Pension Contributions of the UN Organization staff members	Personal Data

*PI = SAP NetWeaver Exchange Infrastructure/Process Integration (XI/PI).

HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

→ Recommendation

We strongly recommend using secure protocols (SSL, HTTPS) whenever possible.

For more information on ABAP platform security, see ABAP Platform Security Guide.

For more information about B2A security, see B2A: Communication with Authorities.

Communication Destinations

You can communicate with Pension Fund Authorities (UNJSPF). The communication channel is encrypted with 128 Bit SSL. The staff members' HR master data and pension contribution data are transferred via RFC connections and using the protocol HTTPS.

Data Storage Security

Use

The following contains specific information about the logical file names and path names for Payroll Non-Profit Organizations (PY-NPO).

Logical File Names Used in Payroll Non-Profit Organizations

The following logical file names and logical file paths were created to facilitate the validation of physical file names:

Logical File Names, Reports, and File Paths

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_HUNUCMT_LOADER_FILE	HUNUCMT_LOADER	HR_UN_FILE_PATH
HR_HUNCPFY0_FILE	HUNCPFY0	HR_UN_FILE_PATH

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects.

More Information

See [Payroll \(PY\)](#) in the SAP S/4HANA Security Guide for Human Resources

13.3.4.2.7.37 Country/Region-Specific Features: Other Countries

Data Storage Security

For general information about data storage security in Payroll, see [Data Storage Security](#).

The following contains specific information about the logical file names and path names for [Payroll for Other Countries](#) (PY-XX).

Logical File Names Used in Payroll for Other Countries

The following logical file names and logical file paths were created to facilitate the validation of physical file names:

Logical File Names, Reports/Function Modules, and File Paths

Logical File Name	Reports or Function Modules That Use These Logical File Names	Logical File Path
HR_XX_DIR_B2AFIIE	Report H99_B2AFIIE	HR_XX_DIR_B2AFIIE
HR_XX_DIR_RPUFCP01	Report RPUFCP01	HR_XX_DIR_RPUFCP01

Logical File Name	Reports or Function Modules That Use These Logical File Names	Logical File Path
HR_XX_DIR_RH_CALL_ORGDISPLAY	Function module RH_CALL_ORGDISPLAY	HR_XX_DIR_RH_CALL_ORGDISPLAY
HR_XX_DIR_RHMOVE40	Report RHMOVE40	PD_DATASET
HR_OT_FILEPORT	Report RPUOTFL0	HR_OT_DIR_FILEPORT

More Information

See [Payroll \(PY\)](#) in the SAP S/4HANA Security Guide for Human Resources.

13.3.4.3 Self-Services

13.3.4.3.1 Important SAP Notes

Definition

This chapter of the Security Guide provides you with information about the following self-service components:

- *Business Unit Analyst (BUA)*
- *Project Self-Services (PSS)*
- *Higher Education and Research (IS-HER-CSS)*
- *General Parts (PCUI_GP)*

If not stated otherwise, the security settings for user management and authorizations apply to all of the afore-mentioned components.

The following self-service components have their own sections in this chapter:

- *Employee Self-Service*
- *Manager Self-Service*

i Note

For these components, all security-relevant information is included in the relevant subsections.

Important SAP Notes

The table below shows important SAP Notes that apply to the security for some *Self-Service* applications. For more information about standard roles for assigning authorization in the Self-Service applications, see the *Authorizations* section of this Security Guide.

Important SAP Notes

SAP Note Number	Title	Comment
846439	PSS: Authorizations and roles for Web Dynpro	This SAP Note contains the authorization objects and the default values defined for the Web Dynpro applications for <i>Project Self-Services</i> (component EP-PCT-PLM-PSS).

13.3.4.3.2 User Management

Use

User management for *Self-Service* applications uses the mechanisms provided with ABAP Platform, for example, tools, user types, and password policy. For an overview of how these mechanisms apply for *Self-Service* applications, see the sections below.

User Administration Tools

The table below shows the tools to use for user management and user administration with the *Self-Service* applications.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance in AS ABAP (transactions SU01 and PFCG)	You can use the Role Maintenance (PFCG) transaction to generate profiles for your self-service users.	

For more information, see the *User and Roles* section.

User Types

For information about the user types, see the Application Server ABAP Security Guide.

→ Recommendation

For portal roles, we recommend that you set up the connection between the portal and the connected systems (ECC system, J2EE Engine, BW system) such that each individual user has access.

Standard Users

Component	Standard Users
Project Self-Service Business Unit Analyst	No standard users exist in the standard SAP system for these components.
Higher Education and Research	For information about the standard users for this component, see the Security Guide for this component.

13.3.4.3.3 Authorizations

Use

The *Self-Service* applications use the authorization concept provided by *Application Server ABAP*. Therefore, the recommendations and guidelines for authorizations as described in the *ABAP Platform Security Guide for ABAP* also apply to the *Self-Service* applications.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the *Profile Generator* (transaction PFCG). For more information, see *Editing Roles and Authorizations for Web Dynpro Services*.

Standard Roles

Business Unit Analyst and Project Self-Services

There are no standard roles for these components.

Higher Education and Research

For information about the standard roles for this component, see the Security Guide for this component.

Standard Authorization Objects

The table below shows the general security-relevant authorization objects that are used by the *Self-Service* applications.

Standard Authorization Objects for Self-Service Applications:

Authorization Object	Field	Value	Description
S_RFC	RFC_NAME	Depends on service	Saves data when the back-end system is accessed via RFC from the Web Dynpro front end.

Higher Education and Research

For information about the standard authorization objects for this component, see the Security Guide for this component.

Internal Service Request and Personnel Change Requests

For information about standard authorization objects for the *Internal Service Request (ISR)* and *Personnel Change Requests*, see SAP Note 623650.

13.3.4.3.3.1 Maintain Roles and Authorizations for Web Dynpro Services

Use

You use this procedure to maintain roles, their associated Web Dynpro services, and authorizations.

Procedure

1. In transaction PFCG, create a role or select an existing default role for the component. Choose *Create Role* or copy the existing default role.
2. Assign the services you require to the role.
 1. On the *Menu* tab page, choose *Authorization Default*.
The *Service* dialog box appears.
 2. Select the *External Service* checkbox.
 3. Select *WEBDYNPRO* as the external service type.
 4. In the *Service* field, select the Web Dynpro service you require.
 5. Choose *Save*.
The authorization objects and default values maintained for the service are then displayed in the menu tree structure.
In the same manner, select all the Web Dynpro services that you want to use.

3. Assign the required authorizations.
To do this, choose the [Authorizations](#) tab page to maintain the authorization objects and values in accordance with your requirements.

For more detailed information about role maintenance, see [Role Administration \[page 13\]](#).

13.3.4.3.3.2 Authorizations for Controlling Services (BUA)

The table below shows the standard authorization objects that are used by the controlling services in *Business Unit Analyst (BUA)*.

i Note

These authorization objects are also used by the controlling services in *Business Package for Manager Self-Service (MSS)*.

Authorization Object	Description
K_CCA	General authorization object for Cost Center Accounting. Is checked in the relevant Monitor iViews, Master Data iViews, and Express Planning services.
K_ORDER	General authorization object for internal orders. Is checked in the relevant Monitor iViews, Master Data iViews, and Express Planning services.
K_PCA	Area responsible, Profit Center. Is checked in the relevant Monitor iViews, Master Data iViews, and Express Planning services.
K_CSXS_PLA	Cost element planning. Is checked in the relevant Express Planning services.
K_FPB_EXP	Authorization object for Express Planning. This authorization object checks the Express Planning Framework call and the planning round call. The actual plan data is protected by the authorization objects for the individual Express Planning services.

i Note

For more information about the fields for the authorization objects K_CCA, K_ORDER, and K_PCA, see SAP Note 15211.

13.3.4.3.4 Employee Self-Service

About This Document

This chapter provides an overview of the security-relevant information that applies to Employee Self-Service (CA-ESS).

The following deployment options are available for Employee Self-Service (ESS):

- **Business Package for Employee Self-Service** (up to and including 1.50)
This Business Package is a “classic” SAP Business Package that runs in the SAP Enterprise Portal. The Portal role consists of worksets and iViews based on Web Dynpro ABAP technologies.
- **Business Package for Employee Self-Service (WDA)**
This Business Package also runs in the SAP Enterprise Portal but it has only one workset with one iView that launches the role structure with the applications maintained in the back-end system. In this business package, all applications are based on Web Dynpro ABAP technology.
- **Employee Self-Service in SAP Business Client for HTML**
The role structure of this deployment option is maintained in the back-end system with the SAP role maintenance transaction `PF03`. All applications available with this role are based on Web Dynpro ABAP technology.

i Note

Some parts of the security information in this chapter only apply to individual ESS deployment options. In this case, you will find a comment explaining for which deployment option this information is valid right at the beginning of each section. If not stated otherwise, the security information in this chapter applies to all ESS deployment options.

See also:

- For more information about the roles in SAP Business Client, go to https://help.sap.com/s4hana_op_2020, enter *Roles in SAP Business Client* into the search bar, press `Enter`, and open the search result with that title.
- For more information about SAP Business Client, go to https://help.sap.com/s4hana_op_2020, enter *SAP Business Client* into the search bar, press `Enter`, and open the search result with that title.

Overview of the Main Sections of This Chapter

This chapter comprises the following sections with security-related topics specific to Employee Self-Service:

- *Before You Start*
This section comprises references to other Security Guides that are relevant for Employee Self-Service and a list of the most important notes for Employee Self-Service regarding security.
- *User Administration and Authentication*

This section provides an overview of the following user administration and authentication aspects for Employee Self-Service:

- [User Management](#)
This section contains information about the user types that are required by Employee Self-Service and standard users for Employee Self-Service.
- [Integration into Single Sign-On Environments](#)
This topic describes how the Employee Self-Service supports Single Sign-On mechanisms.
- [Authorizations](#)
This section provides an overview of the authorization concept that applies to Employee Self-Service.
- [Session Security Protection](#)
This section provides information on activating secure session management.
- [Network and Communication Security](#)
This section provides an overview of the communication paths used by Employee Self-Service and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level:
 - [Communication Channel Security](#)
 - [Network Security](#)
 - [Communication Destinations](#)
- [Internet Communication Framework Security](#)
This section provides an overview of the Internet Communication Framework (ICF) services that are used by Employee Self-Service.
- [Security-Relevant Logging and Tracing](#)
This section provides an overview of the logging and tracing mechanisms that apply to Employee Self-Service.

13.3.4.3.4.1 User Administration and Authentication

User management for Employee Self-Service uses the mechanisms provided with the Application Server ABAP:

The security recommendations and guidelines for user administration and authentication as described in the Application Server ABAP Security Guide apply for *Employee Self-Service (WDA) in SAP Business Client for HTML* apply to the ESS business packages (*Business Package for Employee Self-Service*) and *Business Package for Employee Self-Service (WDA)*.

In addition to these guidelines, information about user administration and authentication that specifically applies to Employee Self-Service is included in the following sections:

- [User Management](#)
- [Integration into Single Sign-On Environments](#)

13.3.4.3.4.1.1 User Management

Use

User management for *Employee Self-Service (WDA) in SAP Business Client for HTML* uses the mechanisms provided with the Application Server ABAP.

For an overview of how these mechanisms apply to Employee Self-Service, see the sections below.

User Administration Tools

The table below shows the tools to use for user management and user administration with Employee Self-Service.

User Management Tools

Tool	Detailed Description	Comment
User maintenance for ABAP-based systems (transaction SU01)	You use the user maintenance transaction to generate users in the ABAP-based systems and to assign authorization profiles.	Used for all ESS deployment options
Role maintenance (transaction PFCG)	You use the role maintenance transaction to generate authorization profiles for your self-service users. For more information, see User and Role Administration of AS ABAP .	Used for all ESS deployment options

i Note

For the ESS business packages, you must perform user mapping for the users in the ABAP system and the Portal. For more information, see [Assigning Portal Roles to Users](#).

⚠ Caution

Ensure that you give end users general reading permission for the SAP Enterprise Portal. For more information, see SAP Note [939412](#).

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively must change their passwords on a regular basis, but not those users under which background processing jobs run.

User types that are required for Employee Self-Service include:

- Individual users:
 - Dialog users (Used for SAP GUI for Windows or RFC connections)
 - Internet users (Same policies apply as for dialog users, but used for Internet connections).
- Technical users:
 - Service users .

For more information on these user types, see User Types in the [AS ABAP Security Guide](#).

i Note

For the [Business Package for Employee Self-Service](#) (up to and including 1.41), we recommend you set up the connection between the SAP Enterprise Portal and the connected systems (ECC system, J2EE Engine, BW system) so that each individual user has access. This does not apply to the [Business Package for Employee Self-Service \(WDA\)](#).

Standard Users

For Employee Self-Service, no standard users are delivered.

13.3.4.3.4.1.2 Integration into Single Sign-On Environments

Use

Employee Self-Service supports the Single Sign-On (SSO) mechanisms provided by ABAP Platform. Therefore, the security recommendations and guidelines for user administration and authentication as described in the ABAP Platform Security Guide also apply to Employee Self-Service.

For more information about the available authentication mechanisms, see [User Authentication and Single Sign-On](#).

Configuration of Web Services with Client Certificates

For ESS applications of the [Business Package for Employee Self-Service](#), the use of client certificates should be configured for authentication when users access the J2EE Engine using an end-to-end connection. To achieve this, follow the instructions under [Configuring the Use of Client Certificates for Authentication](#).

13.3.4.3.4.2 Authorizations

Use

Employee Self-Service uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to ESS.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF00`) on the AS ABAP.

i Note

For more information about how to create roles, see [Role Administration](#).

Role and Authorization Concept for Employee Self-Service

Employee Self-Service embraces services from a variety of SAP applications and also uses the authorizations of these individual components. Most of these services belong to HCM components, see [Authorizations for Human Resources](#).

Standard Roles

The tables below show the standard roles that are used for authorizations by the [Business Package for Employee Self-Service](#) (up to and including 1.50) and by [Employee Self-Service \(WDA\)](#).

Standard Roles for the Business Package for Employee Self-Service

Role	Name	Description
SAP_ESSUSER_ERP05	Single Role with all Non-Country-Specific Functions	Single role that comprises all non country-specific functions.
SAP_EMPLOYEE_ERP05_XX	ESS ERP05: Country-Specific Functions for <Country>	Single role comprising country-specific functions. A separate role exists for each country version (xx = country ID). The corresponding composite role is SAP_EMPLOYEE_ERP05.

Role	Name	Description
SAP_ASR_EMPLOYEE	HR Administrative Services: Employee	Enhancement of the role SAP_ESSUSER_ERP05 for the employees that use the functions of the component PA-AS (HR Administrative Services) in the <i>Business Package for Employee Self-Service</i> (up to and including 1.4.1).

Caution

For the *Business Package for Employee Self-Service*, you also need SAP Note [857431](#) for generating the authorization profiles.

Standard Roles for Employee Self-Service (WDA)

Role	Name	Description
SAP_EMPLOYEE_XX_ESS_WDA_2	ESS International Single Role	Authorizations for all international services in Employee Self-Service (WDA). For more information about this and all other Employee Self-Service (WDA) roles, see <i>Single Roles for Employee Self-Service (WDA)</i> .
SAP_EMPLOYEE_AU_ESS_WDA_1	ESS Single Role for Australia	Authorizations for country-specific services for Australia in Employee Self-Service (WDA).
SAP_EMPLOYEE_CA_ESS_WDA_2	ESS Single Role for Canada	Authorizations for country-specific services for Canada in Employee Self-Service (WDA).
SAP_EMPLOYEE_CH_ESS_WDA_1	ESS Single Role for Switzerland	Authorizations for country-specific services for Switzerland in Employee Self-Service (WDA).
SAP_EMPLOYEE_CN_ESS_WDA_1	ESS Single Role for China	Authorizations for country-specific services for China in Employee Self-Service (WDA).
SAP_EMPLOYEE_DE_ESS_WDA_1	ESS Single Role for Germany	Authorizations for country-specific services for Germany in Employee Self-Service (WDA).
SAP_EMPLOYEE_HK_ESS_WDA_1	ESS Single Role for Hong Kong, China	Authorizations for country-specific services for Hong Kong, China in Employee Self-Service (WDA).

Role	Name	Description
SAP_EMPLOYEE_IN_ESS_WDA_2	ESS Single Role for India	Authorizations for country-specific services for India in Employee Self-Service (WDA).
SAP_EMPLOYEE_JP_ESS_WDA_2	ESS Single Role for Japan	Authorizations for country-specific services for Japan in Employee Self-Service (WDA).
SAP_EMPLOYEE_MY_ESS_WDA_1	ESS Single Role for Malaysia	Authorizations for country-specific services for Malaysia in Employee Self-Service (WDA).
SAP_EMPLOYEE_PT_ESS_WDA_1	ESS Single Role for Portugal	Authorizations for country-specific services for Portugal in Employee Self-Service (WDA).
SAP_EMPLOYEE_SG_ESS_WDA_1	ESS Single Role for Singapore	Authorizations for country-specific services for Singapore in Employee Self-Service (WDA).
SAP_EMPLOYEE_TH_ESS_WDA_1	ESS Single Role for Thailand	Authorizations for country-specific services for Thailand in Employee Self-Service (WDA).
SAP_EMPLOYEE_US_ESS_WDA_1	ESS Single Role for the United States	Authorizations for country-specific services for the USA in Employee Self-Service (WDA).
SAP_FI_TV_WEB_ESS_TRAVELER_2	ESS Single Role for the Traveler	Authorizations for ESS services for the traveler role in Employee Self-Service (WDA).
SAP_ASR_EMPLOYEE_SR_HCM_CI_3	ESS Single Role for HCM P&F Services	Authorizations for international ESS services from the <i>HR Process and Forms</i> application in Employee Self-Service (WDA).
SAP_PM_EMPLOYEE_HCM_CI_1	ESS Single Role for HCM PM Services	Authorizations for ESS services from the <i>Performance Management</i> application in Employee Self-Service (WDA).
SAP_TMC_EMPLOYEE_6	Employee in Talent Management	Authorizations for ESS services from the <i>Talent Management and Talent Development</i> application in Employee Self-Service (WDA). For more information, see <i>Employee in Talent Management</i> .

Role	Name	Description
SAP_RCF_ESS_SR_ERC_CI_4	E-Recruiting services for ESS (WDA)	Authorizations in SAP E-Recruiting for employees that use SAP E-Recruiting services in ESS (WDA).
/SAPSRM/EMPLOYEE_ESS	SAP SRM Employee for ESS	Authorizations in SAP SRM for employees that use services from Purchasing in ESS (WDA).

Note

The composite role `SAP_EMPLOYEE_ESS_WDA_2`, which contains the single roles listed above (except for the last two roles), is required for *Employee Self-Service (WDA) in SAP Business Client for HTML*. For more information on all roles for ESS (WDA), see also *Roles in Employee Self-Service (WDA)*.

Standard Authorization Objects

The following table presents the general authorization objects relevant for security that are used by the *Business Package for Employee Self-Service* (up to and including 1.50).

Standard Authorization Objects for Self-Service Applications

Authorization Object	Field	Value	Description
S_RFC	RFC_NAME	Depends on service	Saves data from RFC access to Web Dynpro front end to the back-end system.

Apart from these authorization objects, all Employee Self-Service deployment options use the authorization objects from the following application areas or application components:

- *Human Capital Management*
See the SAP S/4HANA Security Guide at [Human Capital Management > Authorizations](#).
- *SAP E-Recruiting*
See the SAP S/4HANA Security Guide at [Human Capital Management > Talent Management > SAP E-Recruiting > Authorizations](#).
- *HCM Processes and Forms*
See the SAP S/4HANA Security Guide at [Human Capital Management > Personnel Administration \(PA\) > HCM Processes and Forms > Authorizations](#).
- *Travel Management*
See the SAP S/4HANA Security Guide at [Accounting > Financial Accounting > Travel Management \(FI-TV\)](#).

13.3.4.3.4.3 Session Security Protection

Use

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management.

We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

The following section is relevant for *Employee Self-Service (WDA)*:

To prevent access in javascript or plug-ins to the SAP logon ticket and security session cookies (SAP_SESSIONID_<sid>_<client>), activate secure session management. With an existing security session, users can then start applications that require a user logon without logging on again. When a security session is ended, the system also ends all applications that are linked to this security session.

Use the transaction SICF_SESSIONS to specify the following parameter values shown in the table below in your AS ABAP system:

Session Security Protection Profile Parameters

Profile Parameter	Recommended Value	Comment
icf/ set_HTTPOnly_flag_on_cookies	0	Client-Dependent
login/ticket_only_by_https	1	Not Client-Dependent

For more information, a list of the relevant profile parameters, and detailed instructions, see *Activating HTTP Security Session Management on AS ABAP* in the AS ABAP security documentation.

13.3.4.3.4.4 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the back-end system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for Employee Self-Service is based on the topology used by the ABAP Platform. Therefore, the security guidelines and recommendations described in the ABAP Platform Security Guide also

apply to Employee Self-Service. Details that specifically apply to Employee Self-Service are described in the following sections:

- [Communication Channel Security](#)
This topic provides an overview of the communication channels used by Employee Self-Service, the protocol used for the connection, and the type of data transferred.
- [Network Security](#)
This topic describes the recommended network topology for Employee Self-Service. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate Employee Self-Service.
- [Communication Destinations](#)
This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the ABAP Platform Security Guide:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

13.3.4.3.4.4.1 Communication Channel Security

Use

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

For more information, see Transport Layer Security in the ABAP Platform Security Guide.

→ Recommendation

We strongly recommend using secure protocols (SSL, SNC) whenever possible.

SSL connections for Adobe Document Services

For ESS applications to perform security-related functions such as digitally signing PDF documents or launching of PDF forms, you must set up an SSL connection to the Web service. To achieve this, follow the instructions under [Configuration of the Web Service SSL Connection](#) in the Adobe Document Services Configuration Guide.

13.3.4.3.4.4.2 Network Security

Ports

The Employee Self-Service runs on SAP NetWeaver and uses the port from the AS ABAP (for *Employee Self-Service (WDA)*).

For more information, see the topics for AS ABAP Ports in the corresponding ABAP Platform Security Guide.

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see <https://help.sap.com/viewer/ports>.

13.3.4.3.4.4.3 Communication Destinations

Use

The tables below provide an overview of the communication destinations required for the three Employee Self-Service deployment options.

Employee Self-Service (WDA) in SAP Business Client for HTML

For this deployment option, you have to maintain RFC connections using the transaction SM59, see also the following table 1.

Table 1: Connection Destinations for Employee Self-Service (WDA) in NWBC for HTML

Destination	Delivered	Type	Recommended User Authorizations	Description
SAP_ECC_HumanResources	No	ABAP connection	n/a	System alias for the ECC HCM system
SAP_ECC_HumanResources_HTTP	No	HTTP connection	n/a	System alias for the ECC HCM system
SAP_SRM	No	ABAP connection	n/a	System alias for the SRM system for Purchasing applications
SAP_SRM_HTTP	No	HTTP connection	n/a	System alias for the SRM system for Purchasing applications
SAP_EREC_TalentManagement	No	ABAP connection	n/a	System alias for the SAP E-Recruiting system
SAP_EREC_TalentManagement_HTTP	No	HTTP connection	n/a	System alias for the SAP E-Recruiting system

Business Package for Employee Self-Service (WDA)

For this deployment option, you have to maintain system aliases in the Portal System Landscape Administration, see also the following table 2.

Table 2: Connection Destinations for the Business Package for Employee Self-Service (WDA)

Destination	Delivered	Type	Recommended User Authorization	Description
SAP_ECC_HumanResources	Yes	Entry in Portal System Landscape Administration	n/a	System alias for the ECC HCM system
SAP_SRM	Yes	Entry in Portal System Landscape Administration	n/a	System alias for the SRM system for Purchasing applications
SAP_EREC_TalentManagement	Yes	Entry in Portal System Landscape Administration	n/a	System alias for the SAP E-Recruiting system

More Information

For the Business Package for Employee Self-Service (WDA):

- [Setting Up the System Landscape](#)

For the Business Package for Employee Self-Service:

- [Setting Up the System Landscape](#)

13.3.4.3.4.5 Internet Communication Framework Security

Use

You should only activate those services that are needed for the applications running in your system. For Employee Self-Service (WDA), the following services are needed which, unless stated otherwise, you can find in the path `default_host/sap/bc/webdynpro/sap/`:

For general ESS applications:

- HRESS_A_MENU
- HRESS_A_PERSINFO
- hress_a_payslip
- HRESS_A_TCS

For applications from *HCM Processes and Forms* (PA-AS):

- asr_form_display
- ars_personnel_file
- asr_processes_display

- ASR_PROCESS_EXECUTE_FPM

For applications from *Cross-Application Time Sheet* (CA-TS) and *Personal Time Management* (PT):

- hress_a_cats_1
- hress_a_cats_print
- hress_a_corrections
- hress_a_lea_team_calendar
- hress_a_ptarq_leavreq_appl
- HRESS_A_PTARQ_TIMEACC
- HRESS_A_TIME_DATESEL
- hress_a_time_persel

For applications from *Benefits* (PA-BN):

- HRESS_A_BEN_PART_OVERVIEW
- HRESS_A_BENEFITS_ENROLLMENT
- HRESS_A_BEN_PRINT_ENRO_FORM
- HRESS_A_BEN_FSA_CLAIMS
- HRESS_A_BEN_PRINT_ENRO_FORM
- HRESS_A_BEN_PRINT_CONF_FORM

For applications from *Performance Management* (PA-PD-PM):

- HAP_CONFIGURATION
- HAP_DOCUMENT_LINK
- HAP_MAIN_DOCUMENT
- HAP_QUALIFICATION_PROFILE
- HAP_START_PAGE_POWL_UI_ESS
- HAP_a_ESS_Startpage

For applications from *Travel Management* (FI-TV):

- FITE_EXPRESS_EXPENSES
- FITE_REQUEST_DELETE
- FITE_EXPENSES_DELETE
- FITP_PLAN_CANCEL
- FITV_UNLOCK_PERSNO
- FITV_TRIP_FORM
- FITV_ROUTING
- FITP_PROFILE
- FITE_REQUEST
- FITP_PLANNING FITE_EXPENSES
- FITV_POWL_TRIPS

And in the path default_host /sap/bc/bsp/sap/ :

- fitv_bsp_pfcg

For applications from *Self-Service Procurement* (SRM-EBP-SHP) in the path /default_host/sap/bc/webdynpro/sapsrm/:

- WDA_L_FPM_OIF
- WDA_L_FPM_OVP
- WDA_L_PRINT_PREVIEW

For applications from *ERP E-Procurement* (MM-PUR-SSP):

- /SRMERP/WDA_I_SC_ESS
- /SRMERP/WDA_I_SC_FS_ESS
- /SRMERP/WDA_I_WSCP

For applications from *SAP E-Recruiting* (PA-ER):

- All services with the prefix hrrcf in the path /default_host/sap/bc/webdynpro/sap/
- All services in the path /default_host/sap/bc/erecruiting/
- All services with the prefix hrrcf_wd in the path /default_host/sap/bc/bsp/sap/

i Note

You activate the services in Customizing for SAP E-Recruiting under ► [Technical Settings](#) ► [User Interfaces](#) ► [Candidate](#) ► [Front-End Candidate](#) ► [Specify E-Recruiting Services \(Web Dynpro ABAP\)](#) ►.

For country-specific applications:

- HRESS_A_PAYINFO
- HRESS_A_REP_AU_PS
- Hress_a_rep_ca_tfr
- HRESS_A_REP_CH_PKB1
- HRESS_A_REP_CH_PKB4
- HRESS_A_REP_CN_CTXD
- HRESS_A_REP_HK_IR56B
- HRESS_A_REP_HK_IR56F
- HRESS_A_REP_HK_IR56G
- HRESS_A_REP_IN_FORM16
- HRESS_A_REP_JP_YEA_DEP
- HRESS_A_REP_JP_YEA_INS
- HRESS_A_REP_JP_YEA_WTS
- HRESS_A_REP_MY_EA
- HRESS_A_REP_MY_PCB2
- HRESS_A_REP_PT_IID
- HRESS_A_REP_SG_IR21
- HRESS_A_REP_SG_IR8A
- HRESS_A_REP_SG_IR8E
- HRESS_A_REP_SG_IR8S
- HR_EA_A_OVERVIEW_EE
- HR_EA_A_OVERVIEW_CU

- HR_EA_A_OVERVIEW_AP
- HR_EA_A_OVERVIEW_TO
- HRESS_A_REP_IN_SSITP
- HRESS_A_CLAIM_IN
- HRESS_A_ITDCL_IN
- HRESS_FWS_EMP_CALENDAR
- ASR_PROCESS_EXECUTE_FPM

Activities

Use the transaction `SICF` to activate these services.

If your firewalls use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

More Information

For more information, see *Activating and Deactivating ICF Services* in the SAP NetWeaver Library documentation.

For more information about ICF security, see the RFC/ICF Security Guide.

13.3.4.3.4.6 Leave Request-Specific Virus Scan Profile (ABAP)

Attackers can abuse a file upload to modify displayed application content or to obtain authentication information from a legitimate user. Usually, virus scanners are not able to detect files designed for this kind of attack.

For this reason, the standard SAP Virus Scan Interface includes an enhancement option to protect the user and/or the SAP system from potential attacks.

For more information about the behavior of the virus scanner when default virus scan profiles (VSP) are activated, see SAP note [1693981](#) (Unauthorized modification of displayed content).

SAP *Leave Request* Application (`HRESS_A_PTARQ_LEAVREQ_APPL`) changes this behavior so that the file types (`EXE`, `RAR`, `DLL`) are blocked.

When you have created and activated the application-specific virus scan profile (`SIHTTP/HTTP_UPLOAD`), this profile produces the following impact: The MIME sniffing check is activated, and the MIME type `APPLICATION/OCTET-STREAM` will be blocked.

13.3.4.3.4.7 Security-Relevant Logging and Tracing

Employee Self-Service relies on the logging and tracing mechanisms from ABAP Platform.

For more information, see the following topics:

- For the AS ABAP (relevant for *Employee Self-Service (WDA)*):
[Auditing and Logging](#)

13.3.4.3.5 Manager Self-Service

About This Document

This chapter provides an overview of the security-relevant information that applies to Manager Self-Service (EP-PCT-MGR).

The following deployment options are available for Manager Self-Service (MSS):

- **Business Package for Manager Self-Service**
This Business Package is a “classic” SAP Business Package that runs in the SAP Enterprise Portal. The Portal role consists of worksets and iViews based on Web Dynpro ABAP technologies.
- **Manager Self-Service in SAP Business Client**
The role structure for this deployment option is maintained in the back-end system with the SAP role maintenance transaction `PF03`. All applications available with this role are based on Web Dynpro ABAP technology.

i Note

Some parts of the security information in this chapter only apply to one of the MSS deployment options. In this case, you will find a comment explaining for which deployment option this information is valid right at the beginning of each section. If not stated otherwise, the security information in this chapter applies to both MSS deployment options.

See also:

- For more information about the roles in SAP Business Client, go to https://help.sap.com/s4hana_op_2020, enter *Roles in SAP Business Client* into the search bar, press , and open the search result with that title.
- For more information about SAP Business Client, see https://help.sap.com/viewer/p/SAP_BUSINESS_CLIENT.

Overview of the Main Sections of This Chapter

This chapter comprises the following sections with security-related topics specific to Manager Self-Service:

- [Before You Start](#)
This section comprises references to other Security Guides that are relevant for Manager Self-Service and a list of the most important notes for Manager Self-Service regarding security.
- [User Administration and Authentication](#)
This section provides an overview of the following user administration and authentication aspects for Manager Self-Service:
 - [User Management](#)
This section contains information about the user types that are required by Manager Self-Service and standard users for Manager Self-Service.
 - [Integration into Single Sign-On Environments](#)
This topic describes how the Employee Self-Service supports Single Sign-On mechanisms.
- [Authorizations](#)
This section provides an overview of the authorization concept that applies to Manager Self-Service.
- [Session Security Protection](#)
This section provides information about activating secure session management, which prevents JavaScript or plug-ins from accessing the SAP logon ticket or security session cookie(s).
- [Network and Communication Security](#)
This section provides an overview of the communication paths used by Manager Self-Service and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level:
 - [Network Security](#)
 - [Communication Destinations](#)
- [Internet Communication Framework Security](#)
This section provides an overview of the Internet Communication Framework (ICF) services that are used by Manager Self-Service.
- [Security-Relevant Logging and Tracing](#)
This section provides an overview of the logging and tracing mechanisms that apply to Manager Self-Service.

13.3.4.3.5.1 User Administration and Authentication

User management for Manager Self-Service uses the mechanisms provided with the Application Server ABAP.

The security recommendations and guidelines for user administration and authentication as described in the Application Server ABAP apply for [Manager Self-Service in SAP Business Client](#).

In addition to these guidelines, information about user administration and authentication that specifically applies to Manager Self-Service is included in the following sections:

- [User Management](#)
- [Integration into Single Sign-On Environments](#)

13.3.4.3.5.1.1 User Management

Use

User management for Manager Self-Service uses the mechanisms provided with the Application Server ABAP (for example, tools, user types, and password policies).

For an overview of how these mechanisms apply for Manager Self-Service, see the sections below.

User Administration Tools

The table below shows the tools to use for user management and user administration with Manager Self-Service.

User Management Tools

Tool	Detailed Description	Comment
User maintenance for ABAP-based systems (transaction SU01)	You use the user maintenance transaction to generate users in the ABAP-based systems.	Used for both MSS deployment options
Role maintenance (transaction PFCG)	You use the role maintenance transaction to generate profiles for your self-service users. For more information, see User and Role Administration of AS ABAP .	Used for both MSS deployment options

i Note

For the [Business Package for Manager Self-Service](#), it is necessary to perform user mapping for the users in the ABAP system and the Portal. For more information, see [Assigning Portal Roles to Users](#).

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively must change their passwords on a regular basis, but not those users under which background processing jobs run.

The user types that are required for the Manager Self-Service are Individual users:

- Dialog users (Used for SAP GUI for Windows or RFC connections)
- Internet users (Same policies apply as for dialog users, but used for Internet connections).

For more information about these user types, see User Types in the AS ABAP Security Guide.

→ Recommendation

For the *Business Package for Manager Self-Service*, we recommend you set up the connection between the SAP Enterprise Portal and the connected systems (ECC system, J2EE Engine, BI system) so that each individual user has access. This does not apply to *Manager Self-Service in SAP NWBC*.

Standard Users

For Manager Self-Service, no standard users are delivered.

13.3.4.3.5.1.2 Integration into Single Sign-On Environments

Use

Manager Self-Service supports the Single Sign-On (SSO) mechanisms provided by ABAP Platform. Therefore, the security recommendations and guidelines for user administration and authentication as described in the ABAP Platform Security Guide also apply to Manager Self-Service.

For more information about the available authentication mechanisms, see *User Authentication and Single Sign-On* and [Integration into Single Sign-On Environments \[page 13\]](#).

Configuration of Web Services with Client Certificates

For MSS applications of the *Business Package for Manager Self-Service*, the use of client certificates should be configured for authentication when users access the J2EE Engine using an end-to-end connection. To achieve this, follow the instructions under [Configuring the Use of Client Certificates for Authentication](#).

13.3.4.3.5.2 Authorizations

Use

Manager Self-Service uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the Application Server ABAP Security Guide also apply to Manager Self-Service. The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF03`) on the AS ABAP.

i Note

For more information about how to create roles, see [Role Administration](#).

Role and Authorization Concept for Manager Self-Service

Manager Self-Service embraces services from a variety of SAP applications and also uses the authorizations of these individual components. Many services belong to HCM components, see [Authorizations for Human Resources](#).

→ Recommendation

For Manager Self-Service, we highly recommend that you use the HCM-specific structural authorization check in addition to the general SAP authorization check. For more information see SAP Library for SAP S/4HANA on SAP Help Portal at [Human Resources > HR Tools > Authorizations for Human Resources > Structural Authorization Check](#).

Standard Roles

The table below shows the standard roles that are used for authorizations by Manager Self-Service.

Standard Roles for Manager Self-Service

Role	Description
SAP_ASR_MANAGER	Authorizations for the functions of the PA-AS component (HR Administrative Services) for line managers in Manager Self-Service.
SAP_TIME_MGR_XX_ESS_WDA_1	Authorizations for line managers in Manager Self-Service for services used to approve leave requests and working times from Employee Self-Service (WDA).
SAP_TMC_MANAGER	Authorizations for managers relating to Talent Management activities. For more information, see Manager in Talent Management . The structural authorization profile TMS_MAN_PROF is also available as a template for the manager. For more information, see Customizing for Talent Management and Talent Development under Basic Settings → Authorizations in Talent Management → Define Structural Authorizations .
SAP_RCF_MANAGER	Authorizations for the Manager role, which enables access to SAP E-Recruiting from the Portal (Manager Self Service).
SAP_MANAGER_MSS_OTH_NWBC	Authorizations for remote system applications including applications from SAP E-Recruiting.

Role	Description
SAP_HR_LSO_HR-MANAGER	Authorizations for the applications of the HR Manager Training role of the SAP Learning Solution component.
SAP_HR_LSO_MANAGER	Authorizations for the applications of the Manager role of the SAP Learning Solution component.
SAP_FI_TV_WEB_APPROVER	Authorizations for applications of the Travel Approver role of the SAP Travel Management component.
SAP_HR_CPS_DET_PLAN_L_SR_NWBC	Authorizations for applications of the manager role of the Personnel Cost Planning component.
SAP_SR_MSS_FIN_5	Authorizations for the Financials applications in Manager Self-Service.

⚠ Caution

For the *Business Package for Manager Self-Service*, you also need SAP Note [844639](#) for generating the authorization profiles.

i Note

The composite role `SAP_MANAGER_MSS_NWBC`, which contains the single roles listed above, is required for *Manager Self-Service in SAP Business Client*.

Standard Authorization Objects

The following section provides an overview of the security-relevant authorization objects that are used by Manager Self-Service.

Standard Authorization Objects for the Business Package for Manager Self-Service

Authorization Object	Field	Value	Description
S_RFC	RFC_NAME	Depends on service	Saves data from RFC access to Web Dynpro front end to the back-end system.

Standard Authorization Objects for Controlling Services in MSS (Both Deployment Options)

Authorization Object	Description
K_CCA	General authorization object for Cost Center Accounting. Is checked in the relevant Monitor iViews, Master Data iViews, and Express Planning services.

Authorization Object	Description
K_ORDER	<p>General authorization object for internal orders.</p> <p>Is checked in the relevant Monitor iViews, Master Data iViews, and Express Planning services.</p>
K_PCA	<p>Area responsible, Profit Center.</p> <p>Is checked in the relevant Monitor iViews, Master Data iViews, and Express Planning services.</p>
K_CSXS_PLA	<p>Cost element planning.</p> <p>Is checked in the relevant Express Planning services.</p>
K_FPB_EXP	<p>Authorization object for Express Planning.</p> <p>This authorization object checks the Express Planning Framework call and the planning round call. The actual plan data is protected by the authorization objects for the individual Express Planning services.</p>

i Note

For more information about the fields for the authorization objects K_CCA, K_ORDER, and K_PCA, see SAP Note [15211](#).

Apart from these authorization objects, both Manager Self-Service deployment options use the authorization objects from the following application areas or application components:

- *Human Capital Management*
See the SAP S/4HANA Security Guide at [▶ Human Capital Management ▶ Authorizations ▶](#).
- *SAP E-Recruiting*
See the SAP S/4HANA Security Guide at [▶ Human Capital Management ▶ Talent Management ▶ SAP E-Recruiting ▶ Authorizations ▶](#).
- *HCM Processes and Forms*
See the SAP S/4HANA Security Guide at [▶ Human Capital Management ▶ Personnel Administration \(PA\) ▶ HCM Processes and Forms ▶ Authorizations ▶](#).
- *Travel Management*
See the SAP S/4HANA Security Guide at [▶ Accounting ▶ Financial Accounting ▶ Travel Management \(FI-TV\) ▶](#).

Authorizations for Business Intelligence (BI) iViews (BP MSS)

For the BI iViews in the *Business Package for Manager Self-Service*, users need the standard BI authorizations for executing queries. For more information, see [Authorization Check When Executing a Query](#) (in the *Data Warehouse Management* section of the documentation for SAP NetWeaver Business Intelligence).

In Human Capital Management, BI queries use a BI variable for personalization. Data is read from the DataStore object for personalization `OPERS_VAR`. If required, you can fill this DataStore Object from structural authorizations (see [Structural Authorizations - Values \(0PA_DS02\)](#) and [Structural Authorizations - Hierarchy \(0PA_DS03\)](#)).

13.3.4.3.5.3 Session Security Protection

Use

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management.

We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

The following section is relevant for [Manager Self-Service in SAP Business Client](#):

To prevent access in javascript or plug-ins to the SAP logon ticket and security session cookies (`SAP_SESSIONID_<sid>_<client>`), activate secure session management. With an existing security session, users can then start applications that require a user logon without logging on again. When a security session is ended, the system also ends all applications that are linked to this security session.

Use the transaction `SICF_SESSIONS` to specify the following parameter values shown in the table below in your AS ABAP system:

Session Security Protection Profile Parameters

Profile Parameter	Recommended Value	Comment
<code>icf/ set_HTTPOnly_flag_on_cookies</code>	0	Client-Dependent
<code>login/ticket_only_by_https</code>	1	Not Client-Dependent

For more information, including a list of the relevant profile parameters and detailed instructions, see [Activating HTTP Security Session Management on AS ABAP](#) in the AS ABAP security documentation.

13.3.4.3.5.4 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and application level) or network attacks such as eavesdropping. If users cannot log on to your

application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the back-end system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for Manager Self-Service is based on the topology used by the ABAP Platform. Therefore, the security guidelines and recommendations described in the ABAP Platform Security Guide also apply to Manager Self-Service. Details that specifically apply to Manager Self-Service are described in the following topics:

- **Network Security**
This topic describes the recommended network topology for Manager Self-Service. It shows the appropriate network segments for the various client and server components and where to use fire walls for access protection. It also includes a list of the ports needed to operate Manager Self-Service.
- **Communication Destinations**
This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the ABAP Platform Security Guide:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

13.3.4.3.5.4.1 Network Security

Ports

Manager Self-Service runs on SAP NetWeaver and uses the ports from the AS ABAP (for *Manager Self-Service in SAP NWBC*).

For more information, see the topic for AS ABAP Ports in the corresponding ABAP Platform Security Guides.

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see <https://help.sap.com/viewer/ports>.

13.3.4.3.5.4.2 Communication Destinations

The tables below provide an overview of the communication destinations required for the MSS deployment options.

Manager Self-Service in SAP Business Client

For this deployment option, you have to maintain RFC connections using the transaction SM59, see also the following table 1.

Table 1: Connection Destinations for Manager Self-Service in SAP Business Client

Destination	Delivered	Type	Recommended User Authorizations	Description
SAP_ECC_HumanResources	No	ABAP connection	n/a	System alias for the ECC HCM system
SAP_ECC_HumanResources_HTTP	No	HTTP connection	n/a	System alias for the ECC HCM system
SAP_ECC_FINANCIALS	No	ABAP connection	n/a	System alias for the ECC FI system for Financials applications
SAP_ECC_FINANCIALS_HTTP	No	HTTP connection	n/a	System alias for the ECC FI system for Financials applications
SAP_EREC_TalentManagement	No	ABAP connection	n/a	System alias for the SAP E-Recruiting system
SAP_EREC_TalentManagement_HTTP	No	HTTP connection	n/a	System alias for the SAP E-Recruiting system

13.3.4.3.5.5 Internet Communication Framework Security

Use

You should only activate the services needed for the applications running in your system. For Manager Self-Service in SAP Business Client, the following services are needed which you can find under the path `default_host/sap/bc/webdynpro/sap/`:

For applications from the *Suite Inbox* (CA-EPT-IBO):

- IBO_WDA_INBOX

For applications from *HCM Processes and Forms* (PA-AS):

- asr_form_display
- asr_mass_start_process
- asr_pa_pd_processes_display
- asr_processes_display
- ASR_PROCESS_EXECUTE_FPM
- asr_process_select
- asr_srch_pd_process

For applications from *Cross-Application Time Sheet* (CA-TS) and *Personal Time Management* (PT):

- HRMSS_A_CATS_APPROVAL
- HRESS_A_PTARQ_LEAVREQ_APPL
- HRESS_A_LEA_TEAM_CALENDAR

For applications from *Talent Management and Talent Development* (PA-TM):

- HRTMC_EMPLOYEE_PROFILE
- HRTMC_LONG_PROFILE
- hrtmc_side_by_side
- HRTMC_TA_ASSESSMENT
- HRTMC_TA_DASHBOARD
- HRTMC_TA_DEV_PLAN
- hrtmc_teamviewer

For applications from *Performance Management* (PA-PD-PM):

- HAP_MAIN_DOCUMENT
- HAP_START_PAGE_POWL_UI_MSS
- HAP_A_PMP_PIE_CHART
- HAP_A_PMP_GOALS
- HAP_A_PMP_OVERVIEW
- HAP_A_PMP_MAIN

For applications from *Enterprise Compensation Management* (PA-ECM):

- HCM_ECM_PLANNING_OVERVIEW_OIF
- HCM_ECM_PLANNING_UI_GAF
- HCM_ECM_PROFILE_OIF
- HCM_ECM_SIDEBYSIDE_OIF
- HCM_ECM_TEAMVIEWER_OIF

For applications from *Personnel Cost Planning* (PA-CP):

- WDA_HCP_DET_PLAN

For applications from *SAP Learning Solution* (PE-LSO):

- LSO_MANAGE_PARTICIPANTS
- LSO_MANAGE_MANDATORY_ASSIGN

For applications from *SAP E-Recruiting* (PA-ER):

- default_host/sap/bc/erecruiting/dataoverview
- hrrcf_a_dataoverview
- hrrcf_a_requi_monitor
- hrrcf_a_req_assess
- hrrcf_a_tp_assess
- hrrcf_a_qa_mss
- hrrcf_a_substitution_manager
- hrrcf_a_substitution_admin

i Note

You activate the services in Customizing for SAP E-Recruiting at [▶▶ Technical Settings ▶ User Interfaces ▶ Manager Involvement ▶ Specify E-Recruiting Services for MSS ▶](#).

For applications from *Travel Management* (FI-TV):

- FITV_POWL_APPROVER
- FITV_TRIP_FORM
- FITV_POWL_PERSONALIZATION

For applications from the *Financials* (FI) application area:

- QISR_UI_STATUSOVERVIEW
- QISR_UI_STATUSOVERVIEW
- QISR_UI_STATUSOVERVIEW
- FPB_EXP_OVERVIEW
- FCOM_PBC_MONITOR
- FCOM_PBC_MONITOR
- FPB_VARIANCE_MONITOR_OVERVIEW
- FCOM_EQM_MONITOR
- FPB_LINEITEM_MONITOR_OVERVIEW
- FPB_VARIANCE_MONITOR_OVERVIEW
- FPB_LINEITEM_MONITOR_OVERVIEW
- FCOM_EQM_MONITOR
- FCOM_PBC_MONITOR
- FCOM_PBC_MONITOR
- FPB_LINEITEM_MONITOR_OVERVIEW
- FPB_VARIANCE_MONITOR_OVERVIEW

Activities

Use the transaction SICF to activate these services.

If your firewalls use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

More Information

For more information, see *Activating and Deactivating ICF Services* in the SAP NetWeaver Library documentation.

For more information about ICF security, see the *RFC/ICF Security Guide* .

13.3.4.3.5.6 Security-Relevant Logging and Tracing

Manager Self-Service relies on the logging and tracing mechanisms from ABAP Platform.

For more information, see the following topics:

- For the AS ABAP (relevant for *Manager Self-Service in SAP Business Client*):
 - Auditing and Logging
 - Tracing and Logging (for NWBC)

13.3.5 Talent Management

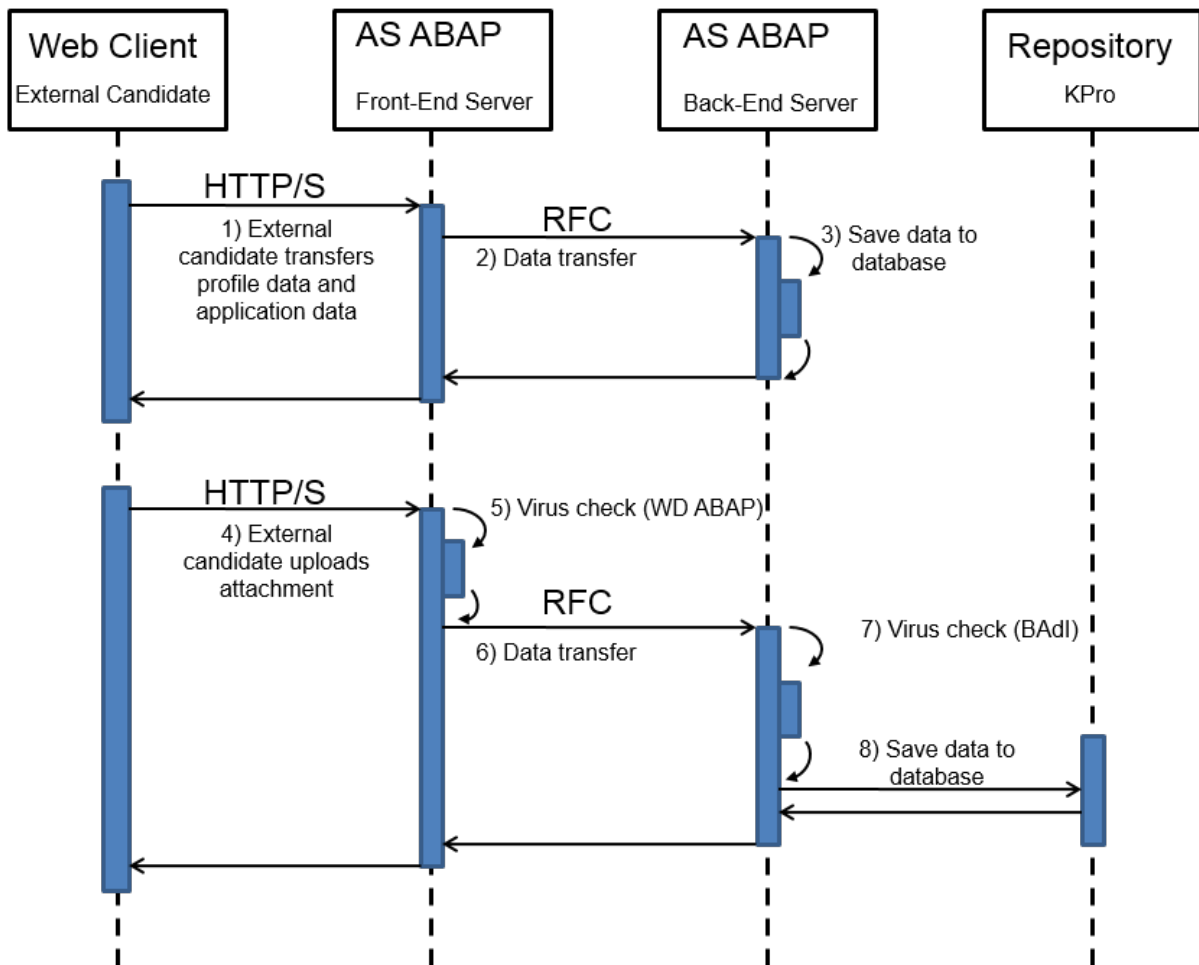
13.3.5.1 SAP E-Recruiting

13.3.5.1.1 Security Aspects of Data Flow and Processes

The following section provides an overview of the data flows in the security-relevant scenarios for SAP E-Recruiting.

13.3.5.1.1.1 Data Entry by External Candidate in Distributed System

The figure below provides an overview of the data flow for the following scenario: Data entry by the external candidate in the distributed system



The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Measure
1	External candidate transfers profile data and application data	External candidate has to confirm the data privacy statement.
2	Data transfer	Access authorization using RFC user
3	Save data to database	Not relevant
4	External candidate uploads attachments	Not relevant
5	Virus check (WD ABAP)	Standard virus check provided by SAP NetWeaver Application Server (front-end server)
6	Data transfer	Not relevant

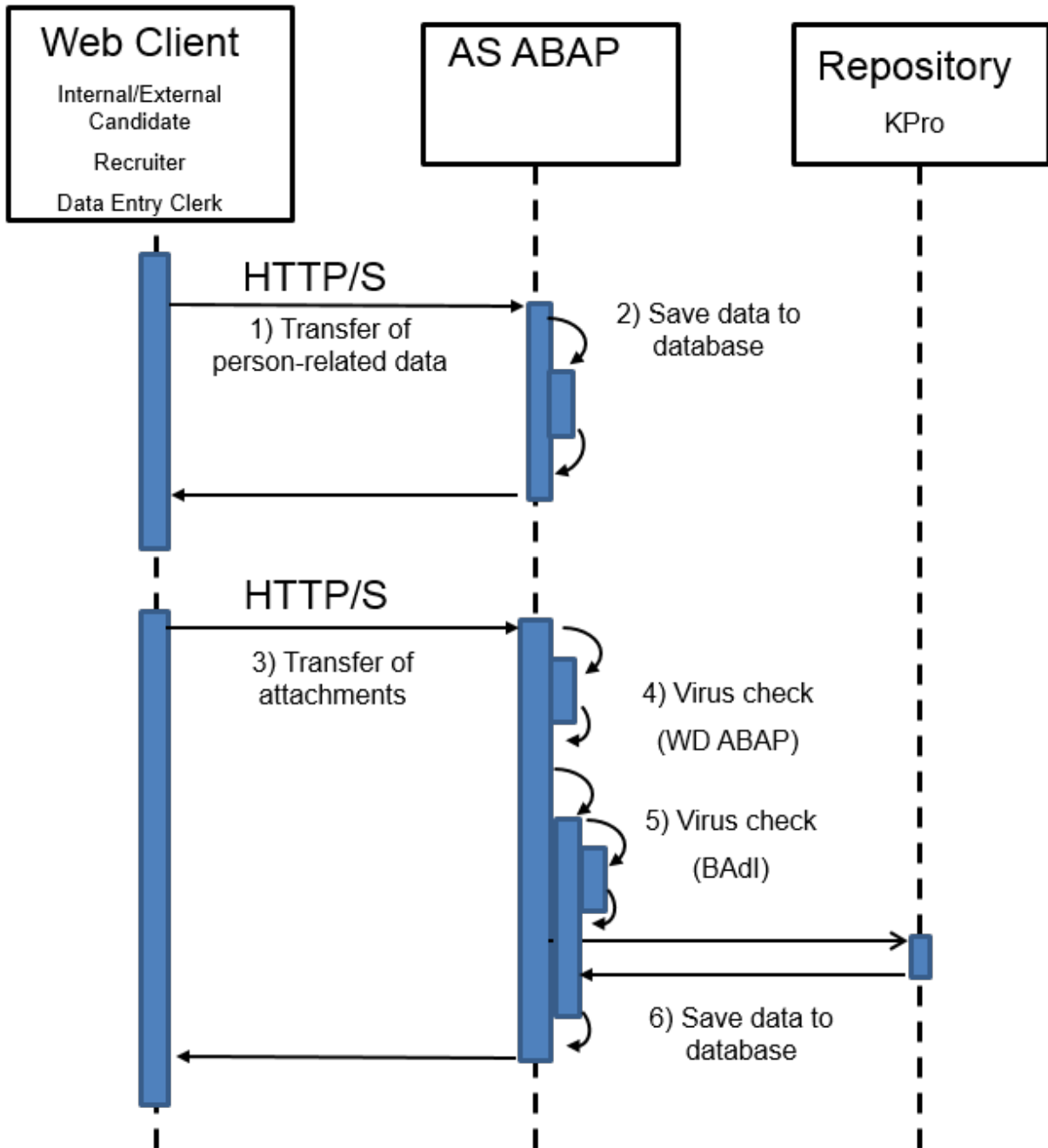
Step	Description	Security Measure
7	Virus check (BAI)	Additional virus check using the BAI HRRCF00_ DOC _UPLOAD (back-end server) (see Customizing activity BAI:Upload Documents)
8	Save data to database	Not relevant

13.3.5.1.1.2 Data Entry in Nondistributed System

The figure below provides an overview of the data flow for the following scenario: Data entry in nondistributed system.

The data flow is relevant within the framework of the following scenarios:

- The internal or external candidate maintains his or her profile and application.
- The recruiter maintains a candidate's profile.
- The recruiter or data entry clerk enters an application in the system.



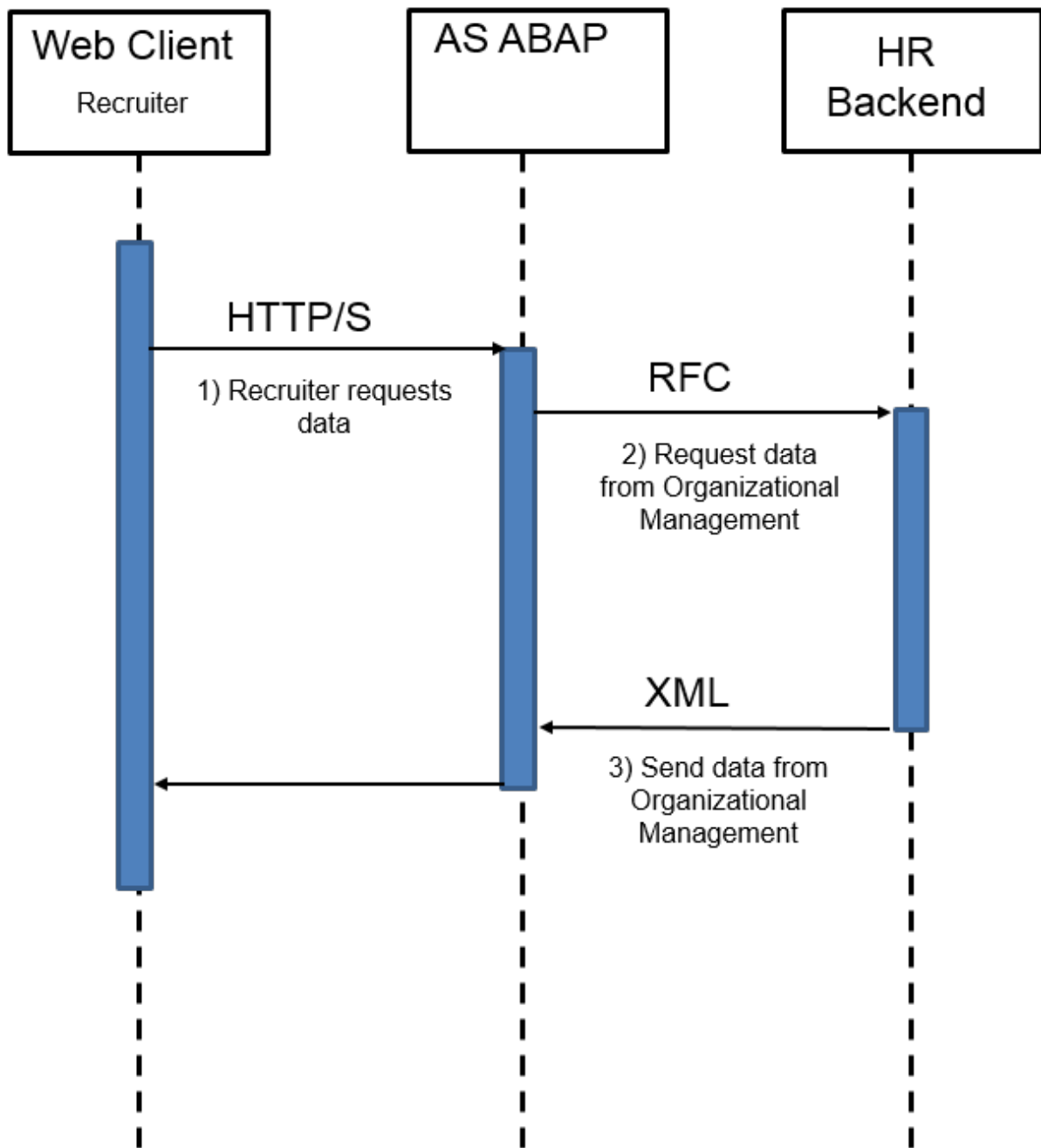
The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Measure
1	Transfer of data	External candidate has to confirm the data privacy statement.
2	Save data to database	Not relevant

Step	Description	Security Measure
3	Transfer of attachments	Not relevant
4	Virus check (WD ABAP)	Standard virus check provided by SAP NetWeaver Application Server (front-end server)
5	Virus check (BAI)	Additional virus check using the BAI HRRCF00_DOC_UPLOAD (back-end server) (see Customizing activity BAI:Upload Documents)
6	Save data to database	Not relevant

13.3.5.1.1.3 Integration of Org. Mgmt/E-Recruiting in Distributed System

The figure below provides an overview of the data flow for the following scenario: Integration of Organizational Management in SAP E-Recruiting in a distributed system.



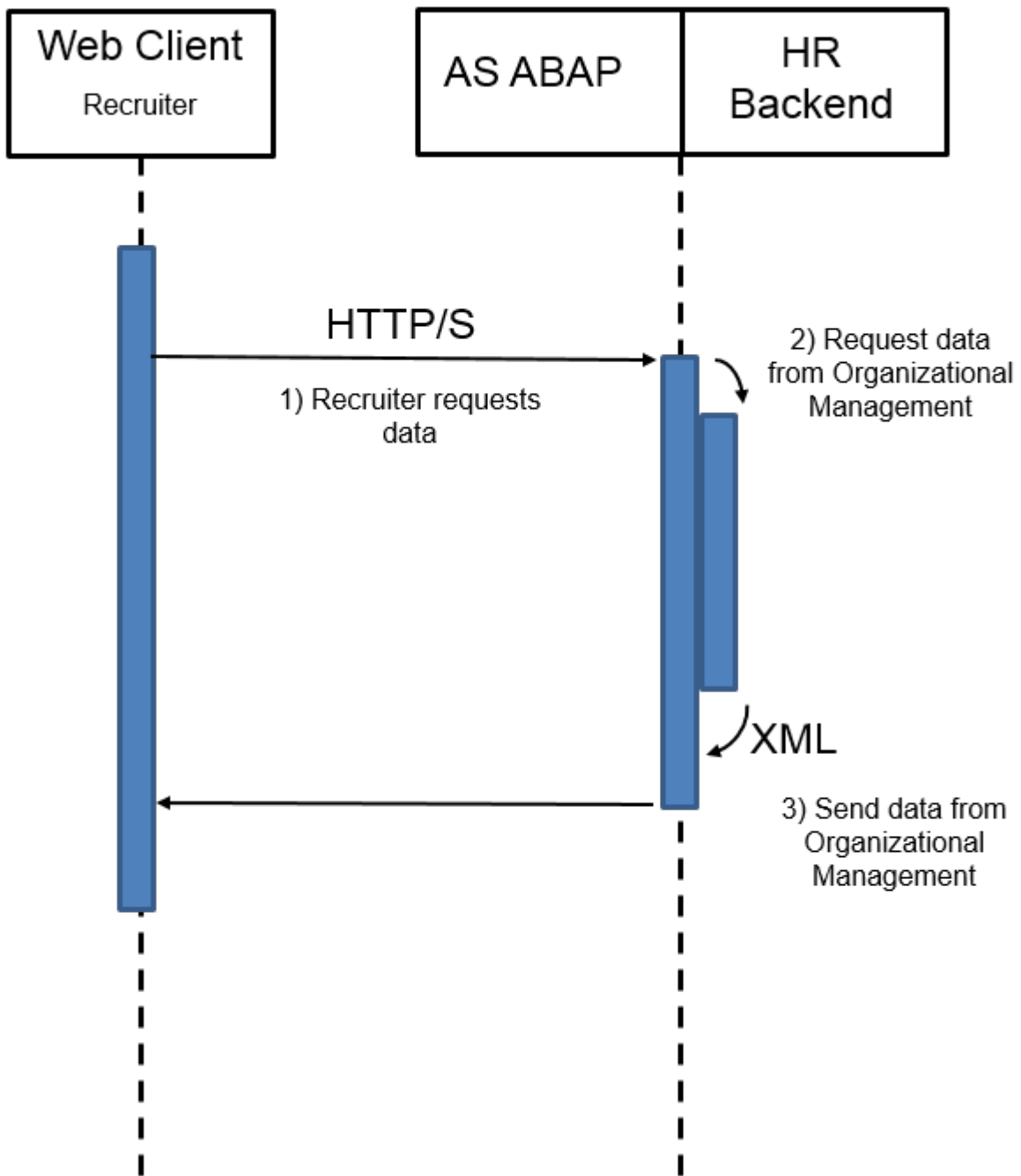
The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Measure
1	The recruiter requests data overviews for organizational units, positions, or jobs.	Not Relevant

Step	Description	Security Measure
2	The SAP NetWeaver Application Server requests the Organizational Management data using RFC in the connected HR system.	Access authorization using RFC user
3	The HR system transfers the data using XML to the SAP NetWeaver Application Server.	XML encryption

13.3.5.1.1.4 Integration of Org. Mgmt/E-Recruiting in Integrated System

The figure below provides an overview of the data flow for the following scenario: Integration of Organizational Management in SAP E-Recruiting in an integrated system.



The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Measure
1	The recruiter requests data overviews for organizational units, positions, or jobs.	Not Relevant

Step	Description	Security Measure
2	The SAP NetWeaver Application Server requests the Organizational Management data in the integrated HR system.	Not relevant
3	The integrated HR system transfers the data using XML to the SAP NetWeaver Application Server.	XML encryption

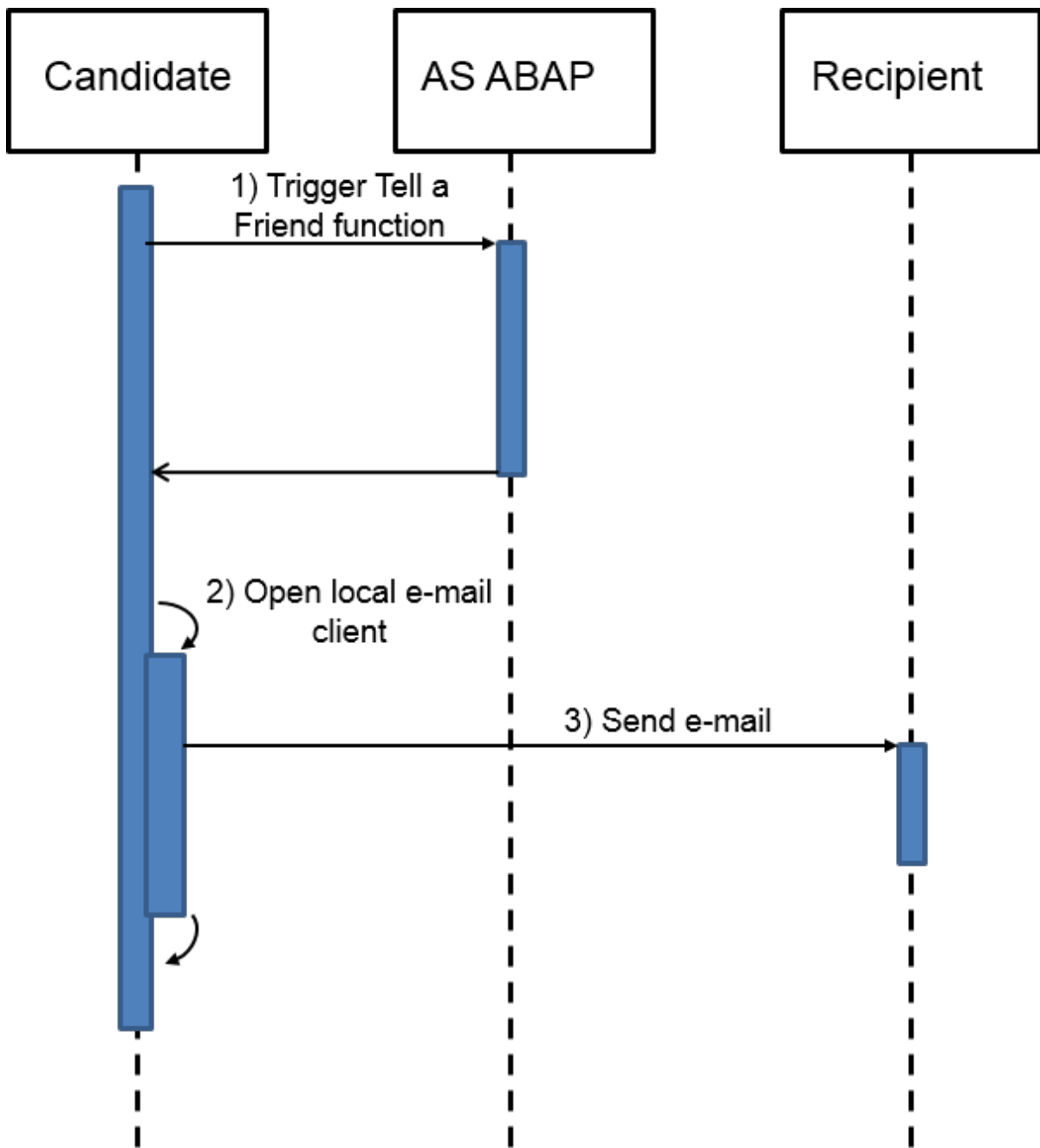
13.3.5.1.1.5 Recommendation of Job Posting (Tell a Friend)

The figure below provides an overview of the data flow for the following scenario: The candidate uses the *Tell A Friend* function to inform another person about an employment opportunity.

The process runs as described below if you enter the value MAILTO or MAILTO_REGONLY for the parameter TF_SEND_METHOD in Customizing for SAP E-Recruiting under *Technical Settings* → *User Interfaces* → *Candidate* → *Backend Candidate* → *Assign Values to Interface Parameters (Web Dynpro ABAP)*.

We recommend that you do not use the default delivery TF_SEND_METHOD = '' as this means that the e-mails with the recommendation letter are sent using your e-mail server. As the candidate is responsible for specifying the recipient and content of the e-mail message to be sent, undesirable content could be sent from the sender address of your e-mail server.

For more information, see the documentation for the Customizing activity *Assign Values to Interface Parameters (Web Dynpro ABAP)* and SAP Note [1390162](#).



The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

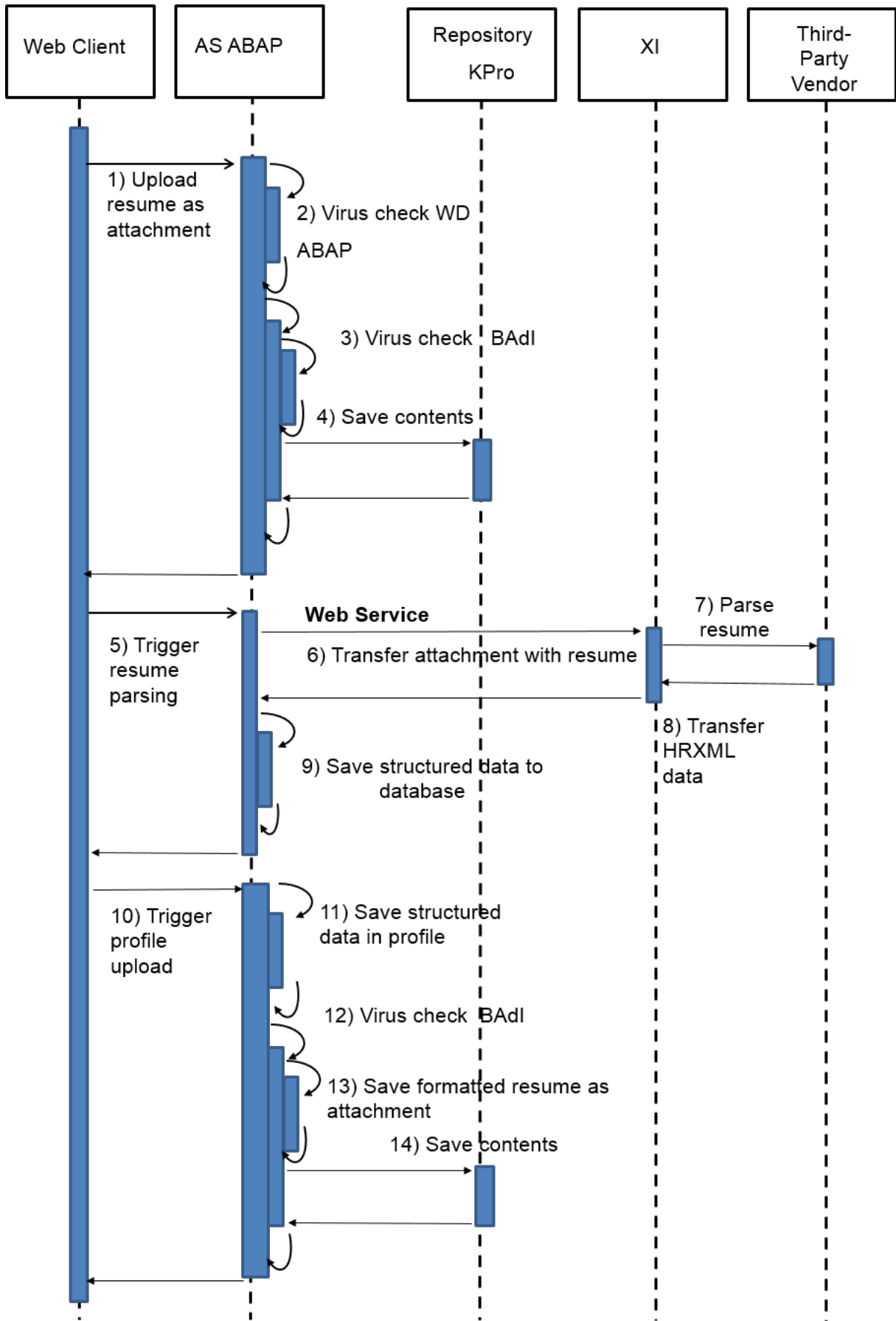
Step	Name	Security Measure
1	Trigger Tell a Friend function	Not relevant

Step	Name	Security Measure
2	Open local e-mail client	The e-mail client (for example, Microsoft Outlook) is opened locally on the candidate's computer. This client (and not the central e-mail client) then sends the e-mail. You activate this process using the parameter TF_SEND_METHOD in the Customizing activity Assign Values to Interface Parameters (Web Dynpro ABAP) .
3	Send e-mail	Not relevant

13.3.5.1.1.6 Resume Parsing (Candidate, Integrated System)

The figure below provides an overview of the data flow for the following scenario:

The candidate uploads his or her resume as an attachment and then sends it to a third-party vendor for parsing. The front end and backend for the candidate's user run on the same system.

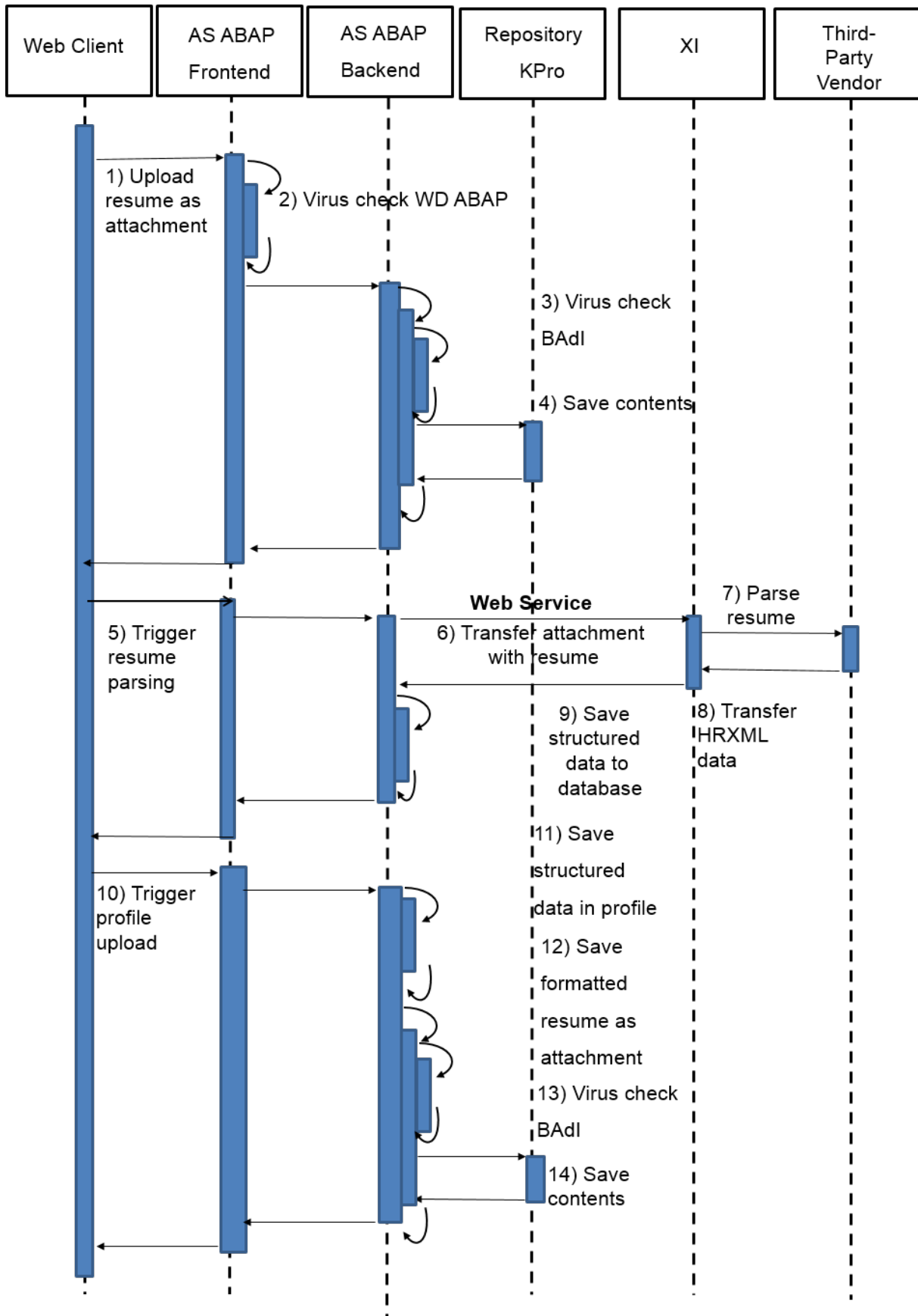


The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Name	Security Measure
1	Upload resume as attachment	Not relevant
2	Virus check WD ABAP	Standard virus check provided by SAP NetWeaver Application Server (front-end server)
3	Virus check BAdI	Additional virus check using the BAdI HRRCF00_DOC_UPLOAD (backend server) (see Customizing activity BAdI: Upload Documents)
4	Save contents	Not relevant
5	Trigger Resume Parsing	Not relevant
6	Transfer attachment with resume	Not relevant
7	Parse resume	For XI-relevant security topics, see Process Integration (PI) Security Guides .
8	Transfer HRXML data	HRXML coding
9	Save structured data to database	Not relevant
10	Trigger profile upload	Not relevant
11	Save structured data in profile	Not relevant
12	Virus check BAdI	Additional virus check using the BAdI HRRCF00_DOC_UPLOAD (backend server) (see Customizing activity BAdI: Upload Documents)
13	Save formatted resume as attachment	Not relevant
14	Save contents	Not relevant

13.3.5.1.1.7 Resume Parsing (Candidate, Distributed Scenario)

The figure below provides an overview of the data flow for the following scenario: The candidate uploads his or her resume as an attachment and then sends it to a third-party vendor for parsing. The front end and backend for the candidate's user run on different systems.



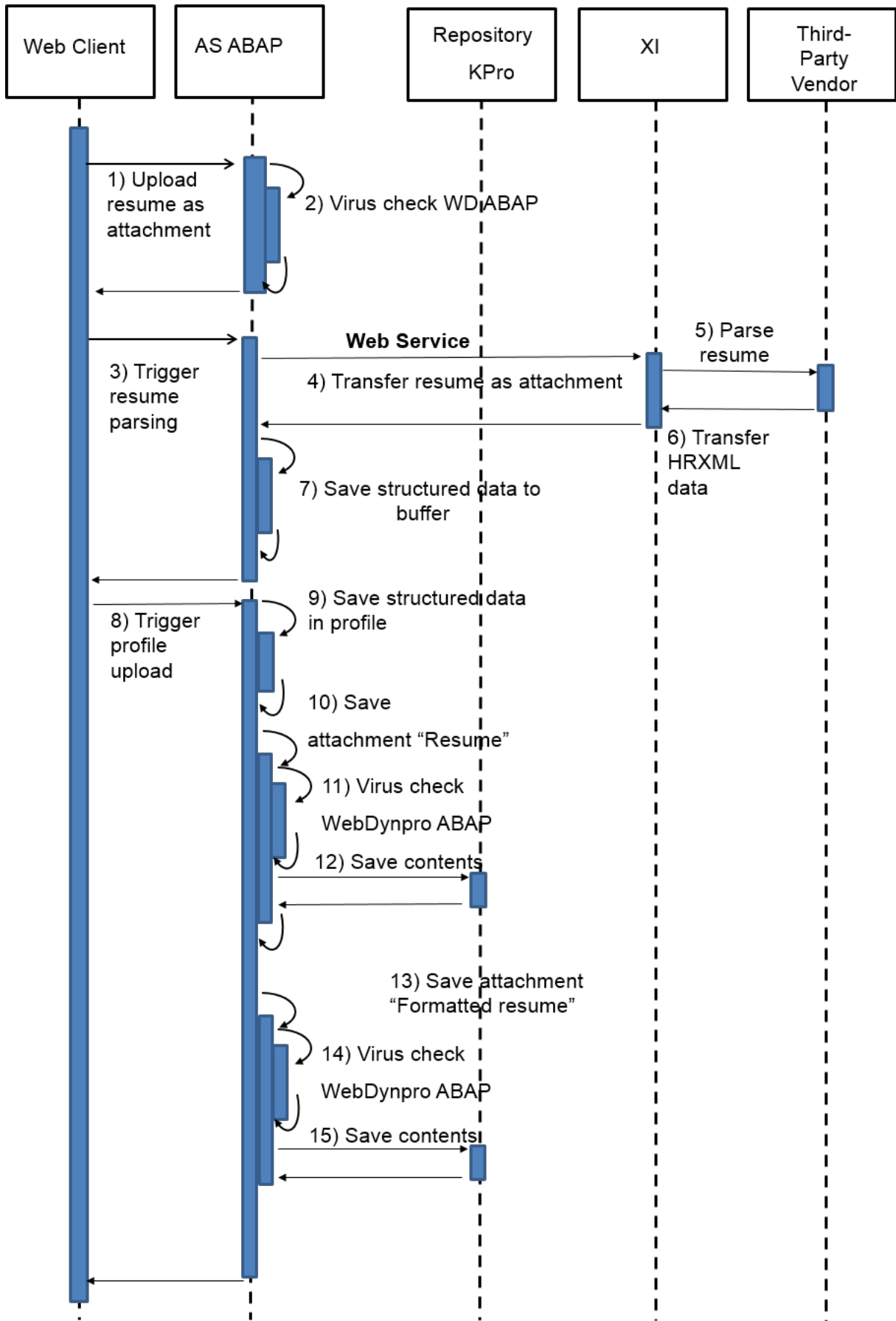
The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Name	Security Measure
1	Upload resume as attachment	Not relevant
2	Virus check WD ABAP	Standard virus check provided by SAP NetWeaver Application Server (front-end server)
3	Virus check BAdI	Additional virus check using the BAdI HRRCF00_DOC_UPLOAD (backend server) (see Customizing activity BAdI: Upload Documents)
4	Save contents	Not relevant
5	Trigger Resume Parsing	Not relevant
6	Transfer attachment with resume	Not relevant
7	Parse resume	For XI-relevant security topics, see SAP Process Integration (PI) Security Guides .
8	Transfer HRXML data	HRXML coding
9	Save structured data to database	Not relevant
10	Trigger profile upload	Not relevant
11	Save structured data in profile	Not relevant
12	Virus check BAdI	Additional virus check using the BAdI HRRCF00_DOC_UPLOAD (backend server) (see Customizing activity BAdI: Upload Documents)
13	Save formatted resume as attachment	Not relevant
14	Save contents	Not relevant

13.3.5.1.1.8 Resume Parsing (Recruiter)

The figure below provides an overview of the data flow for the following scenario:

The recruiter uploads a candidate's resume as an attachment and then sends it to a third-party vendor for parsing. The data is then transferred to the corresponding fields of the form for the *Entry of External Applications* application.

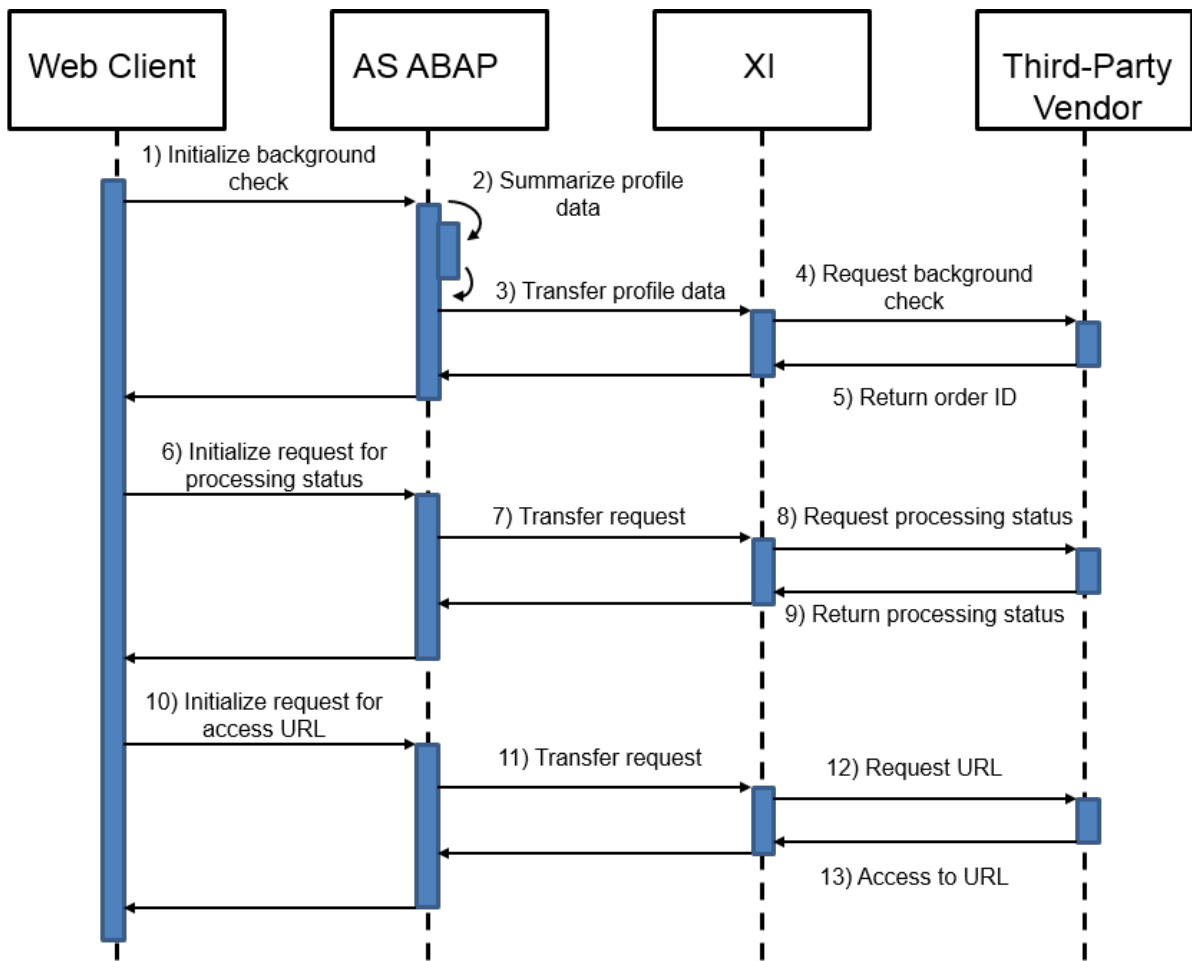


The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Name	Security Action
1	Upload resume as attachment	Not relevant
2	Virus check WD ABAP	Standard virus check provided by SAP Netweaver Application Server (front-end server)
3	Trigger Resume Parsing	Not relevant
4	Transfer resume as attachment	Not relevant
5	Parse resume	For XI-relevant security topics, see SAP Process Integration (PI) Security Guides .
6	Transfer HRXML data	HRXML coding
7	Save structured data to buffer	Not relevant
8	Trigger profile upload	Not relevant
9	Save structured data in profile	Not relevant
10	Save attachment "Resume"	Not relevant
11	Virus check WD ABAP	Standard virus check provided by SAP Netweaver Application Server (front-end server)
12	Save contents	Not relevant
13	Save attachment "Formatted resume"	Not relevant
14	Virus check WD ABAP	Standard virus check provided by SAP Netweaver Application Server (front-end server)
15	Save contents	Not relevant

13.3.5.1.1.9 Background Check

The figure below provides an overview of the data flow for the following scenario: The recruiter forwards data regarding a candidate's education, work experience, or qualifications to an external provider, who then checks that this data is correct.



The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Name	Security Measure
1	Initialize background check	Not Relevant
2	Summarize profile data	Not Relevant
3	Transfer profile data	Not Relevant
4	Request background check	For XI-relevant security topics, see: SAP Process Integration Security Guide
5	Return order ID	Not Relevant
6	Initialize request for processing status	Not Relevant
7	Transfer request	Not Relevant

Step	Name	Security Measure
8	Request processing status	For XI-relevant security topics, see: SAP Process Integration Security Guide
9	Return processing status	Not Relevant
10	Initialize request for access URL	Not Relevant
11	Transfer request	Not Relevant
12	Request URL	For XI-relevant security topics, see: SAP Process Integration Security Guide
13	Access to URL that the third-party vendor uses to display the report for the background check	Not Relevant

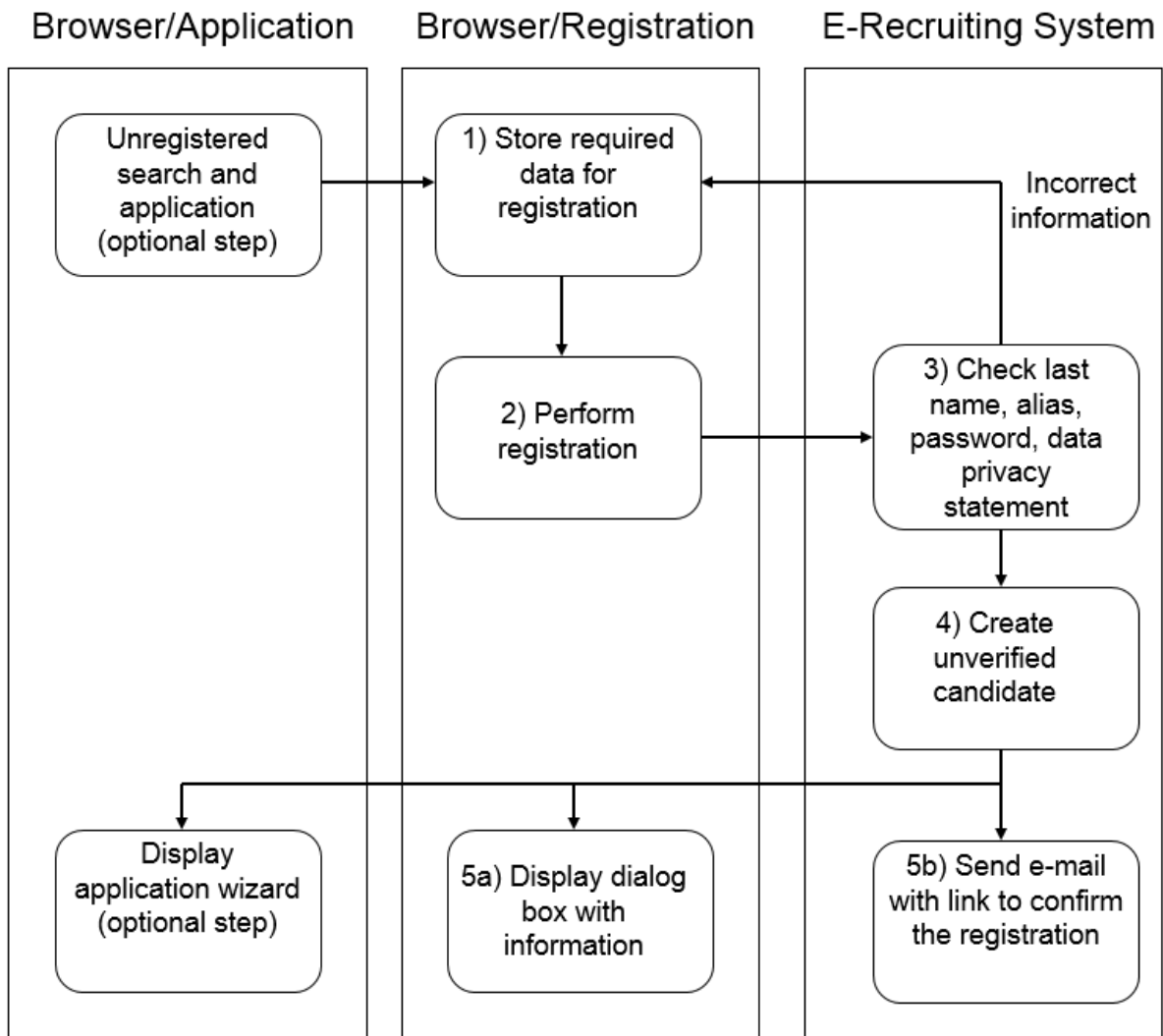
13.3.5.1.1.10 Registration Process with E-Mail Verification

The figures below provide an overview of a candidate's registration process with e-mail verification. This is relevant for persons who want to register their details in the Talent Warehouse or for persons who want to submit an application for an employment opportunity and who have to register their details first in order to do so. The process description is divided into two parts in the figures below. The first figure shows the process up to the point in time when the system sends a confirmation mail for the e-mail address. The second figure shows the process from the moment that the candidate finds this e-mail in his or her e-mail inbox.

For more information about the registration process, see section [Registration with E-Mail Verification](#) in the SAP Library for SAP S/4HANA under [Human Resources](#) > [Talent Management](#) > [SAP E-Recruiting \(PA-ER\)](#) > [Candidate](#) > [Storage of Data in Talent Warehouse](#) > [Registration](#). For more information about the application process with registration at the same time, see section [Online Application of Unregistered Candidate](#) in the SAP Library for SAP S/4HANA under [Human Resources](#) > [Talent Management](#) > [SAP E-Recruiting \(PA-ER\)](#) > [Candidate](#).

i Note

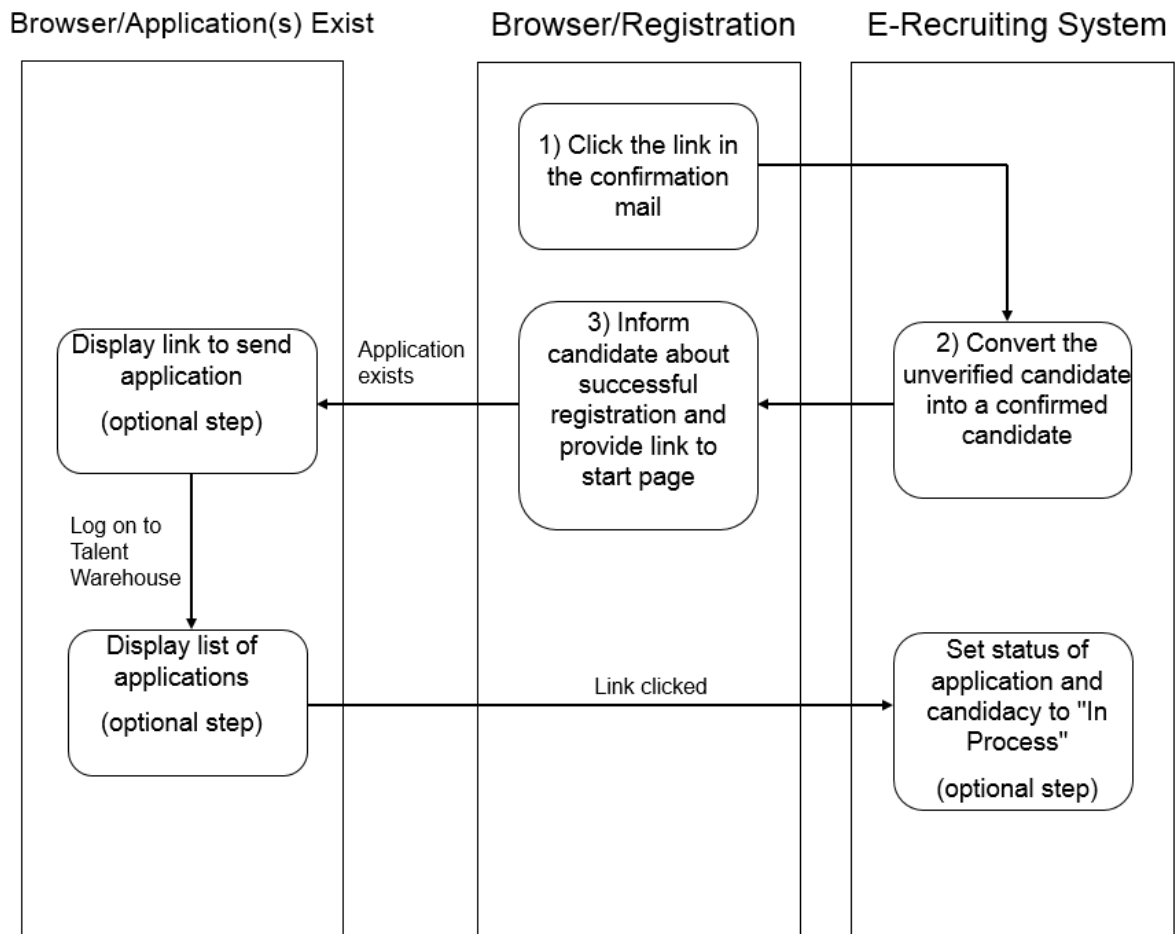
This process is relevant if the switch RECFA VERIF is set in the Customizing activity [Set System Parameters](#).



The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Action
Optional step	The unregistered candidate finds a suitable job posting and submits an application for this posting. In this case, the candidate has to register his or her details before the application can be submitted. (Continue with step 1)	For the unregistered candidate, the system uses the service user that is assigned to the corresponding ICF service in the Customizing activity Specify E-Recruiting Services (WebDynpro ABAP) .

Step	Description	Security Action
1	The unregistered candidate calls the screen page for the registration and enters the data required for the registration in the Talent Warehouse.	For the unregistered candidate, the system uses the service user that is assigned to the corresponding ICF service in the Customizing activity <i>Specify E-Recruiting Services (WebDynpro ABAP)</i> .
2	The unregistered candidate performs the registration.	
3	The system checks the information for completeness and correctness and, if applicable, asks the unregistered candidate to correct the information.	
4	The system creates an unverified candidate.	In the <i>Candidate Overview</i> infotype (5102) in the <i>Status of E-Mail Verification</i> field, the system enters the value 1 (<i>Outstanding</i>). At the same time, the system creates a user for the candidate.
5a	The system informs the candidate that the registration process was triggered and that he or she will receive a confirmation mail.	
5b	At the same time, the system sends a confirmation mail via the mail server to the e-mail address stored by the candidate. This contains a link that the candidate must use to confirm his or her e-mail address and so complete the registration.	If the user does not subsequently confirm his or her e-mail address, the user cannot access the Talent Warehouse. In the Customizing activity <i>Determine Rules for Periodic Services</i> , you can specify for how long the link for confirming the e-mail address is to be valid.
Optional step	If the candidate has registered his or her details as part of submitting an application, the system now displays the application wizard. The candidate can complete the application but cannot send it until he or she has confirmed the e-mail address and completed the registration process.	



The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Action
1	The unverified candidate finds the confirmation mail in his or her e-mail inbox, opens the mail, and clicks the link to confirm the e-mail address.	<p>In the Customizing activity <i>Determine Rules for Periodic Services</i>, you can specify the following (in addition to the validity period of the link for the confirmation):</p> <ul style="list-style-type: none"> • Period after which a reminder mail is sent to the unverified candidate • Maximum number of possible requests for a new confirmation mail • Option whether candidates can request a new confirmation mail even though the validity period of the last confirmation mail sent was exceeded

Step	Description	Security Action
2	The system converts the unverified candidate into a confirmed candidate.	In the <i>Candidate Overview</i> infotype (5102) in the <i>Status of E-Mail Verification</i> field, the system enters the value 0 (<i>Confirmed</i>).
3	The candidate is informed about the successful registration. At the same time, the candidate receives a link that he or she can use to log on to the Talent Warehouse.	For security reasons, the confirmation does not contain the password that the user needs to log on to the Talent Warehouse and which he or she entered on the registration screen.
Optional step	If the candidate registered his or her details while submitting an application and has already created one or more applications, the system displays a link that the candidate can then use to display a list of the applications.	To do this, the candidate has to log on to the Talent Warehouse with his or her user alias and password.
Optional step	The system displays a list of applications that have not yet been sent. The candidate submits an application.	The candidate can now submit applications because his or her e-mail address has now been confirmed.
Optional step	The system set the status of the application and the candidacy to <i>In Process</i> .	Recruiters can now view the application and the candidate profile.

13.3.5.1.1.11 Deregistration and Deletion of External Candidates

Definition

In SAP E-Recruiting, there is a two-step process to delete a candidate. The first step is deregistering the external candidate. The second step is deleting the candidate data from the Talent Warehouse.

This document describes how the system handles the candidate's data in the different scenarios.

i Note

If you delete the external candidates via the `HRRCF_CAND` archiving object and the functions of the *SAP Information Lifecycle Management* (ILM) at the same time with the processes described here, data inconsistencies may occur. For more information, see *Destroying Candidate Data Using HRRCF_CAND*.

Candidates delete their registration themselves

For information about the service, see [Deleting the Registration](#).

If the candidate requests the deletion of his or her own registration, the system performs the following steps:

- The *Registration of Candidate Deleted* indicator is set in infotype 5102 (Candidate Overview).
- The candidate's user is locked.
- The workflow ERCCandDerig is triggered. The workflow runs automatically in the background. For information about which data of the candidate is processed by the workflow, see the documentation for the [Workflow for Deleting a Candidate's Registration](#).

The remaining data for the candidate is retained in the database.

Administrator deletes the registration of external candidates

For information about the service, see [Deleting Registration of External Candidates](#).

If the administrator deletes the registration of an external candidate, the system performs the following steps:

- The *Registration of Candidate Deleted* indicator is set in infotype 5102 (Candidate Overview).
- The workflow ERCCandDerig is triggered. The workflow runs automatically in the background. For information about which data of the candidate is processed by the workflow, see the documentation for the [Workflow for Deleting a Candidate's Registration](#).

The remaining data for the candidate is retained in the database.

Administrator deletes the external candidates

Even after an external candidate is deregistered, the candidate's data still exists in the system. To delete the candidate completely from the system, the administrator has to delete the external candidate.

For information about the service, see [Deleting External Candidates](#).

i Note

The administrator can only delete candidates for whom there are no applications or assignments with the status *In Process* or *To Be Hired*.

When deleting data, the system also takes into account the legal time limits for retaining data (see the end of this document).

When the candidates are deleted, the associated business partners are not deleted, but are archived. You can delete business partners later using the transaction BUPA_ DEL.

If the prerequisites for the deletion are met, the system executes the following steps:

- Deletion of the candidate's applications and any related objects:
 - HR object Application

- Audit Trails
- Documents for the application in Knowledge Provider (KPro)
- Activities
- Deletion of the candidate's candidacies and any related objects:
 - HR object Candidacy
 - Documents for the candidacy in Knowledge Provider (KPro)
 - Activities
- Deletion of the job agents created by the candidate
- Deletion of the candidate and any related objects:
 - HR object Candidate
 - The candidate's user in the backend system; in the distributed system, also the candidate's user in the front-end system
 - Documents for the candidate in Knowledge Provider (KPro)
 - Activities

Delete External Candidates (report)

Another option for deleting external candidates is to use the RCF `_DELETE_EXT_ CAND` report.

You call this report in Customizing for SAP E-Recruiting under [Tools](#) → [Delete External Candidates](#). For more information, see the documentation for the Customizing activity.

We recommend you use this report instead of using the [Delete External Candidates](#) service as the report enables you to use multiple selection criteria. In this way, the user can specifically select deregistered candidates, for example.

The report is otherwise identical to the [Delete External Candidates](#) service.

Retention periods for candidate-based data

You enter the retention periods that the report has to take into account in Customizing for SAP E-Recruiting under [Store Legal Periods](#). For more information, see the documentation of the Customizing activity.

13.3.5.1.1.12 Sending E-Mails Using the Workflow

SAP E-Recruiting uses workflows that send various documents by e-mail.

The table below shows the workflows and lists the e-mails that are sent using the relevant workflows.

E-Mails Using Workflows

Workflow Template	Description	E-Mail Recipient	E-Mail Content	How E-Mail Is Sent
WS51800042	ERCAAdjEntry	-	-	-
WS51900003	ERCSendPwd	Candidate	Send password	Method
WS51900005	ERCStatusChg	Candidate	Confirmation of receipt of application	Method

Workflow Template	Description	E-Mail Recipient	E-Mail Content	How E-Mail Is Sent
		Candidate	Correspondence: Rejection	Method
		Recruiter	Notification that application is withdrawn	WF E-Mail
WS51900006	ERCCandDerig	Candidate	Confirmation that candidate has been deregistered	Method
WS51900007	ERCAprReqWD	Approver	Notification to the approver	WF E-Mail
		Requester	Notification of the decision	WF E-Mail
WS51900008	ERCObjCreate	Candidate	Acknowledge Candidate	Method
		Candidate	Verification mail	Method
WS51900009	ERCActCreate	-	-	-
WS51900010	ERCStatChg_2	Candidate	Confirmation of receipt of application	Method
		Candidate	Correspondence: Rejection	Method
		Recruiter	Notification that application is withdrawn	WF E-Mail
WS51900011	ERCActCrea_2	-	-	-
WS51900018	ERCSendVerif	Candidate	Confirmation mail	Method

13.3.5.1.2 User Administration and Authentication

SAP E-Recruiting uses the user management and authentication mechanisms provided with ABAP Platform, in particular the Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the Application Server ABAP Security Guide also apply to SAP E-Recruiting.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP E-Recruiting in the following topics:

- User Management
This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with SAP E-Recruiting.

- Integration into Single-Sign-On Environments
This topic describes how SAP E-Recruiting supports Single Sign-On mechanisms.

13.3.5.1.2.1 User Management

Definition

User management for SAPE-Recruiting uses the mechanisms provided by SAP Web Application Server ABAP such as tools, user types, and password policies. For an overview of how these mechanisms apply for SAPE-Recruiting, see the sections below.

User Administration Tools

The following table shows the tools to use for user management and user administration for *SAPE-Recruiting*.

User Management Tools

Tool	Detailed Description	Prerequisites
User and Role Maintenance (transaction PFCG)	You can use the Role Maintenance transaction PFCG to generate profiles for the SAPE-Recruiting users.	
Technical Settings for User Management in SAPE-Recruiting	For more information on user profiles and the roles, see Customizing for SAP E-Recruiting under ▶ Technical Settings ▶ User Administration .	
Workflow Settings	For more information, see the Customizing for SAPE-Recruiting under ▶ Technical Settings ▶ Workflow ▶ Workflow in E-Recruiting .	You use the SAP Workflow.

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not users who run background processing jobs.

i Note

For more information, see the Customizing for SAPE-Recruiting under [▶ Technical Settings ▶ User Administration ▶ Create Special Users](#).

The user types required for SAPE-Recruiting are:

- **Reference user**
You can create reference users to simplify authorization maintenance. You assign different roles to each reference user. If you then assign a reference user to a user, the user inherits all of the reference user's role attributes and authorization profile.
- **Service user**
Some scenarios are accessible for registered users only; other scenarios are also accessible for unregistered users (registration, job postings, direct application). You must assign a service user to these services so that an unregistered user can use them.
- **Background User for Workflow**
To be able to use the workflow functions, you must create a system user (such as WF-BATCH) in the standard system.
For more information, see the Customizing for SAP E-Recruiting under ► [Technical Settings](#) ► [Workflow](#) ► [Workflow in E-Recruiting](#) ►.
In SAP E-Recruiting, you must assign a candidate to this user. To do this, you can use the report RCF_CREATE_USER, irrespective of whether you run SAP E-Recruiting and the HR system on the same instance or on different instances.
For more information, see [Background User for Workflow](#) under ► [Talent Management](#) ► [SAP E-Recruiting](#) ► [Authorizations](#) ► in the SAP S/4HANA Security Guide for Human Resources.

Standard Users

We do not deliver standard users within SAP E-Recruiting.

13.3.5.1.2.2 Integration into Single Sign-On Environments

The most widely-used supported mechanisms are listed below. For a complete list, see the link provided below.

- **Secure Network Communications (SNC)**
SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.
- **SAP logon tickets**
SAP E-Recruiting supports the use of logon tickets for SSO when using a Web browser as the frontend client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.
- **Client certificates**
As an alternative to user authentication using a user ID and passwords, users using a Web browser as a frontend client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

- Security Assertion Markup Language (SAML) 2.0
SAML 2.0 provides a standards-based mechanism for SSO. The primary reason to use SAML 2.0 is to enable SSO across domains.

SAP E-Recruiting supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Security Guide also apply to SAP E-Recruiting.

For more information about the available authentication mechanisms, see *User Authentication and Single Sign-On* in the SAP NetWeaver Library.

13.3.5.1.3 Authorizations

SAP E-Recruiting uses the authorization concept provided by AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to SAP E-Recruiting.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the SAP Web AS ABAP.

i Note

For more information about how to create roles, see section *Role Administration* under *Identity Management* in the SAP Library for SAP S/4HANA.

The following section shows the standard roles and the relevant authorization objects that SAP E-Recruiting uses. These are:

- Background User for Workflow
- Recruiter, Administrator, and Data Entry Clerk
- Manager
- Candidate

Authorization Object S_ICF

We strongly recommend that you use the authorization object *S_ICF* to safeguard the Web Dynpro applications in SAP E-Recruiting. For the relevant applications, see the ICF service tree (transaction *SICF*) under */default_host/sap/bc/webdynpro/sap*. The names of the applications in SAP E-Recruiting start with ERC for the recruiter and the administrator, and with HRRCF for the candidate.

You can safeguard each application by entering a character string for it in the *SAP Authorization* field under *Service Data* and using this character string in the field *ICF_VALUE* of the authorization object *S_ICF* in the corresponding user roles. For more information, see the documentation for *Authorization Object S_ICF*.

For information about services relevant for SAP E-Recruiting in the ICF service tree, see *Internet Communication Framework Security of SAP E-Recruiting*.

13.3.5.1.3.1 Background User for Workflow

Standard Roles

The table below shows the standard role that SAP E-Recruiting uses for the background user. SAP E-Recruiting requires this background user for the execution of the workflow. The background user is usually the WF-BATCH user.

Standard Role for the Workflow

Role	Description
SAP_RCF_INT_CANDIDATE_SERVER	<i>Internal Candidate (Server)</i> under <i>Roles (User Profiles)</i> This role provides the necessary authorizations for an internal candidate in SAP E-Recruiting that are required on the backend system when using a separated system (front-end and backend on different systems).

You have to create a corresponding candidate for the background user of the workflow. You use the RCF_CREATE_USER report to do this. For more information, see the Customizing for SAP E-Recruiting under [Technical Settings](#) → [Workflow](#) → [Workflow in E-Recruiting](#) .

For the background user to be used in SAP E-Recruiting, the background user requires the authorization to make status changes to the SAP E-Recruiting objects (authorization object P_RCF_STAT) in addition to all of the authorizations usually assigned to an internal candidate.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP E-Recruiting .

For more information, see section [Authorizations](#) for SAP E-Recruiting under [Roles \(User Profiles\)](#) .

Standard Authorization Objects

Authorization Object	Field	Value	Description
P_RCF_APPL	RCF_APPL	SAP E-Recruiting applications	Authorization object that specifies within SAP E-Recruiting which SAP E-Recruiting applications a user can call. The authorization object is used for the (internal and external) candidates' applications.

Authorization Object	Field	Value	Description
R_RCF_VIEW	RCF_VIEW	SAP E-Recruiting data over-views	Authorization object that specifies within SAP E-Recruiting which data overviews a user can access.
P_RCF_POOL	RCF_POOL	The following ways to access the candidate pool directly are available: <ul style="list-style-type: none"> • Status-Independent Access to Candidates (DIRECT_ACC) • Recognition of Multiple Applicants (DUPL_CHECK) • Maintenance of Candidate Data (CAND_MAINT) 	Authorization object that specifies within SAP E-Recruiting which type of direct access a user can have to the candidates in the Talent Pool.
P_RCF_STAT	OTYPE RCF_STAT	SAP E-Recruiting objects and permitted object status	Authorization object that specifies within SAP E-Recruiting the authorization for status changes to SAP E-Recruiting objects (for example, candidate, application, candidacy).
P_RCF_ACT	ACTVT	<ul style="list-style-type: none"> • Activities, processes, and the following accesses to the activities: • Add or Create • Change • Delete 	Authorization object that specifies within SAP E-Recruiting which type of access a user can have to activities. An activity in SAP E-Recruiting is therefore identified through the assigned process and through the activity type.

13.3.5.1.3.2 Recruiter, Administrator, and Data Entry Clerk

Standard Roles

The following table shows the standard roles that are used by SAP E-Recruiting for recruiters, administrators, and data entry clerks .

Standard Roles for Recruiters, Administrators, and Data Entry Clerks

Role	Description
SAP_RCF_REC_ADMIN_ERC_CI_2	Recruiting Administrator (Obsolete) Administrator for SAP E-Recruiting
	<p>i Note</p> <p>This role is obsolete and has been replaced with the role SAP_ERC_REC_ADMIN_CI_4.</p>
SAP_RCF_REC_ADMIN_ERC_CI_4	Recruiting Administrator (NWBC) (Obsolete) You need this role if you want to use the Recruiting Administrator based on SAP Business Client for HTML. The role is a composite role consisting of the single roles SAP_RCF_REC_ADMIN_SR_ERC_CI_4 and SAP_RCF_REC_ADMIN_ERC_CI_2.
	<p>i Note</p> <p>This role is obsolete and has been replaced with the role SAP_ERC_REC_ADMIN_CI_4.</p>
SAP_RCF_REC_ADMIN_SR_ERC_CI_4	Recruiting Administrator (NWBC) (Obsolete) This role contains the recruiting administrator's menu for display based on SAP Business Client for HTML.
	<p>i Note</p> <p>This role is obsolete and has been replaced with the role SAP_ERC_REC_ADMIN_CI_4.</p>
SAP_ERC_REC_ADMIN_CI_4	Recruiting Administrator
SAP_RCF_DATA_TYPIST_ERC_CI_2	Data Entry Clerk (Obsolete) The role contains the authorization for minimum data entry for incoming paper applications.
	<p>i Note</p> <p>This role is obsolete and has been replaced with the role SAP_RCF_DATA_TYPIST_ERC_CI_4.</p>
SAP_RCF_DATA_TYPIST_ERC_CI_4	Data Entry Clerk

Role	Description
SAP_RCF_RECRUITER_ERC_CI_2	<p data-bbox="804 371 1007 394">Recruiter (Obsolete)</p> <p data-bbox="804 423 1206 445">The role has access to the following data:</p> <ul data-bbox="815 472 1390 685" style="list-style-type: none"> <li data-bbox="815 472 1390 528">• Candidate data: The data is displayed for all candidates who stored their data in the Talent Pool. <li data-bbox="815 544 999 566">• All publications <li data-bbox="815 582 1034 604">• All requisition data <li data-bbox="815 620 1038 642">• All application data <li data-bbox="815 658 1190 680">• All data for the selection processes <p data-bbox="804 712 1374 768">The role also contains the authorization for minimum data entry for incoming paper applications.</p> <div data-bbox="804 792 1390 943" style="background-color: #f0f0f0; padding: 5px;"> <p data-bbox="826 801 911 831">i Note</p> <p data-bbox="826 860 1374 916">This role is obsolete and has been replaced with the role SAP_ERC_RECRUITER_CI_4.</p> </div>
SAP_RCF_RECRUITER_ERC_CI_4	<p data-bbox="804 983 1091 1005">Recruiter (NWBC) (Obsolete)</p> <p data-bbox="804 1034 1342 1191">You need this role if you want to use the Recruiter based on SAP Business Client for HTML. The role is a composite role consisting of the single roles SAP_RCF_RECRUITER_SR_ERC_CI_4 and SAP_RCF_RECRUITER_ERC_CI_2.</p> <div data-bbox="804 1216 1390 1368" style="background-color: #f0f0f0; padding: 5px;"> <p data-bbox="826 1225 911 1254">i Note</p> <p data-bbox="826 1283 1374 1339">This role is obsolete and has been replaced with the role SAP_ERC_RECRUITER_CI_4.</p> </div>
SAP_RCF_RECRUITER_SR_ERC_CI_4	<p data-bbox="804 1408 1091 1431">Recruiter (NWBC) (Obsolete)</p> <p data-bbox="804 1460 1382 1516">This role contains the recruiter's menu for display based on SAP Business Client for HTML.</p> <div data-bbox="804 1541 1390 1688" style="background-color: #f0f0f0; padding: 5px;"> <p data-bbox="826 1550 911 1579">i Note</p> <p data-bbox="826 1608 1374 1664">This role is obsolete and has been replaced with the role SAP_ERC_RECRUITER_CI_4.</p> </div>
SAP_ERC_RECRUITER_CI_4	Recruiter

Role	Description
SAP_RCF_RES_RECRUITER_ERC_CI_2	<p>Restricted Recruiter (Obsolete)</p> <p>This role contains the same authorizations as the Recruiter role. However, restricted recruiters cannot change the status of requisitions and publications (see authorization object P_RCF_STAT).</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>i Note</p> <p>This role is available only if you activate the business function HCM_ERC_CI_3.</p> <p>This role is obsolete and has been replaced with the role SAP_ERC_RES_RECRUITER_CI_4.</p> </div>
SAP_ERC_RES_RECRUITER_CI_4	Restricted Recruiter

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP E-Recruiting .

For more information, see the documentation for SAP E-Recruiting under Authorizations.

Standard Authorization Objects

Authorization Object	Field	Value	Description
P_RCF_WDUI	RCF_APPL	SAP E-Recruiting applications	<p>Authorization object that specifies within SAP E-Recruiting which SAP E-Recruiting application a user can call.</p> <p>The authorization object is used for the recruiter's, administrator's, and data entry clerk's applications.</p>
R_RCF_VIEW	RCF_VIEW	Data Overview	Authorization object that specifies within SAP E-Recruiting which data overviews a user can access.

Authorization Object	Field	Value	Description
P_RCF_POOL	RCF_POOL	The following ways to access the candidate pool directly are available: <ul style="list-style-type: none"> • Status-Independent Access to Candidates (DIRECT_ACC) • Recognition of Multiple Applicants (DUPL_CHECK) • Maintenance of Candidate Data (CAND_MAINT) 	Authorization object that specifies within SAP E-Recruiting which type of direct access a user can have to the candidates in the Talent Pool.
P_RCF_STAT	OTYPE RCF_STAT	SAP E-Recruiting objects and permitted object status	Authorization object that specifies within SAP E-Recruiting the authorization for making status changes to SAP E-Recruiting objects (for example, candidate, application, candidacy).
P_RCF_ACT	ACTVT	<ul style="list-style-type: none"> • Add or Create • Change • Delete 	Authorization object that specifies within SAP E-Recruiting which type of access a user can have to activities. An activity in SAP E-Recruiting is therefore identified through the assigned process and through the activity type.
CA_POWL	POWL_APPID, POWL_CAT , POWL_LSEL, POWL_QUERY, POWL_RA_AL, POWL_TABLE	<ul style="list-style-type: none"> • POWL_APPID: ERC-WORKCENTER 	Authorization object that specifies the authorizations for the Personal Object Worklist (POWL) iViews.

13.3.5.1.3.3 Manager

Using the *Manager Involvement in E-Recruiting* business function (Manager Self-Service) affects the two software components SAP Enterprise Extension HR (EA-HR) and SAP E-Recruiting (ERECRUIT). You have to create an RFC connection from the HR system (EA-HR) to the E-Recruiting system (ERECRUIT). You store

an anonymous service user (that was defined in the E-Recruiting system) for this RFC connection. The SAP _RFC_MANAGER_SERVICE role is assigned to the service user.

Standard Roles

The following table shows the standard roles that are used by SAP E-Recruiting for managers .

Standard Roles for Manager Scenario

Role	Description
SAP_RCF_MANAGER	<p><i>Manager</i></p> <p>This role is required so that managers can access SAP E-Recruiting from the Portal (<i>Manager Self Service</i>).</p> <p>The manager wants to fill the vacant jobs in his or her area. To do this, the manager creates requisitions with the status <i>In Process</i> that are then processed further by recruiters.</p> <p>The role has access to the following data:</p> <p>Candidate data: The manager can see only the candidate data that is assigned to requisitions for which the manager is responsible.</p> <p>Requisition data and data for selection processes: The manager can only see data for which he or she is responsible.</p> <p>The role also contains the authorization to respond to questionnaires about candidates that are assigned to the relevant requisitions.</p>
SAP_RFC_MANAGER_SERVICE	<p>Service user</p> <p>This role is required to request a requisition from the HR system. The service user to which this role is assigned must exist in the E-Recruiting system.</p>

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP E-Recruiting .

For more information, see the documentation for SAP E-Recruiting under [Authorizations \(Recruitment\)](#) .

Standard Authorization Objects

Authorization Object	Field	Value	Description
P_RCF_APPL	RCF_APPL	SAP E-Recruiting applications	Authorization object that specifies within SAP E-Recruiting which SAP E-Recruiting applications a user can call.
R_RCF_VIEW	RCF_VIEW	SAP E-Recruiting data overviews	Authorization object that specifies within SAP E-Recruiting which data overviews a user can access.
P_RCF_POOL	RCF_POOL	The following ways to access the candidate pool directly are available: Status-Independent Access to Candidates (DIRECT_ACC) Recognition of Multiple Applicants (DUPL_CHECK) Maintenance of Candidate Data (CAND_MAINT)	Authorization object that specifies within SAP E-Recruiting which type of direct access a user can have to the candidates in the Talent Pool.
P_RCF_STAT	OTYPE RCF_STAT	SAP E-Recruiting objects and permitted object status	Authorization object that specifies within SAP E-Recruiting the authorization for status changes to SAP E-Recruiting objects (for example, candidate, application, candidacy).
P_RCF_ACT	ACTVT	Add or Create Change Delete	Authorization object that specifies within SAP E-Recruiting which type of access a user can have to activities. An activity in SAP E-Recruiting is therefore identified through the assigned process and through the activity type.

13.3.5.1.3.4 Candidate

Standard Roles

The table below shows the standard roles that are used by SAP E-Recruiting for candidates .

Standard Roles for Candidate Scenario

Role	Description
SAP_RCF_UNREG_CANDIDATE_CLIENT	<p>Unregistered Candidate (Client) (Obsolete)</p> <p>This role contains the necessary authorizations for unregistered candidates/service users that are required on the front-end system when using a separated system (front-end and backend on different systems).</p> <p>If you execute unregistered scenarios directly on the backend system, you must also assign this role to the service user in the backend system.</p> <div data-bbox="821 965 1394 1111"><p>i Note</p><p>This role is obsolete and has been replaced with the role SAP_ERC_UNR_CAND_CLIENT_CI_4.</p></div>
SAP_ERC_UNR_CAND_CLIENT_CI_4	Unregistered Candidate (Client)
SAP_RCF_UNREG_CANDIDATE_SERVER	<p>Unregistered Candidate (Server)</p> <p>This role provides the necessary authorizations for an unregistered candidate/service user in SAP E-Recruiting that are required on the backend system when using a separated system (front-end and backend on different systems).</p>
SAP_RCF_UNREGISTERED_CANDIDATE	<p>(Unregistered) Candidate – Service User (Obsolete)</p> <p>This role provides the necessary authorizations for an unregistered candidate/service user in SAP E-Recruiting that are required when using the front-end and backend on one system.</p> <div data-bbox="821 1630 1394 1776"><p>i Note</p><p>This role is obsolete and has been replaced with the role SAP_ERC_UNR_CANDIDATE_CI_4.</p></div>
SAP_ERC_UNR_CANDIDATE_CI_4	Unregistered Candidate

Role	Description
SAP_RCF_EXT_CANDIDATE_CLIENT	<p data-bbox="804 371 1177 394">External Candidate (Client) (Obsolete)</p> <p data-bbox="804 423 1382 551">This role contains the necessary authorizations for external candidates that are required on the front-end system when using a separated system (front-end and backend on different systems).</p> <div data-bbox="804 573 1398 741" style="background-color: #f0f0f0; padding: 5px;"> <p data-bbox="826 584 911 607">i Note</p> <p data-bbox="826 636 1375 696">This role is obsolete and has been replaced with the role SAP_ERC_EXT_CAND_CLIENT_CI_4.</p> </div>
SAP_ERC_EXT_CAND_CLIENT_CI_4	External Candidate (Client)
SAP_RCF_EXT_CANDIDATE_SERVER	<p data-bbox="804 837 1075 860">External Candidate (Server)</p> <p data-bbox="804 889 1382 1016">This role provides the necessary authorizations for an external candidate in SAP E-Recruiting that are required on the backend system when using a separated system (front-end and backend on different systems).</p>
SAP_RCF_EXTERNAL_CANDIDATE	<p data-bbox="804 1055 1098 1077">External Candidate (Obsolete)</p> <p data-bbox="804 1106 1394 1196">This role may only display its own data. The role can only see job postings that you published via publications using the external posting channels.</p> <div data-bbox="804 1218 1398 1368" style="background-color: #f0f0f0; padding: 5px;"> <p data-bbox="826 1229 911 1252">i Note</p> <p data-bbox="826 1281 1375 1346">This role is obsolete and has been replaced with the role SAP_ERC_EXT_CANDIDATE_CI_4.</p> </div>
SAP_ERC_EXT_CANDIDATE_CI_4	External Candidate
SAP_RCF_INT_CANDIDATE_CLIENT	<p data-bbox="804 1469 1171 1491">Internal Candidate (Client) (Obsolete)</p> <p data-bbox="804 1520 1382 1648">This role contains the necessary authorizations for internal candidates that are required on the front-end system when using a separated system (front-end and backend on different systems).</p> <p data-bbox="804 1677 1382 1767">If you allow internal candidates direct access to the backend system, you must also assign this role to the reference user for internal candidates in the backend system.</p> <div data-bbox="804 1789 1398 1939" style="background-color: #f0f0f0; padding: 5px;"> <p data-bbox="826 1800 911 1823">i Note</p> <p data-bbox="826 1852 1375 1917">This role is obsolete and has been replaced with the role SAP_ERC_INT_CAND_CLIENT_CI_4.</p> </div>

Role	Description
SAP_ERC_INT_CAND_CLIENT_CI_4	Internal Candidate (Client)
SAP_RCF_INT_CANDIDATE_SERVER	Internal Candidate (Server) This role provides the necessary authorizations for an internal candidate in SAP E-Recruiting that are required on the backend system when using a separated system (front-end and backend on different systems).
SAP_RCF_INTERNAL_CANDIDATE	Internal Candidate (Obsolete) This role may only display its own data. The role can only see job postings that you published via publications using the internal posting channels. The role does not have access to the following data: <ul style="list-style-type: none"> • Requisition data • Posting data • Application data • Data for the selection process <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>i Note</p> <p>This role is obsolete and has been replaced with the role SAP_ERC_INT_CAND_CLIENT_CI_4.</p> </div>
SAP_ERC_INT_CAND_CLIENT_CI_4	Internal Candidate
SAP_RCF_ESS_SR_ERC_CI_4	E-Recruiting Services for ESS (WDA) (Obsolete) This role contains the authorizations in SAP E-Recruiting for employees that use E-Recruiting services in ESS WDA (Employee Self-Service Web Dynpro ABAP). <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>i Note</p> <p>This role is obsolete and has been replaced with the role SAP_ERC_INT_CAND_CLIENT_CI_4.</p> </div>

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP E-Recruiting .
For more information, see the documentation for SAP E-Recruiting under Authorizations (Recruitment) .

Standard Authorization Objects

Authorization Object	Field	Value	Description
P_RCF_APPL	RCF_APPL	SAP E-Recruiting applications	Authorization object that specifies within SAP E-Recruiting which SAP E-Recruiting applications a user can call. The authorization object is used for the (internal and external) candidates' applications.
R_RCF_VIEW	RCF_VIEW	SAP E-Recruiting data overviews	Authorization object that specifies within SAP E-Recruiting which data overviews a user can access.
P_RCF_STAT	OTYPE RCF_STAT	SAP E-Recruiting objects and permitted object status	Authorization object that specifies within SAP E-Recruiting the authorization for making status changes to SAP E-Recruiting objects (for example, candidate, application, candidacy).
P_RCF_ACT	ACTVT	<ul style="list-style-type: none"> • Add or Create • Change • Delete 	Authorization object that specifies within SAP E-Recruiting which type of access a user can have to activities. An activity in SAP E-Recruiting is therefore identified through the assigned process and through the activity type.

Additional Standard Authorization Objects when Using Candidate Scenario with Front-end and Backend on Separate Systems

Authorization Object	Field	Value	Description
S_RCF	ACTTV RFC_NAME RFC_TYPE		Authorization object for RFC access (For more information, see the documentation for Authorization Object S_RFC .)

Authorization Object	Field	Value	Description
S_RFCALC	ACTTV		Authorization check for RFC users (for example, <i>Trusted System</i>) (For more information, see the documentation for <i>Authorization Object S_RFCACL</i> .)
	RFC_CLIENT		
	RFC_EQUSER		
	RFC_INFO		
	RCF_SYSID		
	RCF_TCODE		
	RCF_USER		
S_ICF	ICF_FIELD	Internet Communication Framework Service	Authorization checks for using services in Internet Communication Framework (SICF), for calling remote function modules using an RFC destination (SM59), and for configuring proxy settings (SICF). (For more information, see the documentation for <i>Authorization Object S_ICF</i> .)

i Note

You can use the authorization object S_ICF to safeguard the use of RFC destinations and access to individual SICF services.

13.3.5.1.4 Session Security Protection

Definition

To prevent access in JavaScript or plug-ins to the SAP logon ticket and security session cookies, we recommend activating secure session management.

We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

To prevent access in JavaScript or plug-ins to the SAP logon ticket and security session cookies (SAP_SESSIONID_<sid>_<client>), activate [Secure Session Management](#). With an existing security session, users can then start applications that require a user logon without logging on again. When a security session is ended, the system also ends all applications that are linked to this security session.

Use the transaction SICF_SESSIONS to specify the following parameter values shown in the table below in your AB ABAP system:

Session Security Protection Profile Parameters

Profile Parameter	Recommended Value	Comment
icf/set_HTTPOnly_flag_on_cookies	0	Client-dependent
login/ticket_only_by_https	1	Not client-dependent

For more information and detailed instructions, see section [Activating HTTP Security Session Management on AS ABAP](#) in the AS ABAP security documentation.

13.3.5.1.5 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for SAP E-Recruiting is based on the topology used by the ABAP Platform. Therefore, the security guidelines and recommendations described in the ABAP Platform Security Guide also apply to SAP E-Recruiting. Details that specifically apply to SAP E-Recruiting are described in the following topics:

- **Communication Channel Security**
This topic describes the communication paths and protocols used by SAP E-Recruiting.
- **Network Security**
This topic describes the recommended network topology for SAP E-Recruiting. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate SAP E-Recruiting.
- **Communication Destinations**
This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the ABAP Platform Security Guide:

- **Network and Communication Security**
- **Security Aspects for Connectivity and Interoperability**

13.3.5.1.5.1 Communication Channel Security

Use

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

Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Front-end client that uses SAP GUI for Windows as the application server	DIAG	All Customizing data	Passwords
Front-end client that uses a Web browser as the application server	HTTP, HTTPS	All application data	Passwords, personal data

i Note
We generally recommend using HTTPS

DIAG and RFC connections can be protected using [Secure Network Communications](#) (SNC). HTTP connections are protected using the [Secure Sockets Layer](#) (SSL) protocol.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the SAP NetWeaver Security Guide under Transport Layer Security.

Printing

SAP E-Recruiting has numerous options for printing contents. For information about security while printing, see the [SNC User's Guide](#).

13.3.5.1.5.2 Network Security

Definition

You can operate SAP E-Recruiting in different ways. You can run the front end and backend for candidates' users on different systems. You can also operate SAP E-Recruiting and the HR system integrated on one system or on different instances.

We recommend that you run the front end and backend of candidates' users on different systems and that you do not integrate SAP E-Recruiting and the HR system on one system.

Firewall Settings

For more information, see [Using Firewall Systems for Access Control](#) in the ABAP Platform Security Guide.

Ports

SAP E-Recruiting runs on SAP NetWeaver and uses the ports from AS ABAP. For more information, see the topics for [AS ABAP Ports](#) in the corresponding ABAP Platform Security Guides.

For other components, for example, SAPinst, SAProuter, or SAP Web Dispatcher, see <https://help.sap.com/viewer/ports>.

13.3.5.1.5.3 Communication Destinations

The following sections provide an overview of the communication destinations that are relevant for the user in the SAP E-Recruiting roles.

13.3.5.1.5.3.1 Communication Destinations (Recruiter, Administrator, and Data Entry Clerk)

The following table provides an overview of the communication destinations that SAP E-Recruiting uses.

You use the following communication destinations depending on which application you use to manage your HR master data:

- If you use the SAP GUI transactions to maintain HR master data (for example, transactions PA*), communication with SAP E-Recruiting runs via RFC connections.
- If you use the [HR Administrative Services](#) application, communication with SAP E-Recruiting runs via SAP PI (Process Integration).

Destination	Delivered	Type	Users, Authorizations	Description
SAP E-Recruiting to SAP Human Resources Management	No	RFC	See Customizing	IMG: ▶ SAP E-Recruiting ▶ Applicant Tracking ▶ Activities ▶ Set Up Data Transfer for New Employees ▶

Destination	Delivered	Type	Users, Authorizations	Description
From SAP Human Resources Management to SAP E-Recruiting	No	RFC	See Customizing	<ul style="list-style-type: none"> ▶ SAP E-Recruiting ▶ Technical Settings ▶ SAP ERP Central Component (ECC) Integration ▶ Software Runs on Different Instances ▶ Set Up Data Transfer from SAP ECC ▶
From SAP E-Recruiting to TREX	No	RFC	See Customizing	<ul style="list-style-type: none"> ▶ SAP E-Recruiting ▶ Technical Settings ▶ User Administration ▶ Create Special Users ▶ ▶ SAP E-Recruiting ▶ Technical Settings ▶ Search Engine ▶ Set Up Search Engine for E-Recruiting ▶
From SAP E-Recruiting to HR Administrative Services	No	XI messages		Transfer external candidate's data when hiring
From HR Administrative Services to SAP E-Recruiting	No	XI messages		Return personnel number of former external candidate to SAP E-Recruiting

i Note

Changes to the HR master data are transferred to SAP E-Recruiting using the master data distribution in the ALE scenario.

13.3.5.1.5.3.2 Communication Destinations for Manager Involvement

The following table provides an overview of the communication destinations that SAP E-Recruiting uses for Manager Involvement.

Communication Destinations for Manager Involvement (Manager Self-Service)

Destination	Delivered	Type	Users, Authorizations	Description
From HR system (Manager Self-Service) to SAP E-Recruiting	No	RFC	See Customizing	SAP Customizing Implementation Guide → Integration with Other SAP Components → Business Packages / Functional Packages → Manager Self Service → Recruitment → Create RFC Connection to E-Recruiting System.

In the HR system, the methods of the CL_IM_HRRCF_REQUI_REQUEST class use the RFC connection to call function modules in the E-Recruiting system.

The IF_HRASR00 GEN_SERVICE_ADVANCED~FLUSH method transfers information from the requisition request form to the corresponding infotypes of SAP E-Recruiting.

The methods call the following function modules in the E-Recruiting system:

- HRRCF_MDL_UIS_ATT_TYPE_GET
- ERC_SE_REQUI_CREATE_RC

The IF_HRASR00 GEN_SERVICE~GET_HELP_VALUES method fills the value helps for input fields in the requisition request form with values from SAP E-Recruiting.

The method calls the following function modules in the E-Recruiting system:

- HRRCF_MDL_UIS_VH_COMMON
- HRRCF_GET_MANAGERS_FOR_SUBST
- HRRCF_MDL_VH_EMPLOYMENT_FRACT
- HRRCF_MDL_VH_SALARY_CURRENCY
- HRRCF_MDL_VH_SALARY_RANGE
- HRRCF_MDL_VH_CONTRACT_TYPE
- HRRCF_MDL_UIS_SUPPORT_GRP_GET

The IF_HRASR00 GEN_SERVICE~DO_OPERATIONS method determines the manager's substitutes in SAP E-Recruiting. In addition, you can use the method to determine a user in SAP E-Recruiting for a personnel number.

The method calls the following function modules in the E-Recruiting system:

- HRRCF_GET_MANAGERS_FOR_SUBST
- HRRCF_MDL_UIS_USER_GET
- HRRCF_MDL_UIS_ASSIGNED_GRP_GET

13.3.5.1.5.3.3 Communication Destinations (Candidates)

The following table provides an overview of the communication destinations that SAP E-Recruiting uses for the candidate scenario with the front-end and backend on separate systems.

Destinations	Delivered	Type	Users, Authorizations	Description
SAP E-Recruiting (front-end) to SAP E-Recruiting (backend)	No	RFC	See Customizing	<ul style="list-style-type: none"> ▶ SAP E-Recruiting ▶ Technical Settings ▶ User Interfaces ▶ Candidate ▶ Frontend Candidate ▶ Enter RFC Destination of Receiving Backend System ▶ <p>You enter the RFC destination as a value of the <code>RECFA_UI2BL</code> parameter.</p>
SAP E-Recruiting (backend) to SAP E-Recruiting (front-end)	No	RFC	See Customizing	<ul style="list-style-type: none"> ▶ SAP E-Recruiting ▶ Technical Settings ▶ User Interfaces ▶ Candidate ▶ Backend Candidate ▶ Specify System Parameters for Web Dynpro ▶ <p>You enter the RFC destination as a value of the <code>RECFA_BL2UI</code> parameter.</p>

Note that the communication destination "SAP E-Recruiting (front-end) to SAP E-Recruiting (backend)" was defined as a "trusted system connection". In this connection, no users can be stored in the credentials. For more information, see consulting note 1017866.

13.3.5.1.6 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For SAP E-Recruiting, the following services are needed for the relevant roles:

- Administrator and Recruiter
 - All services with the prefix `ERC` in the path `/default_host/sap/bc/webdynpro/sap/`

You activate the services in Customizing for SAP E-Recruiting under [Technical Settings](#) → [User Interfaces](#) → [Administrator and Recruiter](#) → [General Settings](#) → [Determine E-Recruiting Services](#).

- Candidates
 - All services with the prefix *hrrcf* in the path /default_host/sap/bc/webdynpro/sap/
 - All services in the path /default_host/sap/bc/erecruiting/
 - All services with the prefix *hrrcf_wd* in the path /default_host/sap/bc/bsp/sap/

You activate the services in Customizing for SAP E-Recruiting under [Technical Settings](#) → [User Interfaces](#) → [Candidate](#) → [Front-End Candidate](#) → [Specify E-Recruiting Services \(Web Dynpro ABAP\)](#).
- Manager (within the framework of Manager Involvement)
 - default_host/sap/bc/erecruiting/dataoverview
 - default_host/sap/bc/webdynpro/sap/hrrcf_a_dataoverview
 - default_host/sap/bc/webdynpro/sap/hrrcf_a_requi_monitor
 - default_host/sap/bc/webdynpro/sap/hrrcf_a_req_assess
 - default_host/sap/bc/webdynpro/sap/hrrcf_a_tp_assess
 - default_host/sap/bc/webdynpro/sap/hrrcf_a_qa_mss
 - default_host/sap/bc/webdynpro/sap/hrrcf_a_substitution_manager
 - default_host/sap/bc/webdynpro/sap/hrrcf_a_substitution_admin

You activate the services in Customizing for SAP E-Recruiting under [Technical Settings](#) → [User Interfaces](#) → [Manager Involvement](#) → [Specify E-Recruiting Services for MSS](#).

If your firewall(s) use(s) URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information, see [Activating and Deactivating ICF Services](#) in the SAP NetWeaver documentation in SAP Library.

For more information about ICF security, see the RFC/ICF Security Guide

13.3.5.17 Data Storage Security

Data Storage

The SAP E-Recruiting data is saved as follows:

- If you use SAP E-Recruiting integrated with other SAP applications, the data is saved in the SAP Web AS or SAP ECC databases.
- If you use SAP E-Recruiting as a standalone application, the data is saved directly in the SAP E-Recruiting databases. You do not need to use any other databases in addition to these standard databases.

SAP E-Recruiting stores the data in the following locations:

Data	Storage Location
Master data	PD infotype tables
Attachments and user-defined texts	Knowledge Provider (KPro)

Data	Storage Location
Search query logs	Cluster table PCL_RCF (SI)
Audit Trails	Cluster table PCL_RCF (SI)
Infotype Log	Cluster table PCI_RCF (IL)

Cookies

The application uses a Web browser. The SAP Web AS must issue cookies as well as accepting them.

13.3.5.1.8 Enterprise Services Security

The following chapters in the ABAP Platform Security Guide and documentation are relevant for all enterprise services delivered with SAP E-Recruiting:

- Security Guide Web Services
- Recommended WS Security Scenarios
- SAP Process Integration Security Guide

13.3.5.1.9 Other Security-Relevant Information

Virus scan when uploading attachments

SAP E-Recruiting allows the user to upload files as attachments at various times in the program. Since attachments can potentially contain viruses, these viruses could enter your system when you upload the attachments. To reduce this risk as much as possible, we recommend you use an external virus scanner and restrict the MIME types of the attachments.

In the [Virus Scan when Uploading Documents](#) Customizing activity, you activate the virus scan profile / PAOC_RCF_BL/HTTP_UPLOAD that you use in SAP E-Recruiting to perform a virus check when uploading attachments. This enables you to include external virus scanners to increase the security of your system.

You can use the Business Add-In (BAI) HRRCF00_DOC_UPLOAD to check files that are uploaded as attachments to the E-Recruiting system. When doing so, you can use the CHECK_ATTACH_FILE_TYPE method to specify which MIME types are permitted for the attachments. You call the BAI using the [BAI: Upload Documents](#) Customizing activity.

Access to attachments via Microsoft Internet Explorer

You use *Microsoft Internet Explorer* and want to display attachments in the browser. To do this, *Microsoft Internet Explorer* checks the content of the attachment to determine the file type and display the attachment correctly (*MIME Type Sniffing*). In the worst case, it is thus possible that damaging files of an undesired file type are displayed in the browser or cause damage in another way. To avoid this potential threat to security, deselect *MIME Type Sniffing* in the security settings of *Microsoft Internet Explorer*.

13.3.5.1.10 Security-Relevant Logging and Tracing

Application Log

SAP E-Recruiting uses the logging and tracing mechanisms from ABAP Platform. SAP E-Recruiting then writes exceptions in the Application Log. These exceptions can occur due to failed authorization checks, for example, and are therefore relevant for security.

For information about logging and tracing mechanisms of Application Server ABAP, see *Auditing and Logging* under *Application Logging*, there is more information about the application log.

You can access the part of the application log specific to SAP E-Recruiting by using the transaction *SLG1* (Analyze Application Log) and entering the parameter *Object = HRRCF*.

Audit Trail

SAP E-Recruiting creates an audit trail with the candidate profile and search queries. For more information, see *Access Audit Trails*.

13.3.5.1.11 Services in Lifecycle Management for Security

The following services are available from SAP Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWatch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.
In this case, analyze and implement the identified Notes, if possible. If you cannot implement the Notes, the report should be able to help you decide on how to handle the individual cases.
- Whether an accumulation of critical basis authorizations has been identified.

In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation okay, you should still check for any significant changes compared to former EWA reports.

- Whether standard users with default passwords have been identified on your system. In this case, change the corresponding passwords to non-default values.

Security Optimization Service (SOS)

The Security Optimization Service can be used for a more thorough security analysis of your system, including:

- Critical authorizations in detail
- Security-relevant configuration parameters
- Critical users
- Missing security patches

This service is available as a self-service within the SAP Solution Manager or as a remote or on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation for a system audit.

Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance with predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers configuration parameters, but it also covers critical security properties like the existence of a non-trivial Gateway configuration or making sure standard users do not have default passwords.

Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in a secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

More Information

For more information about these services, see:

- SAP EarlyWatch Alert: <https://support.sap.com/en/offerings-programs/support-services/earlywatch-alert.html>
- SAP Security Optimization Service / Security Notes Report: <https://support.sap.com/en/offerings-programs/support-services/security-optimization-services-portfolio.html>

- Comprehensive list of SAP Security Notes: <https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html>
- Configuration Validation
- SAP Activate Methodology Roadmaps: <https://support.sap.com/en/offerings-programs/methodologies/implement.html>

13.3.5.2 Performance Management

About This Chapter

This chapter of the Security Guide provides an overview of the security-relevant information for the *Performance Management* (PA-PD-PM) application component.

i Note

We use the name of the *Performance Management* to mean the same as the name *Objective Setting and Appraisals*. Both names correspond to the technical application component ID PA-PD-PM.

Overview of the Main Sections of This Chapter

The following sections contain the security-relevant information that is specific to “Performance Management”:

- *Important SAP Notes*
This section provides information on why security is necessary and how the document is used, as well as references to other Security Guides on which this Security Guide is based.
- *Security Aspects for Data, Data Flow, and Processes*
This section provides an overview of the security aspects of the most frequently used processes in Performance Management.
- *Authorizations*
This section provides an overview of the authorization concept used for Performance Management.
- *Network and Communication Security*
This section provides an overview of the following aspects:
 - *Communication Channel Security*
 - *Network Security*
- *Internet Communication Framework Security*
This section provides an overview of the services for the Internet Communication Framework (ICF) used by Performance Management.
- *Data Storage Security*
This section provides an overview of all critical data used by the scenario, component, and application as well as the security mechanisms used.
- *Other Security-Relevant Information*
This section contains information on uploading and displaying attachments.

- [Security-Relevant Logging and Tracing](#)
This section provides an overview of the trace and log files that contain security-relevant information and that enable you to reproduce activities, for example, if there is a security violation.

13.3.5.2.1 Technical System Landscape

Overview of the technical system landscape for Performance Management:

- Front-end system: Web Dynpro for ABAP in applications in Manager Self-Service and Employee Self-Service
- Back-end system: Customizing for the [Objective Setting and Appraisals](#) application component (for example, Customizing for applications using Web Dynpro technology for ABAP).
- Back-end system: Transactions for administrators and HR specialists
- Download of Documents from the Back-End System in Knowledge Provider (KPro)
- Workflow
Example: Sending notifications to managers or employees
- SAP Interactive Forms by Adobe
For offline processing of the appraisal document (downloading and uploading of appraisal documents). For more information, see the guide for [SAP Interactive Forms by Adobe](#) under [SAP Interactive Forms by Adobe Security Guide](#).
- Printing of Appraisal Documents
 - SAP Smart Forms
 - PDF-based print form

13.3.5.2.2 Security Aspects for Data, Data Flow, and Processes

In Performance Management, data for the appraisal process are processed as follows:

- For Managers in the Manager Self-Service applications.
For more information about the Manager role, see the SAP S/4HANA Security Guide and choose:
[▶ Human Resources ▶ Self-Services ▶ Manager Self-Service ▶](#)
- For Employees in the Employee Self-Service applications.
For more information about the Employee role, see the SAP S/4HANA Security Guide and choose
[▶ Human Resources ▶ Self-Services ▶ Employee Self-Service ▶](#)

❖ Example

Managers as well as employees can work on appraisal documents in the applications (Web Dynpro for ABAP). The system saves the relevant data to the database. The system saves attachments to files (such as appraisals by an additional appraiser) in the Knowledge Provider (KPro).

13.3.5.2.3 Authorizations

Performance Management uses the authorization concept provided by Application Server ABAP (AS ABAP). Therefore, the security recommendations and guidelines for authorizations detailed in the ABAP Platform Security Guide ABAP also apply to Performance Management.

The ABAP Platform authorization concept is based on the assignment of authorization to users based on role. For role maintenance, use the profile generator (transaction: [Role Maintenance](#) (PFCG)) on the AS ABAP.

Note

For more information about creating roles, see [Role Maintenance](#) under [Identity Management](#).

Authorizations for personnel appraisal implemented in Human Resources have a special significance. The [Performance Management](#) application component uses objects from the following components, among others:

- [Manager Self-Service](#)
For more information, see [Authorizations](#) in Manager Self-Service.
- [Employee Self-Service](#)
For more information, see [Authorizations](#) in Employee Self-Service.
- [Organizational Management](#)
- [Personnel Development](#)
- [Training and Event Management](#)
- [SAP Learning Solution](#)
For more information, see [Authorizations](#) in [SAP Learning Solution](#).

The [Performance Management](#) application component is therefore subject to the general authorization checks in the corresponding application component. Furthermore, the object type Person (P) in Performance Management is of central importance since this object type can be used for appraisers and appraisees (particularly for personnel appraisals). This means that standard checks for people in the SAP system are also valid for Performance Management. Furthermore, Performance Management has additional authorization aspects for controlling authorizations in this application that are realized using specific authorization object and authorization controlling in the Customizing settings for the appraisal template.

For more information about the authorization checks, see [General Authorization Check](#) and [Structural Authorization Check](#) (see SAP Library for SAP S/4HANA and choose ► [Human Resources](#) ► [HR Tools](#) ► [Authorizations for Human Resources](#) ►).

13.3.5.2.3.1 SAP Standard Roles

The following SAP standard roles are used in Performance Management:

PFCG roles for the flexible appraisal process

- SAP_HR_HAP_PMG_ADMIN_SR - Administrator
The authorizations for this role include the following:
 - Applications based on Web Dynpro technology for ABAP, such as Configure User Interfaces for Template (HAP_CONFIGURATION)

- Transactions (for example, administrator functions (PHAP_ADMIN_PA), appraisal catalog (PHAP_CATALOG_PA), Change Appraisal (PHAP_CHANGE_PA), Transport Appraisal Template (PHAP_TRANSPORT))
- SAP_HR_HAP_PMG_MANAGER_SR - Manager
For example, this role contains the authorizations for applications based on Web Dynpro technology for ABAP:
 - Appraisal Document (HAP_MAIN_DOCUMENT)
 - Employee Document Overview (HAP_START_PAGE_POWL_UI_MSS)
 - Application based on Web Dynpro technology for ABAP: Creation and Cascading of Team Goals (HAP_A_PMP_GOALS)
- SAP_HR_HAP_PMG_EMPLOYEE_SR - Employee
For example, this role for employees contains the authorization for applications based on Web Dynpro technology for ABAP:
 - Appraisal Document (HAP_MAIN_DOCUMENT)
 - Employee Document Overview (HAP_START_PAGE_POWL_UI_ESS)
- SAP_HR_HAP_PMG_GOALS_SR - Specialist for Corporate Goals
This role for applications based on Web Dynpro technology for ABAP contains authorization for the following: Creation and Cascading of Corporate Goals and Core Values (HAP_A_PMP_GOALS)

PFCG roles for the Predefined Performance Management Process

- SAP_HR_HAP_PMP_ADMIN_SR - Administrator
The authorizations for this role include the following:
 - Applications based on Web Dynpro technology for ABAP (such as the creation wizard for appraisal templates (HAP_A_TM_CONF), Edit Performance Management Process (HAP_A_PMP_TIMELINE))
 - Transactions (for example, administrator functions (PHAP_ADMIN_PA), appraisal catalog (PHAP_CATALOG_PA), Change Appraisal (PHAP_CHANGE_PA), Transport Appraisal Template (PHAP_TRANSPORT))
- SAP_HR_HAP_PMP_MANAGER_SR - Manager
For example, this role for managers contains the authorizations for applications based on Web Dynpro technology for ABAP:
 - Appraisal Document (HAP_A_PMP_MAIN)
 - Employee Document Overview (HAP_A_PMP_OVERVIEW)
 - Application based on Web Dynpro technology for ABAP: Creation and Cascading of Team Goals (HAP_A_PMP_OVERVIEW)
- SAP_HR_HAP_PMP_EMPLOYEE_SR - Employee
For example, this role for employees contains the authorization for applications based on Web Dynpro technology for ABAP:
 - Appraisal Document (HAP_A_PMP_MAIN)
 - Employee Document Overview (HAP_A_PMP_EMPLOYEE)
- SAP_HR_HAP_PMP_GOALS_SR - Specialist for Corporate Goals
This role for applications based on Web Dynpro technology for ABAP contains authorization for the following: Creation and Cascading of Corporate Goals and Core Values (HAP_A_PMP_GOALS)

Additional PFCG Roles

Note

The following roles are also available in the system: In place of these roles, we recommend you use the roles listed above.

- SAP_HR_HAP_ADMINISTRATOR
(Administrator – Appraisals and objective setting agreements)
- SAP_HR_HAP_MANAGER
(Manager Flexible – Appraisals and objective setting agreements)
- SAP_HR_HAP_EMPLOYEE
(Employee Flexible – Appraisals and objective setting agreements)

Caution

You can call standard roles with the *role maintenance* transaction (PFCG). You must copy these standard roles into a customer-specific namespace for custom implementation to get custom specifications for the roles. When you enter a new name, note that it may not contain an SAP-specific name (SAP, "_"). This is to ensure that a clear distinction can be made between customer-specific roles and standard SAP roles.

13.3.5.2.3.2 Overview of Authorization Objects

In Performance Management, the following authorization objects are essential for enabling users to access the application component for the following roles:

- Transaction authorizations (S_TCODE, P_TCODE)
- Access to HR master data (P_ORGIN/CON, P_PERNR)
- Access to objects in the Personnel Planning database (PLOG)
- Access to appraisals (P_HAP_DOC)

You can control the following for users with named roles using various authorization object fields:

- Activity (display, edit, delete)
- Object set (persons, appraisal templates)
- Content (infotypes)

For more information about these authorizations, see SAP Library under [ERP Central Component](#) > [Human Resources](#) > [Personnel Management](#) > [Personnel Administration](#) > [Technical Processes in Personnel Administration](#) > [Authorizations for Human Resources](#).

13.3.5.2.3.2.1 Authorization Objects S_TCODE and P_TCODE

Authorization object that is used to check whether a user is authorized to start the different HR transactions. The transaction code is checked.

Use

Regardless of the application, the authorization object **S_TCODE** is used to check authorizations for starting the transactions defined for an application.

The authorization object **P_TCODE** is used to check the authorization for starting various HR transactions. The additional check using P_TCODE provides added security for personal data and is therefore used for numerous transactions in HCM applications (such as PA40, PHAP_CHANGE_PA). The authorization object P_TCODE is not used in all HR transactions. Generally, it is used in HR applications where HR-specific authorization objects are not checked when a transaction is called. For more information about this authorization object, see P_TCODE (HR transaction code) .

Necessary Setting for Performance Management:

Transaction code field: PHAP_*_PA (depending on role, specify exact transaction). For administrators, you must include transactions starting with OOHAP_*.

For more information about the authorizations, see SAP Library under [ERP Central Component](#)
[Human Resources Management](#) > [Personnel Management](#) > [Personnel Administration](#) > [Technical Processes in Personnel Administration](#) > [Authorizations for Human Resources Management](#) .

13.3.5.2.3.2.2 Authorization object PLOG (Personnel Planning)

An authorization object that is used to check the authorization for specific fields in the Personnel Management components (*Organizational Management, Personnel Development, Training and Event Management, SAP Learning Solution*, and so on).

Use

Necessary Setting for Performance Management:

INFOTYP: 1000, 1001, 1002, 1048, 5020, 5021, 5022, 5023, 5024, 5025, 5026

ISTAT: 4, 3

OTYPE: VA, VB, VC

PLVAR: *

PPFCODE: Change for Customizing/Administrators, Display for End-Users

SUBTYP: 0001, 5020, A605, A606, A607, B605, B606, B607

Note

The object types have the following meaning:

- VA = Appraisal template
- VB = Criteria group
- VC = Criterion

The Customizing settings for the appraisal templates are made in the aforementioned infotypes (transaction PHAP_CATALOG_PA). Therefore, end users must have at least read authorization for these infotypes. If the appraisal templates include further object types as a result of using free enhancements (such as [Add Business Event Type](#)) or fixed enhancements (such as [Add Individual Development Plan Item](#)), additional authorizations are required for these object types, for example:

- Q = Qualifications
- O = Organizational unit
- S = Position
- C = Job
- D = Course type
- F = Location
- A = Work center

Since individual development plans can also include further standard object types and customer-specific object types, you must also include these when setting up authorizations according to the particular implementation.

For more information on the authorizations, see the SAP Library under [ERP Central Component](#) [> Human Resources Management](#) [> Personnel Management](#) [> Personnel Administration](#) [> Technical Processes in Personnel Administration](#) [> Authorizations for Human Resources Management](#).

13.3.5.2.3.2.3 Authorization Object P_HAP_DOC

An authorization object used to check authorizations for accessing appraisal documents.

Use

Among other things, the distribution of authorization for appraisal templates and appraisal documents is controlled using this authorization object. For more information about this authorization object, see P_HAP_DOC (Appraisal Systems: Appraisal). The P_HAP_DOC authorization object contains the following fields, which are tested during an authorization check:

Authorization Field	Description
ACTVT	Activity (display, change, delete)
PLVAR	Plan version (usually active plan version 01)
HAP_CAT_G	Appraisal category group ID (determines the appraisal category groups that a user can access). The appraisal category groups are contained in table T77HAP_C_GRP (process using transaction OOHAP_CAT_GROUP). For personnel appraisals, use category group 00000001 (see also SAP Note number 497773).
HAP_CAT	Appraisal category ID (determines the appraisal categories that a user can access). Appraisal categories are customer-specific and created in transaction PHAP_CATALOG_PA. They are saved in table T77HAP_C. You can display the numbering of the categories using transaction OOHAP_CATEGORY.
HAP_TEMPL	The appraisal template ID. An appraisal template is customer-specific and created in transaction PHAP_CATALOG_PA. It is an object of type VA. In this field, enter the eight-digit object ID from table HRP1000 of object type VA. This dictates the appraisal templates a user can access.
PROFL	Authorization profile. This field is only used if structural authorizations are used. (See Structural Authorizations in Performance Management).

Necessary Settings for PM:

ACTVT: *

PLVAR: *

HAP_CAT_G: 00000001 (for personnel appraisals)

HAP_CAT:* HAP_TEMPL:* (restrict by customer if necessary)

PROFL: *

Note

You should not assign the authorization object P_HAP_DOC on its own since it is only effective when used in combination with other authorization objects. You must assign it together with the authorization objects PLOG and P_ORGIN(CON). The authorization object PLOG enables users to access appraisal templates and

the criteria they contain (see [Authorization Object PLOG \[page 426\]](#)). The authorization object P_ORGIN(CON) enables users to access HR data (see Authorization Object P_ORGIN / P_ORGINCON). The authorization object P_PERNR is also required to enable users to access their own HR master data (for example, for ESS scenarios) (see Authorization Object P_PERNR).

For more information about the authorizations, see SAP Library under [ERP Central Component](#) [Human Resources Management](#) [Personnel Management](#) [Personnel Administration](#) [Technical Processes in Personnel Administration](#) [Authorizations for Human Resources Management](#).

13.3.5.2.3.2.4 Authorization Objects P_ORGIN

An authorization object used to check the authorization for accessing HR master data.

Use

The checks are run when HR infotypes have to be processed or read. In Performance Management, the persons for whom the user is allowed to process appraisal documents must be authorized via authorization object P_ORGIN. The authorization check is run here using the following fields:

Authorization Field	Description
INFT	Infotype
SUBTY	Subtype
AUTHC	Authorization level (such as read, write, matchcode)
PERSA	Personnel area (from infotype 0001)
PERSG	Employee group (from infotype 0001)
PERSK	Employee subgroup (from infotype 0001)
VDSK1	Organizational key (from infotype 0001)

Necessary Settings for Performance Management:

INFTY: Usually, 0000, 0001, 0002 (depending on the organizational area for which the user is responsible)

SUBTY: *

AUTHC: Read and matchcode

PERSA: (depending on the organizational area for which the user is responsible)

PERSG: (depending on the organizational area for which the user is responsible)

PERSK: (depending on the organizational area for which the user is responsible)

VDSK1: (depending on the organizational area for which the user is responsible)

Note

The authorization object P_ORGIN provides the user with the necessary authorizations he or she needs to access personnel data. This authorization object is mandatory, that is, you cannot define the use of this authorization object as being optional by activating the structural authorizations in Performance Management (table T77S0, switch HAP00/AUTHO). Rather, the structural authorizations comprise an additional filter for accessing appraisal documents for the permitted set of persons (see [Structural Authorizations in Performance Management \[page 432\]](#)). To assign authorizations for accessing infotypes in the authorization object P_ORGIN, you do not need to assign specific infotypes in Performance Management. From a technical perspective, it is sufficient in Performance Management if a person is included in the fields PERSA, PERSG, PERSK, VDSK1 in the permitted amount. However, to ensure consistency for the user (for example, in the display of additional personal data in the appraisal document, in the search function for persons with particular infotype values for filling out selection criteria in Performance Management) it is generally beneficial to provide the user with authorizations for the *Actions* (0000), *Organizational Assignment* (0001), and *Personal Data* (0002) infotypes for the persons for whom the user is to process appraisal documents. It should not be necessary that a user is able to process a person's appraisal document but not read this person's organizational assignment. Such a requirement is not logical from the perspective of the process.

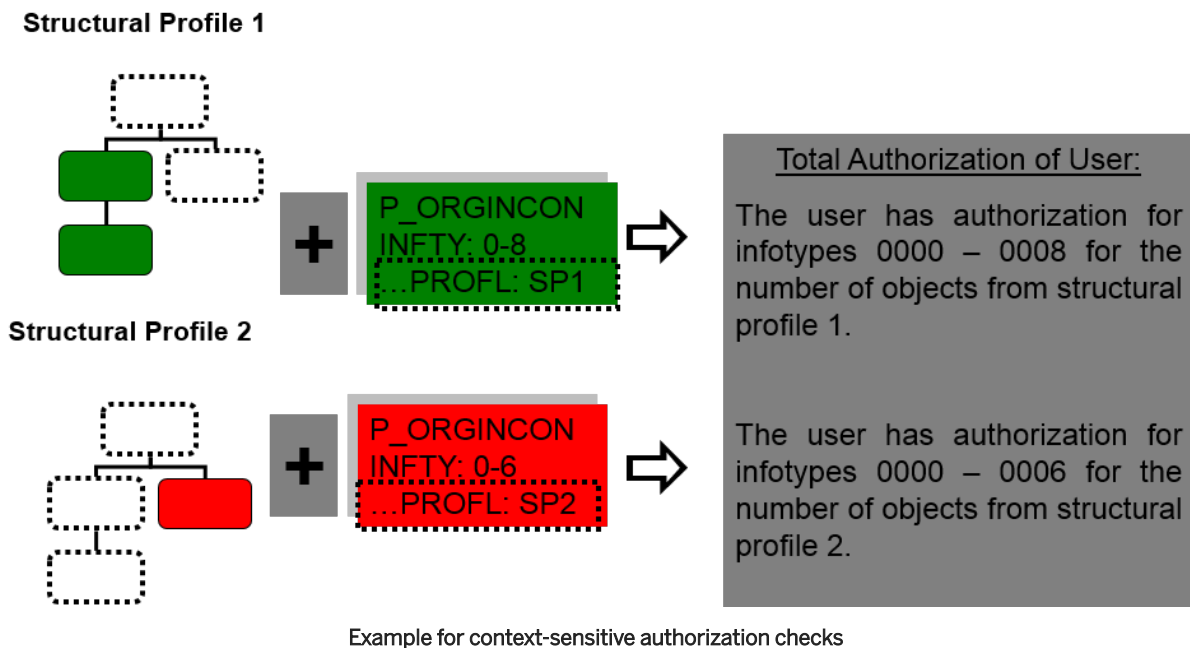
For more information on the authorizations, see the SAP Library under [ERP Central Component > Human Resources Management > Personnel Management > Personnel Administration > Technical Processes in Personnel Administration > Authorizations for Human Resources Management](#).

13.3.5.2.3.2.5 Authorization Object P_ORGINCON

An authorization object that is used during the authorization check for HR data. This check takes place when HR infotypes are edited or read.

Use

You can use this authorization object if structural authorizations are to be checked in context when checking the authorization to access HR master data. This authorization object is used for the authorization check for personnel data. This check takes place when HR infotypes are edited or read. This authorization object consists of the same fields as the authorization object P_ORGIN, and also includes the field PROFL (structural profile). Running the check against this object enables user-specific contexts (using Organizational Management) to be depicted in HR master data.



The checks are made context-sensitive by controlling the various structural sets of persons to different contexts as shown in the example above.

The PROFL field determines the structural profiles the user can access for a particular context. These structural profiles must be assigned to the user in table T77UA.

If you use the Business Add-In (BAI) HRBAS00_GET_PROFL, you do not need to maintain table T77UA manually. This BAI enables you to implement an alternative method for determining structural profiles. The example source code in the standard system determines the user's structural profiles by reading the values entered for the authorization object P_ORGINCON in the user master record.

Structural authorizations in authorization object P_ORGINCON can also be used in combination with structural authorizations in Performance Management (see structural authorizations in Performance Management).

For more information on the authorizations, see the SAP Library under [ERP Central Component](#) [Human Resources Management](#) [Personnel Management](#) [Personnel Administration](#) [Technical Processes in Personnel Administration](#) [Authorizations for Human Resources Management](#).

13.3.5.2.3.2.6 Authorization Object P_PERNR

This authorization object is used to control the user's access to his or her own personnel number and the related HR data separately.

Use

The personnel number is assigned to the user in the *Communication* infotype (0105) (subtype 0001 System User Name). Access to an employee's own master data is used primarily in ESS scenarios in which the user is only to have access to his or her own master data to edit or display this information. To enable access authorizations for the employee's own personnel number to be controlled using the authorization object P_PERNR, the main switch must be activated in table T77S0 (transaction OOAC, switch AUTSW/PERNR). The authorization check is run for the following fields:

Authorization Field	Description
INFTY	Infotype
SUBTY	Subtype
AUTHC	Authorization level (such as read, write, matchcode)
PSIGN	Interpretation of own personnel number (I, include own personnel number, E, exclude own personnel number)

Necessary Settings for Performance Management:

INFTY: Dummy—depends on the ESS scenarios used outside of Performance Management.

SUBTY: Dummy—depends on the ESS scenarios used outside of Performance Management.

AUTHC: *

PSIGN: I (include)

Note

If you use the authorization object P_PERNR, the authorization object P_ORGIN/CON is superfluous. That is, a user who is to be permitted to access his or her own personnel number only (for example, for ESS scenarios), is given all the authorizations required using the authorization object P_PERNR. Therefore, an additional setting for the authorization object P_ORGIN/CON is not required. This also applies to Performance Management.

For more information on the authorizations, see the SAP Library under [ERP Central Component](#) [Human Resources Management](#) [Personnel Management](#) [Personnel Administration](#) [Technical Processes in Personnel Administration](#) [Authorizations for Human Resources Management](#).

13.3.5.2.3.3 Structural Authorizations in Performance Management

Special structural authorizations exist for Performance Management. These authorizations enable you to control access to appraisal documents for persons from defined areas of Organizational Management.

This extended authorization check (structural, context-sensitive authorizations) is activated using the switch HAP00/AUTHO in table T77S0. This switch is specific to Performance Management authorizations.

❖ Example

Example A: Structurally controlled access

The standard SAP authorization check assumes that, once defined, the authorizations (such as change appraisal documents) for a user always apply even when a manager takes on a substituting role for a different organizational unit. If you activate the extended authorization check, you can dictate that a manager can change appraisal documents for employees in his or her organizational unit while he or she can only display appraisal documents for employees in the organizational unit for which he or she is a substitute.

❖ Example

Example B: Structurally controlled access

A user has authorization to read the mini-master record for all employees at a company (P_ORGINCON for infotypes 0000, 0001, 0002 for structural profile A, which is valid for the entire company). This user can maintain simultaneously all infotypes for the employees in his or area of responsibility, displayed via a link between his or her position and the organizational unit for which the user is a substitute (P_ORGINCON for all infotypes for a structural profile B that is valid for the entire area of responsibility). You can use the authorization object P_HAP_DOC to enable the user to display and change the appraisal documents for employees in his or her area of responsibility (structural profile B) and to specify that the user cannot display or change the appraisal documents for employees with structural profile A.

❖ Example

Example C: Structurally and context-sensitively controlled access

A user has the structural profiles outlined in example B.

- Structural profile A for access across whole company
- Structural profile B for area of responsibility

You can also use the authorization object P_HAP_DOC to create a context-sensitive reference to the permitted templates. This means the user can see appraisals from a certain appraisal template, such as qualification checklists, for structural profile A, that is, company-wide. By defining a further setting for the authorization object P_HAP_DOC, you can give the user authorization to access all appraisal templates (such as objective setting agreements, assessments of potential, performance appraisals) that exist in his or her area of responsibility (structural profile B) for the same user.

For more information about structural authorizations, see SAP Library under [ERP Central Component](#) [Human Resources](#) [Personnel Management](#) [Personnel Administration](#) [Technical Processes in Personnel Administration](#) [Authorizations for Human Resources](#).

13.3.5.2.3.3.1 Activating HAP00/AUTHO and Using PA Infotype Authorizations (P_ORGIN) without Structural Authorizations

This combination means that structural restrictions are made during authorization checks **only** for Performance Management and the associated access to personnel appraisals. This is opposed to Personnel Administration, where no structural authorization checks are used.

This means that when HAP00/AUTHO is active, a structural profile must be entered in the authorization object P_HAP_DOC and the user must be entered together with this structural profile in table T77UA.

If, in this authorization object, the value * remains in the *Authorization Profile* field and the user has not been entered in table T77UA, the system interprets this value as structural profile ALL. That is, the user has the authorizations to access the same employee data as defined in the authorization object P_ORGIN. If no value, or an invalid value, is entered in the *Authorization Profile* field for the authorization object P_HAP_DOC, the user cannot access any personnel appraisals (he or she can, however, access the corresponding infotypes in Personnel Administration).

Access using structural authorizations is only possible in Performance Management when a structural profile has been entered in the authorization object P_HAP_DOC and the user is entered in table T77UA has a valid entry for this structural profile.

If this is the case, the structural authorizations function as follows:

- *Filter Function*

❁ Example

In Personnel Administration, a user has authorization for all employees in employee subgroup *AT Employees*. However, the user is to be able to display and process appraisal documents only for those AT employees who are in his or her area of responsibility. To enable this, the structural profile for the user's area of responsibility is entered in the authorization object P_HAP_DOC.

Explanation

The user can only access the personnel appraisals for persons included in his or her structural profile. You can report on the object that can be accessed using the report RHUSERRELATIONS (up to Release 4.7) or using table T77UA (as of the Enterprise Release, using the *Display Objects* function).

This means that structural authorizations for Performance Management work like a filter for people authorized by P_ORGIN: Users can see and process a certain number of people in Personnel Administration via authorization object P_ORGIN. The user can display and maintain only those appraisal documents for persons who are ALSO included in the structural profile of the authorization object P_HAP_DOC (filter/subset).

- *Context Sensitivity*

❁ Example

For persons in area A, a user is to be able to view and/or edit the appraisal template A, *Objective Setting Agreements*, only. For persons in area B, the user is to be able to view and/or edit the appraisal template B, *Qualification Appraisals*, only. This means that the user is not able to show or process the B appraisals, or *Qualification Appraisals*, for employees from area A.

The role requires two instances of the authorization object P_HAP_DOC that differ in the following fields:

	<i>Appraisal Template</i> Field	<i>Authorization Profile</i> Field
1st Proficiency	Template A: Objective Setting Agreements	Structural Profile A: Area A
2nd Proficiency	Template B: Qualification Appraisals	Structural Profile B: Area B

Explanation

A distinction is made between the user's authorizations so that he or she can access different appraisal templates and perform different activities in appraisal templates for the various areas in Organizational Management (context sensitive).

Using report RHUSERRELATIONS (up to Release 4.7) or in table T77UA (as of Enterprise Release, [Display Objects](#) function) you can determine the combination of structural profiles possible for the user (that is, for which persons he or she can access a particular appraisal template and perform specific activities for this appraisal template).

13.3.5.2.3.3.2 Activating HAP00/AUTHO and Using P_ORGINCON (with Structural HR Authorizations)

This setting means that structural authorizations are used to control access to HR master data and personnel appraisals in Performance Management.

To use the authorization object P_ORGINCON, activate the switch AUTSW/INCON in table T77S0.

You must also enter a structural profile in the authorization object P_ORGINCON and P_HAP_DOC.

The user requires a structural profile for all other object types in Organizational Management that do not belong to Performance Management but for which the user nevertheless has authorization using the authorization object PLOG.

In this combination, authorizations between HR master data and appraisals generally work in the same way as described in [Structural Authorizations in Performance Management \[page 432\]](#). In addition, further context-sensitive authorization checks (in combination with structural profiles from Organizational Management) are possible.

If you use both structural, context-sensitive authorization objects P_ORGINCON and P_HAP_DOC, note the following:

- It is not sufficient to give the user a structural profile using authorization object P_HAP_DOC. To enable the user to access employee master data, you must also make a setting for the [authorization object P_ORGINCON \[page 430\]](#) (see also [Authorization Object P_HAP_DOC \[page 427\]](#)).
- You can give the user authorization to access a broader range of HR master data compared with appraisal documents.

❖ Example

In the profile for P_ORGINCON, a user can access the infotypes 0000, 0001, 0002 for all employees at the company who belong to the employee subgroup AT. The structural profile ALL in the authorization object P_ORGINCON (structural profile A) provides the user with this authorization. The user also has a further instance of the authorization object P_ORGINCON that permits him or her to maintain all infotypes for employees in his or her area of responsibility (structural profile B for defining the area of responsibility in Organizational Management).

In the user profile for the authorization object P_HAP_DOC, the user is given authorization to access appraisal documents for employees in his or her area of responsibility (structural profile B) as opposed to for the entire company, 'ALL' profile (structural profile A). This ensures that the user can access the appraisal documents for employees in his or her area of responsibility but not the appraisal documents for employees who belong to the employee subgroup AT, which is valid for the whole company.

- If you use the BAdI HRBAS00_GET_PROFL as opposed to maintaining table T77UA manually (see also [Authorization Object P_ORGINCON \[page 430\]](#)), note that you must also consider the structural profiles from the authorization object P_HAP_DOC.

13.3.5.2.3.4 Controlling Authorizations and Access Using Customizing

The following infotypes are displayed in the form of tab pages and control authorization and access:

- Column Access
- Processing
- Roles

13.3.5.2.3.4.1 Tab: Column Access (Infotype 5023)

On this tab page, you make the settings for access to columns within the (part) appraisal process. You specify display and change authorizations for elements in the appraisal template. You make the following settings:

- You specify the column owner of each separate column group.
You can use an implementation of the BAdI HRHAP00_COL_OWNER to implement customer-specific column access.
- You specify who is authorized to perform which activities in each phase of the appraisal process and which columns are to be shown in the appraisal template.

You can only assign authorizations that are dependent on the various phases to either the **column owner** or all **other** participants involved in the appraisal process. You define who has authorization to execute an activity in a particular phase separately for column owners and all other participants. You can exclude the appraiser from the setting so that he or she has access in every phase (see example below).

You can define the following column access authorizations, for example:

- Free column access for all participants during the entire appraisal process
This setting defines that all participants can display all part appraisals at any time and make changes to the appraisal document.
- Change or display authorization for column owners only.
This setting defines that only column owners can display a column or make changes in a specific appraisal phase.
- On this tab page you can use input help to define that columns are only to be visible to certain participants in the individual phases. To do this, choose the value *Hide*.

The infotype consists of:

- Checkbox: *Default*
Use input help to select default entries for access authorizations. Click on the *Default Access* button to transfer the entries to the *Column Access* group box.
- Indicator: *Changes*
You can accept the transferred defaults without restriction or, if necessary, you can change entries in the individual cells. If you make and save any changes, the *changed* field is marked with an indicator. This makes it easier for you to identify whether these settings are default entries.
- Group box: *Column Access*
In this group box, you make setting for column access.

Example

You depict a part appraisal process with one appraiser (manager), one appraisee (employee), and several part appraisers (colleagues). In the *Part Appraisal* column, the *Part Appraisee* (employee) is the default column owner. In the *Part Appraisal* phase, you assign the column owner change authorization and define that all other participants do not have access during this phase of the part appraisal.

In many cases, you might want the manager to have at least display authorization. You can assign the manager with the necessary authorizations (for example, *Display for Appraiser*, *Hide for Others*) by using input help. This ensures that the column is not displayed for all other part appraisers and that the appraiser has display authorization for the part appraisal column.

Note

- The column access defined for the *Part Appraisal* (PAPP) and *Final Appraisal* (FAPP) columns is possible when one of the following columns is present in the appraisal template:
 - *In Process*
 - *Completed*
 - *Approved*
 - *Rejected*
- The *Objective Setting* (OBJ0) column comprises all objective setting columns (OBJ* and QBH*). The *Part Appraisal* (PAPP) column comprises the *Part Appraisal Weighting* (PWGT) and *Part Appraisal* (PAPP) columns. This is because the SAP system always processes the relevant columns simultaneously.
- If, for a particular phase, a user has *Change* access to the *Objective Setting* (OBJ0) column, he or she can use the *Free Enhancement* function. If this column is not present, the SAP system checks whether

the user has *Change* access to the *Final Appraisal* (FAPP) column for this phase. If this is the case, the user can use a *Free Enhancement* for this phase.

- The column access defined for the *Part Appraisal* (PAPP) and *Final Appraisal* (FAPP) columns is possible when one of the following columns is present in the appraisal template:
 - *In Process*
 - *Completed*
 - *Approved*
 - *Rejected*

You can use an implementation of the BAdI HRHAP00_COL_ACCESS to define customer-specific column access.

13.3.5.2.3.4.2 Tab: Processing (Infotype 5025)

- Setting: *Self Appraisal Not Allowed*
If this setting is activated, a user (that is the user who is logged on) cannot simultaneously perform the role of appraiser and appraisee.
- Setting: *No Authorization Check for Appraiser*
If this setting is activated, an authorization check is not performed for the appraiser. This means that even if a user does not have authorization for the appraiser's person, he or she can nevertheless display and edit all appraisal documents that include this appraiser.

❖ Example

An appraiser has access only to the HR master data of employees in the employee subgroup *Salaried Employees*. That is, he or she can display and edit the appraisal documents for these employees. However, these employees can be appraised by an employee from a different employee subgroup (such as *Managing Employees*). In this case, the administrator does not have access to the appraiser's person. To enable the administrator to nevertheless evaluate and edit appraisal documents for employees in the *Employees* subgroup, you use the setting *No Authorization Check for Appraiser* setting. Consequently, the appraiser's data is not checked for authorization and the administrator can also access the appraisal documents of appraisers in different areas.

- Setting: *Processing Archived Appraisal Documents*
Archived appraisal documents refer to completed appraisal documents. This setting determines whether completed appraisal documents can be deleted in transaction PHAP_CHANGE_PA. If you want this to be possible, select *Delete* or *Reset and Delete*. However, if you do not want this to be possible, select *Do Not Reset or Delete*.
To enable the user to delete completed appraisal documents in transaction PHAP_CHANGE_PA, he or she must have the relevant authorization in authorization object P_HAP_DOC (value *06 -Delete*).
Regardless of this Customizing setting and the user's authorizations defined for this setting *06 -Delete*, the user can always delete completed appraisal documents in transaction PHAP_ADMIN_PA provided that he or she is permitted to use this transaction.

13.3.5.2.3.4.3 Tab: Roles (Infotype 5024)

The Roles tab defines which roles in the appraisal templates are to be used for part appraisals.

You can use roles to define the relationship between the part appraiser and appraisee in the appraisal process. You can edit roles explicitly in the SAP system or have a BAdI (HRHAP00_SELECTION) determine the roles from the enterprise's organizational structure.

You can use roles to restrict or control part appraisal authorizations at the level of individual elements. You make the relevant settings for individual elements in the Customizing settings for the *Roles* tab. If you do not use the role Colleague for a particular element in the appraisal template, this element cannot be appraised by the appraisee's colleague, for example.

This allows you to differentiate between the manager's part appraisal authorizations and the employee's part appraisal authorizations in relation to part appraisal columns in the same appraisal template.

⚠ Caution

The roles to be used in the appraisal process must be selected at category and appraisal-template level.

🔗 Example

Roles delivered in the standard system:

- Colleague
The SAP system uses the organizational structure to identify this role. It interprets all employees located on the same hierarchical level of the organizational structure as colleagues.

⚠ Caution

Organizational Management must be implemented.

- Manager
The SAP system uses the organizational structure to identify this role. It interprets the employee with a managerial function who is located one level higher than the employee in the hierarchical structure as the manager.

⚠ Caution

Organizational Management must be implemented.

- Self
The SAP system identifies this role using the user and, if required user's personnel number (from the *Communication* infotype (0105)). The SAP system can only read the personnel number via the user.

⚠ Caution

The *Communication* infotype (0105) must be available for people.

13.3.5.2.3.4.4 BSP-Specific Authorization Checks

For information about the authorizations for the BSP application, see SAP Note [616900](#).

13.3.5.2.3.4.5 BAdI for Authorization Checks

The BAdI HRHAPO0_AUTHORITY is delivered for extended authorization checks and it can be used as a customer-specific implementation.

13.3.5.2.4 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the back-end system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for Performance Management is based on the topology used by the ABAP Platform. Therefore, the security guidelines and recommendations described in the ABAP Platform Security Guide also apply to Performance Management. Details that specifically apply to Performance Management are described in the following topics:

- **Communication Channel Security**
This topic describes the communication paths and protocols used by Performance Management.
- **Network Security**
This topic describes the recommended network topology for Performance Management. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate Performance Management.

For more information, see the following sections of the ABAP Platform Security Guide:

- Network and Communication Security
- Security Aspects for Connectivity and Interoperability

13.3.5.2.4.1 Communication Channel Security

The table below shows the communication paths used by Performance Management, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Front-end client with SAP GUI for Windows for the application server	DIAG	All application data	Passwords and personal data
Front-end client with a Web browser for the application server	HTTP, HTTPS	All application data	Passwords and personal data
Upload document	HTTP, HTTPS	XML document	Personal data
SAP Business Information Warehouse (SAP BW)	Extractor program	Performance Management data	

You can use Secure Network Communications (SNC) to protect DIAG and RFC connections. The Secure Sockets Layer protocol (SSL protocol) protects HTTP connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the SAP NetWeaver Security Guide under Transport Layer Security.

Printing

Performance Management provides the options for printing content. For information about security while printing, see the *SNC User's Guide*.

13.3.5.2.4.2 Network Security

Ports

Performance Management runs on SAP NetWeaver and uses the ports from the AS ABAP. For more information, see the topic for AS ABAP Ports in the corresponding ABAP Platform Security Guides. For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see <https://help.sap.com/viewer/ports>.

13.3.5.2.5 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For the Manager and Employee roles in Performance Management, all services with the prefix **HAP** in the path / default_host / sap / bc / webdynpro / sap / are required.

- HAP_CONFIGURATION - *Configuration*
- HAP_DOCUMENT_LINK - *Web Dynpro application hap_document_link*

- HAP_MAIN_DOCUMENT - [Appraisal Document](#)
- HAP_QUALIFICATION_PROFILE - [Application for Qualification Profile](#)
- HAP_START_PAGE_POWL_UI_MSS - [Web Dynpro application HAP_START_PAGE_POWL_UI_MSS](#)
- HAP_START_PAGE_POWL_UI_ESS - [Web Dynpro application HAP_START_PAGE_POWL_UI_ESS](#)

Use the transaction [Maintain Services](#) (SICF) to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information, see [Activating and Deactivating ICF Services](#) in the SAP NetWeaver documentation in SAP Library.

For more information about ICF security, see [RFC/ICF Security Guide](#).

13.3.5.2.6 Data Storage Security

HANA

The Performance Management data is saved to the databases of SAP Web Application Server (Web AS) or SAP S/4HANA Component. You do not need to use any other databases in addition to these standard databases.

Performance Management stores the data in the following locations:

Data	Storage Location
Appraisal Templates	PD infotype tables
Cascaded goals	PD infotype tables
Data from appraisal documents	HRHAP* tables
Attachments	Knowledge Provider (KPro)
Download PDF	File system of client

13.3.5.2.7 Other Security-Relevant Information

Access to attachments via Microsoft Internet Explorer

You use [Microsoft Internet Explorer](#) and want to display attachments in the browser. To do this, [Microsoft Internet Explorer](#) checks the content of the attachment to determine the file type and display the attachment correctly ([MIME Type Sniffing](#)). In the worst case, it is thus possible that damaging files of an undesired file type are displayed in the browser or cause damage in another way. To avoid this potential threat to security, deselect [MIME Type Sniffing](#) in the security settings of [Microsoft Internet Explorer](#).

13.3.5.2.8 Security-Relevant Logging and Tracing

Performance Management uses logging and tracing mechanisms from ABAP Platform in the appraisal document. These mechanisms are described in detail under [Auditing and Logging](#).

You can specify the following in the appraisal template:

- Do you want data to be logged?
- The specificity of logging of access to appraisal documents
- The specificity of loggingn of changes to appraisal documents

Changes to appraisal templates are logged using change documents.

13.3.5.3 Talent Management and Talent Development

About This Chapter

This chapter of the Security Guide provides an overview of the security-relevant information for [Talent Management and Talent Development](#) (PA-TM).

Overview of the Main Sections of This Chapter

The following sections contain the security-relevant information that is specific to Talent Management and Talent Development:

- [Important SAP Notes](#)
This section lists the most important SAP Notes with regard to the security of Talent Management.
- [Authorizations](#)
This section provides an overview of the authorization concept used for Talent Management.
- Network and communication security
This section provides an overview of the following aspects:
 - [Communication Channel Security](#)
 - [Communication Destinations](#)
- [Internet Communication Framework Security](#)
This section provides an overview of the services for the Internet Communication Framework (ICF) used by Talent Management.
- [Data Storage Security](#)
This section provides an overview of the critical data used by Talent Management, as well as the security mechanisms used.
- [Security for Third-Party or Additional Applications](#)
This section contains security information that applies to third-party or additional applications that are implemented together with Talent Management.
- [Other Security-Relevant Information](#)
This section contains information on uploading and displaying attachments.

13.3.5.3.1 Authorizations

Use

Talent Management uses the following authorization concepts:

- ABAP Platform authorization concept that is based on assigning authorizations to users based on roles
For this purpose, the roles mentioned under Standard Roles are available as a template. You can copy the standard roles to the customer namespace and adjust them to suit your requirements. You use the profile generator (transaction `PF03`) to maintain roles.
- HR-specific concept for the structural authorization check
For this purpose, the authorization profiles mentioned under Standard Roles are available as a template. You can use the authorization profiles as an example for creating your own authorization profiles and then assign these profiles to the relevant users.
For more information about the authorization profiles, see Customizing for Talent Management and Talent Development and choose [Basic Settings](#) > [Authorizations in Talent Management](#) > [Define Structural Authorizations](#) >
For more information about the structural authorization check, see section [Structural Authorization Check](#) (see SAP Library for SAP S/4HANA and choose [Human Resources](#) > [HR Tools](#) > [Authorizations for Human Resources](#) >).

Role and Authorization Concept for Talent Management

Standard Roles

The table below shows the standard roles and structural authorization profiles that can be used for Talent Management.

Standard Roles and Structural Authorization Profiles

Role	Description	Structural Authorization Profile
SAP_SR_TMC_TMS_6	Authorizations for talent management specialists and talent management superusers (see Talent Management Specialist under Single Roles in Talent Management)	Talent Management Specialist: TMS_PROFILE Talent Management Superuser: TMS_ALL
SAP_SR_TMC_MANAGER_6	Authorizations for managers with regard to Talent Management activities (see Manager in Talent Management under Single Roles in Talent Management)	TMS_MAN_PROF

Role	Description	Structural Authorization Profile
SAP_SR_TMC_EMPLOYEE_6	Authorizations for employees with regard to Talent Management activities (see <i>Employee in Talent Management</i> under <i>Single Roles in Talent Management</i>)	None

For the documentation for the standard roles, see SAP Library for SAP S/4HANA and choose [Human Resources](#) > [Talent Management](#) > [Talent Management and Talent Development](#) > [Roles in Talent Management](#) > [Single Roles in Talent Management](#).

The table below shows the roles that we recommend you no longer use.

Roles No Longer Recommended for Use

Role	Description	Note
SAP_TMC_TALENT_MANA_SPECIALIST	Authorizations for talent management specialists (see <i>Talent Management Specialist</i> under <i>Single Roles in Talent Management</i>)	This role is obsolete and was replaced by the role SAP_SR_TMC_TMS_6.
SAP_TMC_SUPER_TALENT_MANA_SPEC	Authorizations for talent management superusers (see <i>Talent Management Superuser</i> under <i>Obsolete Single Roles in Talent Management</i>)	This role is obsolete and was replaced by the role SAP_SR_TMC_TMS_6.
SAP_TMC_MANAGER	Authorizations for managers with regard to Talent Management activities (see <i>Manager in Talent Management</i> under <i>Single Roles in Talent Management</i>)	We recommend that you use the role SAP_SR_TMC_MANAGER_6 instead of this role.
SAP_TMC_EMPLOYEE	Authorizations for employees with regard to Talent Management activities (see <i>Single Roles in Talent Management</i>)	This role is obsolete and was replaced by the role SAP_SR_TMC_EMPLOYEE_6.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by Talent Management.

Standard Authorization Objects

Authorization Object	Description	More Information
B_BUPA_RLT	Authorizations for business partner roles	Security Guide for Application Server ABAP under SAP Business Partner Security

Authorization Object	Description	More Information
CA_POWL	Authorizations for the personal object worklist (POWL)	SAP Library for SAP S/4HANA under ▶ Cross-Application Functions in SAP ERP ▶ Cross-Application Components ▶ Personal Worklist ▶ in the section Assign Authorizations (Standard POWL)
S_RFC	Authorization check upon RFC access	ABAP Platform Security Guide for Remote Function Call (RFC) and Internet Communication Framework (ICF) under Authorization Object S_RFC
S_WFAR_OBJ	ArchiveLink: Authorizations for accessing documents	For more information, go to https://help.sap.com/s4hana_op_2020 , enter <i>ArchiveLink</i> into the search bar, press <input type="text" value="Enter"/> , and open the search result with that title.
PLOG	Authorization object that checks the authorization for certain fields of Personnel Planning components (Organizational Management, Personnel Development, Training and Event Management, and so on)	SAP Library for SAP S/4HANA under PLOG (Personnel Planning)
P_HAP_DOC	Authorization object that controls a user's access to appraisal templates	SAP Library for SAP S/4HANA under P_HAP_DOC (Appraisal Systems: Appraisal)
P_ORGIN	Authorization object used to check the authorization for accessing HR info-types	SAP Library for SAP S/4HANA under P_ORGIN (HR: Master Data)
P_TCODE	Authorization object used to check whether a user is authorized to start various HR transactions	SAP Library for SAP S/4HANA under P_TCODE (HR: Transaction Code)
P_PERNR	Authorization object used if different authorizations are to be assigned for accessing a user's personnel number	SAP Library for SAP S/4HANA under P_PERNR (HR: Master Data - Personnel Number Check)

For the documentation for the authorization objects PLOG, P_HAP_DOC, P_ORGIN, P_TCODE, and P_PERNR, see SAP Library for SAP S/4HANA and choose [▶ Human Resources ▶ HR Tools ▶ Authorizations for Human Resources ▶ Technical Aspects ▶ Authorization Objects ▶](#).

Critical Combinations

- **Talent Review Meetings**

- All users that have access to the personal object worklist (POWL) for talent review meetings may create talent review meetings.

Note

In the standard SAP system, the POWL for talent review meetings is contained in the roles for talent management specialists for SAP Enterprise Portal and SAP Business Client.

- Users have display and change authorization for all talent review meetings to which they are assigned as members of the support team. The POWL for talent review meetings provides users with a list of talent review meetings, which they can display and edit.

Caution

All members of the support team for a talent review meeting have unrestricted access to all information available within this talent review meeting (for example, to all assigned managers and talents, and their profiles). When this information is accessed, there is no additional authorization check within the talent review meeting.

- Those users that have display or change authorization for the related infotype record of the *Object* infotype (1000) also have display or change authorization for a talent review meeting. The infotype record is identified by the *RM* (*Talent Review Meeting*) object type and the ID of the talent review meeting. Users that have display authorization for this infotype record can call the talent review meeting in display mode. Users with change authorization for this infotype record can call the talent review meeting in change mode.
- **Talent Search**
 - To be able to use the search, a user must be a talent management specialist with an assigned area of responsibility. This means that there must be a relationship 741 (*Is Responsible For/Is in Area of Responsibility Of*) between the user's central person (object type *CP*) and at least one organizational unit (object type *O*).
 - In Customizing, for the search fields that you want to use as search criteria, enter the infotype and the object type, if required, to define which authorization object is used for the authorization check. These settings specify whether this field is available to a user for selection in the search template and in the search results.

Example

The user wants to use the talent group as a search criterion and search for all talents that are assigned to a particular talent group. Therefore, the system checks whether the user has display authorization for relationship 743 (*Has Talent For/Comprises Talent*) between the object types *CP* (*Central Person*) and *TB* (*Talent Group*). To do so, it checks the authorization for the corresponding subtype of the infotype *Relationships* (1001).

For more information, see Customizing for Talent Management and Talent Development and choose [Basic Settings](#) > [Search](#) > [Define Search Requests and Search Field Names](#).

- In the search results, the system displays only the objects for which the user has authorization through the authorization object *PL08* as well as the corresponding structural authorization. For the object type *CP*, the system also checks whether the user has display authorization for the infotype *Organizational Assignment* (0001).

i Note

If more than one person (object type P) is assigned to a central person (CP) (for example, employees in concurrent employment), it is sufficient for the talent search if the user has display authorization for one of these persons.

Additional Functions

You can deactivate specific authorization checks that are performed in the standard SAP system when assigning employees (object type CP (*Central Person*)) to positions, job families, and talent groups. In the standard SAP system, when such relationships are created, the system checks whether the user (in this case, the talent management specialist) has the following authorizations:

- For assigning employees to positions:
Authorizations for
 - Employee (object type CP)
 - Position (object type S)
 - Relationship 740 (*Is Successor Of*)
- For assigning employees to job families:
Authorizations for
 - Employee (object type CP)
 - Job family (object type JF)
 - Relationship 744 (*Has Potential For*)
- For assigning employees to talent groups:
Authorizations for
 - Employee (object type CP)
 - Talent group (object type TB)
 - Relationship 743 (*Has Talent For*)

So that a talent management specialist is also able to create these relationships for employees (object type CP) for which he or she does **not** usually have change authorization (because of his or her structural authorization profile), the authorization check can be deactivated for employees for the respective employee assignment. The talent management specialist then only needs the change authorization for the object (of the object type *Position*, *Job Family*, or *Talent Group*) to which he or she wants to assign the employee, and for the relationship.

For more information, see Customizing for Talent Management and Talent Development and choose

► [Basic Settings](#) ► [Authorizations in Talent Management](#) ► [Deactivate Authorization Check When Assigning Employees](#) ►.

13.3.5.3.2 Communication Channel Security

The table below shows the communication paths used by Talent Management, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Front-end client with SAP GUI for Windows for the application server	DIAG	Customizing data	Passwords
Front-end client with a Web browser for the application server	HTTP(S)	Application data	Passwords, personal data
Front-end client with an SAP Business Client for the application server	HTTP(S)	Application data	Passwords, personal data
Connection of PDF-based print forms to the archive	HTTP(S)	Person-related data (such as an employee's photo)	
SAP Business Information Warehouse (SAP BW)	Extractor program	HR master data, organizational data, Talent Management data	

You can use Secure Network Communications (SNC) to protect DIAG and RFC connections. The Secure Sockets Layer protocol (SSL protocol) protects HTTP connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

i Note

If you convert the protocol from HTTP to HTTPS and implement PDF-based print forms, see SAP Note [1461447](#).

For more information, see the SAP NetWeaver Security Guide under Transport Layer Security.

13.3.5.3.3 Communication Destinations

The table below shows an overview of the communication destinations used by Talent Management.

Communication Destinations

Destination	Delivered	Type	Users, Authorizations	Description
Access to external applications for Talent Management	Yes	RFCs of the function group HRTMC_SERVICES	The following roles require authorization for the authorization object S_RFC to have access to external applications: <ul style="list-style-type: none">• SAP_TMC_TALENT_MANA_SPECIALIST• SAP_TMC_SUPER_TALENT_MANA_SPEC• SAP_TMC_MANAGER	The function group HRTMC_SERVICES contains the Remote Function Calls for external applications that can be used for Succession Planning, for example:
Transfer of talent groups and successor assignments from SAP E-Recruiting to Talent Management	Yes	RFCs of the function group HRSCP_MIGRATION	To run the report RPTMC_MIGRATE_SESSIONS or RPTMC_MIGRATE_TALENT_GROUPS, a user requires authorization for the authorization object S_RFC.	The function group HRSCP_MIGRATION contains the Remote Function Calls for transferring talent groups and successor assignments from SAP E-Recruiting to Talent Management.
Transfer of entries from the candidate profile in SAP E-Recruiting to the talent profile in Talent Management	Yes	RFCs of the function group HRSCP_TP_SYNC	To run the report HRSCP_TP_SYNC_GET_EDU_WE_INFO, a user requires authorization for the authorization object S_RFC.	The function group HRSCP_TP_SYNC contains the Remote Function Calls for synchronizing the talent profile in Talent Management with the candidate profile in SAP E-Recruiting
Jump from queries in SAP Business Information Warehouse (SAP BW) to the talent profile	Yes	RFC for transferring the MEM_ID from the BW system to the S/4HANA system	The user requires authorization for the authorization object S_RFC.	

The table below shows the function modules that the reports use to transfer data to Talent Management:

Function Modules for Transferring Data to Talent Management

Function Group	Function Module	Used by Report
HRSCP_MIGRATION	HRSCP_MIG_SCP_GET_ALL	<i>Transfer Successor Assignments to Talent Management</i> (RPTMC_MIGRATE_SUCCESIONS)
HRSCP_MIGRATION	HRSCP_MIG_TG_GET_ALL	<i>Transfer Talent Groups from E-Recruiting to Talent Management</i> (RPTMC_MIGRATE_TALENT_GROUPS)
HRSCP_MIGRATION	HRSCP_MIG_TG_GET_DETAILS	<i>Transfer Talent Groups from E-Recruiting to Talent Management</i> (RPTMC_MIGRATE_TALENT_GROUPS)
HRSCP_MIGRATION	HRSCP_MIG_TG_GET_TALENTS	<i>Transfer Talent Groups from E-Recruiting to Talent Management</i> (RPTMC_MIGRATE_TALENT_GROUPS)
HRSCP_TP_SYNC	HRSCP_TP_SYNC_GET_EDU_WE_INFO	<i>Synchronization of Talent Profile with Candidate Profile</i> (RPTMC_TP_SYNC_EDU_WE_RCF)

13.3.5.3.4 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For Talent Management the following services are needed:

- Talent Management Specialist
 - default_host/sap/bc/webdynpro/sap/HRTMC_EMPLOYEE_PROFILE
 - default_host/sap/bc/webdynpro/sap/HRTMC_LONG_PROFILE
 - default_host/sap/bc/webdynpro/sap/hrtmc_rm_maintenance
 - default_host/sap/bc/webdynpro/sap/hrtmc_rm_presentation
 - default_host/sap/bc/webdynpro/sap/hrtmc_search
 - default_host/sap/bc/webdynpro/sap/hrtmc_side_by_side
 - default_host/sap/bc/webdynpro/sap/hrtmc_talent_group
 - default_host/sap/bc/webdynpro/sap/HRTMC_TA_DEV_PLAN
- Manager
 - default_host/sap/bc/webdynpro/sap/HRTMC_EMPLOYEE_PROFILE
 - default_host/sap/bc/webdynpro/sap/HRTMC_LONG_PROFILE
 - default_host/sap/bc/webdynpro/sap/hrtmc_side_by_side
 - default_host/sap/bc/webdynpro/sap/hrtmc_talent_group
 - default_host/sap/bc/webdynpro/sap/HRTMC_TA_ASSESSMENT
 - default_host/sap/bc/webdynpro/sap/HRTMC_TA_DASHBOARD

- `default_host/sap/bc/webdynpro/sap/HRTMC_TA_DEV_PLAN`
- `default_host/sap/bc/webdynpro/sap/hrtmc_teamviewer`
- Employee
`default_host/sap/bc/webdynpro/sap/HRTMC_EMPLOYEE_PROFILE`

Use the transaction SICF to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly. For more information, see [Activating and Deactivating ICF Services](#).

For more information about Internet Communication Framework security, see [RFC/ICF Security Guide](#).

13.3.5.3.5 Data Storage Security

Data Storage

The Talent Management data is stored in the SAP Netweaver Application Server or SAP S/4HANA databases. You do not need to use any other databases in addition to these standard databases.

Talent Management stores the data in the following locations:

Data and Storage Locations

Data	Storage Location
Master data, talent assessments	HR infotype tables
Attachments, comments, calibration grid icon	Knowledge Provider (KPro)
Business partner master data	Business partner database
Employee photo	ArchiveLink

Cookies

The application uses a Web browser. SAP Netweaver Application Server must set and accept cookies.

13.3.5.3.6 Security for Additional Applications

You can implement Talent Management together with the product [SAP Talent Visualization by Nakisa](#). [SAP Talent Visualization by Nakisa](#) provides users with a graphical and organization-oriented view of Succession Planning and the job architecture.

i Note

Note that you need to purchase your own license for using the product [SAP Talent Visualization by Nakisa](#).

If you implement *SAP Talent Visualization by Nakisa*, the roles for the talent management specialist, the talent management superuser, and the manager need the authorization for the authorization object S_RFC to be able to access applications that call the HRTMC_SERVICES function group. This function group comprises the Remote Function Calls (RFCs) for external applications such as *SAP Talent Visualization by Nakisa*. This authorization is contained in the standard Talent Management roles. For more information about the standard roles, see section *Authorizations* under *Talent Management and Talent Development*.

For information about the security of *SAP Talent Visualization by Nakisa*, see the documentation for this product.

13.3.5.3.7 Other Security-Relevant Information

Uploading and Displaying Attachments

Uploading Attachments

Talent Management uses the virus scan interface of SAP NetWeaver. You can use this interface to include external virus scanners to increase the security of your system.

For Talent Management, the virus scan profile /HCM_TMC/DOCUMENT_UPLOAD is available for checking that files or documents uploaded as attachments do not contain any viruses. This virus scan profile is **not** active in the standard SAP system. To activate the virus scan profile, in Customizing for Talent Management and Talent Development, make the settings under ► *Basic Settings* ► *Attachments* ► *Define Virus Scan Profiles* ►. In Customizing for SAP NetWeaver under ► *Application Server* ► *System Administration* ► *Virus Scan Interface* ►, you need to first set up the virus scan interface.

For more information about the virus scan interface, see SAP NetWeaver Library and choose ► *SAP NetWeaver by Key Capability* ► *Security* ► *System Security* ►, and the Virus Scan Interface section.

You can also limit the size of files that are uploaded as attachments. To do so, in Customizing for Talent Management and Talent Development, make the settings under ► *Basic Settings* ► *Attachments* ► *Assign Storage Locations and Maximum File Size* ►.

Displaying Attachments Using Microsoft Internet Explorer

If you display attachments in a browser and use Microsoft Internet Explorer for this, Microsoft Internet Explorer checks the content of the attachment to determine the file type and display the attachment correctly based on the type (*MIME Type Sniffing*). In the worst case, it is thus possible that damaging files of an undesired file type are displayed in the browser or cause damage in another way. To avoid this potential threat to security, deselect *MIME Type Sniffing* in the security settings of Microsoft Internet Explorer.

13.3.5.4 Enterprise Compensation Management

About This Chapter

This chapter of the Security Guide provides an overview of the security-relevant information for the *Enterprise Compensation Management* (PA-EC) application component.

Overview of the Main Sections of This Chapter

The following sections contain the security-relevant information that is specific to “Enterprise Compensation Management”:

- *Important SAP Notes*
This section lists the most important SAP Notes with regard to the security of Enterprise Compensation Management.
- *Security Aspects for Data, Data Flow, and Processes*
This section provides an overview of the security aspects of the most frequently used processes in Enterprise Compensation Management.
- *Authorizations*
This section provides an overview of the authorization concept used for Enterprise Compensation Management.
- *Communication Channel Security*
This section describes the communication paths and logs that Enterprise Compensation Management uses.
- *Internet Communication Framework Security*
This section provides an overview of the services for the Internet Communication Framework (ICF) used by Enterprise Compensation Management.
- *Data Storage Security*
This section provides an overview of all critical data used by Enterprise Compensation Management, as well as the security mechanisms used.
- *Security-Relevant Logging and Tracing*
This section provides an overview of the trace and log files that contain security-relevant information and that enable you to reproduce activities, for example, if there is a security violation.

13.3.5.4.1 Security Aspects for Data, Data Flow, and Processes

Enterprise Compensation Management uses applications based on the following technology:

Role: Manager

- Web Dynpro for ABAP in the applications in Manager Self-Service
- Interactive forms based on Adobe software (Interactive forms) in the Total Compensation Statement and *Compensation Review Statement* applications.

For more information, see the guide for *SAP Interactive Forms by Adobe* under *SAP Interactive Forms by Adobe Security Guide*.

For more information about the Manager role, see the SAP S/4HANA Security Guide and choose the following path: ► [Self-Services](#) ► [Manager Self-Service](#) ►.

Role: Employee

- Web Dynpro for ABAP in the applications in Employee Self-Service
- Interactive forms based on Adobe software (Interactive forms) in the *Total Compensation Statement* application.
For more information, see the guide for *SAP Interactive Forms by Adobe* under *SAP Interactive Forms by Adobe Security Guide*.
For more information about the Employee role, see the SAP S/4HANA Security Guide and choose the following path: ► [Self-Services](#) ► [Employee Self-Service](#) ►.

Role: Administrator

- SAP Graphical User Interface (SAP GUI) in Customizing for Enterprise Compensation Management and administrative reports.
- Business Server Page (BSP) in the *Top-Down Budgeting* functions

During compensation planning, Enterprise Compensation Management sends e-mails via workflow. For information about workflow and sending e-mails, see Customizing for *Enterprise Compensation Management* and choose ► [Compensation Administration](#) ► [Workflow Settings](#) ►.

For more information about the settings, see Customizing for *Enterprise Compensation Management*.

13.3.5.4.2 Authorizations

Use

Enterprise Compensation Management uses the following authorization concepts:

- ABAP Platform authorization concept that is based on assigning authorizations to users based on roles
For this, the roles mentioned under “Standard Roles” are available as a template. You can copy the standard roles to the customer namespace and adjust them to suit your requirements. For role maintenance you use the profile generator (transaction `PF00`).
- HR-specific concept for the general and structural authorization check
For more information about the authorization checks, see *General Authorization Check* and *Structural Authorization Check* (see SAP Library for SAP S/4HANA and choose ► [Human Resources](#) ► [HR Tools](#) ► [Authorizations for Human Resources](#) ►).

Roles and Authorization Concept for Enterprise Compensation Management

Standard Roles

Enterprise Compensation Management does not provide its own standard roles. It uses roles from Manager Self-Service and Employee Self-Service.

For more information, see the following:

- [Authorizations](#) in Manager Self-Service.
- [Authorizations](#) in Employee Self-Service.

Standard Authorization Objects

Enterprise Compensation Management uses the same standard authorization objects as all of Human Resources. For more information about the standard authorization objects in Human Resources, see [Authorizations](#). To do this, choose ► [SAP S/4HANA Security Guide for Human Resources](#) ► [Authorizations](#) ►.

13.3.5.4.3 Communication Channel Security

The following table shows the communication paths that Enterprise Compensation Management uses, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
Front-end client that uses SAP GUI for Windows as the application server	DIAG	All Customizing data	Passwords
Front-end client that uses a Web browser as the application server	HTTP, HTTPS	All application data	Passwords, personal data
SAP Business Information Warehouse (SAP BW)	Extractor program	HR master data, organizational data, Enterprise Compensation Management data	

i Note
We generally recommend using HTTPS

You can use Secure Network Communications (SNC) to protect DIAG and RFC connections. The Secure Sockets Layer protocol (SSL protocol) protects HTTP connections.

→ Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) where possible.

For more information, see the SAP NetWeaver Security Guide under Transport Layer Security.

Printing

Enterprise Compensation Management provides a number of options for printing content. For information about security while printing, see the [SNC User's Guide](#).

13.3.5.4.4 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For the Manager role in Enterprise Compensation Management, all services with the prefix **HCM_ECM** in the path `/default_host/sap/bc/webdynpro/sap/` are required.

- HCM_ECM_PLANNING_OVERVIEW_OIF - *Compensation Planning Overview*
- HCM_ECM_PLANNING_UI_GAF - *Planning User Interface*
- HCM_ECM_PROFILE_OIF - *Compensation Profile*
- HCM_ECM_SIDE BYSIDE_OIF - *Side-by-Side Comparison*
- HCM_ECM_TEAMVIEWER_OIF - *Compensation Profile Team Overview*

The Administrator role, the services with the prefix **HRECM_BDG** in the path `/default_host/sap/bc/bsp` are only required if you use top-down budgeting for compensation planning.

- HRECM_BDG_CHKRL - *Check and Release Budget*
- HRECM_BDG_MAINT - *Budget Maintenance*
- HRECM_BDG_RA_VL - *Reassign Budget Value*
- HRECM_BDG_SRV - *Budgeting Services*
- HRECM_BSG_SRV02 - *Budget Structure Services*
- HRECM_BDG_START - *Overview*

Use the transaction *Maintain Services* (SICF) to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information, see *Activating and Deactivating ICF Services* in the SAP NetWeaver documentation in SAP Library.

For more information about ICF security, see RFC/ICF Security Guide.

13.3.5.4.5 Data Storage Security

All data for Enterprise Compensation Management is stored in the database of the SAP system. The data is stored in the *Personnel Administration* (PA) and *Budget Management*(PA-PM) application components as well as in the database tables that govern the processes of Enterprise Compensation Management.

The applications in Enterprise Compensation Management store sensitive, personal data for compensation planning. The data saved when managing the processes of Enterprise Compensation Management can be deleted after the compensation review using the report *Delete Compensation Planning History Data* (RHECM_DELETE_HISTORY_DATA).

For information about data storage security, go to https://help.sap.com/s4hana_op_2020, enter *Security Guides for the Operating System and Database Platforms* into the search bar, press , and open the search result with that title.

13.3.5.4.6 Security-Relevant Logging and Tracing

Enterprise Compensation Management uses logging and tracing mechanisms from ABAP Platform. These mechanisms are described in detail under [Auditing and Logging](#).

Changes to data in Enterprise Compensation Management that are made within the applications of Enterprise Compensation Management are logged by the SAP system. The data can be checked with the following reports:

- [Display Compensation Planning Changes](#) (RHECM_DISPLAY_CHANGES)
- [Display Compensation Planning Progress](#) (RHECM_DISPLAY_PROGRESS)

13.3.6 Time and Attendance Management

13.3.6.1 Personnel Time Management (PT)

Introduction

i Note

This guide does not replace the administration or operation guides that are available for productive operations.

Target Audience

- Technology consultants
- System administrators

This document is not included as part of the installation guides, configuration guides, technical operation manuals, or upgrade guides. Such guides are only relevant for a certain phase of the software lifecycle, whereas the security guides provide information that is relevant for all lifecycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User

errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to the SAP Personnel Time Management. To assist you in securing the SAP Personnel Time Management, we provide this security guide.

About this Document

This security guide provides an overview of the security-relevant information that applies to the SAP Personnel Time Management.

Overview of the Main Sections

The security guide comprises the following main sections:

- **Before You Start**
This section contains information about why security is necessary, how to use this document, and references to other security guides that build the foundation for this security guide.
- **Technical System Landscape**
This section provides an overview of the technical components and communication paths that are used by the SAP Personnel Time Management.
- **Security Aspects of Data, Data Flow, and Processes**
This section provides an overview of security aspects involved throughout the most widely used processes within the SAP Personnel Time Management.
- **Authorizations**
This section provides an overview of the authorization concept that applies to the SAP Personnel Time Management.
- **Session Security Protection**
This section provides information about activating secure session management, which prevents JavaScript or plug-ins from accessing the SAP logon ticket or security session cookie(s).
- **Network and Communication Security**
This section provides an overview of the communication paths used by the SAP Personnel Time Management and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.
- **Internet Communication Framework Security**
This section provides an overview of the Internet Communication Framework (ICF) services that are used by the SAP Personnel Time Management.
- **Security-Relevant Logging and Tracing**
This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

13.3.6.1.1 Important SAP Notes

The SAP Personnel Time Management is built using the HR backend system, CRM backend system and SAP NetWeaver components. Therefore, the corresponding security guides also apply to the SAP Personnel Time Management.

Important SAP Notes

The most important SAP Notes that apply to the security of the SAP Personnel Time Management are shown in the table below.

Title	SAP Note
Authorization objects of shift planning	496993
Transaction authorization PA61 for shift planning	500844
Setting up the HR-PDC interface	647145

For a list of additional security-relevant SAP News and SAP Notes, see <https://support.sap.com/securitynotes>.

Additional Information

For more information about specific topics, see the Quick Links as shown in the table below.

Content	Quick Link
Security	https://www.sap.com/community/topic/security.html
Related SAP Notes	https://support.sap.com/notes https://support.sap.com/securitynotes
Released platforms	https://support.sap.com/pam
SAP Solution Manager	https://support.sap.com/solutionmanager
SAP Community	https://www.sap.com/community/topics.html

13.3.6.1.2 User Management

Use

User management in SAP Personnel Time Management uses the mechanisms provided with the Application Server ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for SAP Personnel Time Management, see the sections below. In addition, we provide a list of the standard users required for operating the SAP Personnel Time Management.

User Administration Tools

The table below shows the tools to use for user management and user administration with SAP Personnel Time Management.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance with AS ABAP (Transactions SU01, PFCG)	For more information, see <i>User and Role Administration of AS ABAP</i> .	

User Types

It is necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively must change their passwords on a regular basis, but not users who run background processing jobs.

The specific user types that are required for the SAP Personnel Time Management include:

Technical users

- To upload time events from the external time recording system you use the RPTCC106 report (*HR-PDC: Download Upload Request for Time Events*). You normally schedule the report as a background processing job. For this you require a technical user. The authorizations of the technical user should be based on the authorizations for the PT80 transaction (*Subsystem Connection*). Time events are uploaded from the subsystem by an IDOC, which stores the time events in the CC1TEV interface table. For the upload, you need a technical user with authorizations for communication with an SAP system using Application Link Enabling (ALE) and the relevant table authorizations. The technical user does not require authorizations specific to the SAP HR solution. You need a technical user with authorizations for the PT45 transaction (*HR-PDC: Post Person Time Events*) for the background processing job that transfers the time events from the interface table to the relevant Time Management tables.
- You need two types of technical users for BAPIs that store data in one of the following interface tables:
 - PTEXDIR
 - PTEX2000
 - PTEX2003
 - PTEX2010

To fill the interface tables, you need a user with authorizations for ALE communication with an SAP system and the relevant table authorizations. For the subsequent background processing job to transfer data from the interface tables to the infotype database tables, you need a technical user with the same authorizations that are required for the CAT6 transaction (*Transfer Time Data to Time Management*).

- For technical users that have read access to the infotypes for the BAPIs, you can use the same authorizations as contained in the SAP_HR_PT_TIMEADMINISTRATOR role.

13.3.6.1.3 Authorizations

Use

The SAP Personnel Time Management component uses the authorization concept provided by AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the AS ABAP Security Guide also apply to SAP Personnel Time Management.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the ABAP.

For more information about how to create roles, see *Role Administration* under *Role and Authorization Concept for SAP Personnel Time Management*.

Standard Roles

The table below shows the standard roles that are used by the SAP Personnel Time Management.

Role	Description
SAP_HR_PT_SHIFT-PLANNER	Shift Planner
SAP_HR_PT_TIME-ADMINISTRATOR	Time Administrator
SAP_HR_PT_TIME-LABOR-ANALYST	Time and Labor Analyst
SAP_HR_PT_TIME-MGMT-SPECIALIST	Time Management Specialist
SAP_HR_PT_TIME-SUPERVISOR	Time Supervisor
SAP_ESSUSER_ERP05	Employee Self-Service
SAP_HR_PT_US_PS_TIME-ADM	Time Recording Administrator This role is used only in the Public Sector in the country version for the USA

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP Personnel Time Management.

Authorization Object	Field	Value	Description
P_PERNR	AUTHC	E, R	Used to assign different authorizations to users for accessing their own personnel number. P_PERNR is relevant for Self-Service Scenarios (Role SAP_EMPLOYEE)

Authorization Object	Field	Value	Description
P_PERNR	INFTY	0000, 0001, 0002, 0007, 0416, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2010, 2011, 2012, 2013	Infotypes required
P_ORGIN	AUTHC	E, R	Used during the authorization check for HR infotypes.
P_ORGIN	INFTY	0000, 0001, 0002, 0007, 0416, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2010, 2011, 2012, 2013	Infotypes required
P_PCLX	AUTHC	W, R	Relevant for both Time Evaluation and Time Recording.
P_PCLX	RELID	B1, B2, L1, G1, PC	Clusters required

13.3.6.1.4 Data Storage Security

Archiving Objects and Reports

The following tools and reports are available for archiving data:

- Archiving Object: `PA_TIME` (Time Evaluation Results from Cluster B2)
- Data Writing Report: `RPAR5W00`
- Data Deletion Report: `RPAR5D00`

Archiving is done using transactions `PU22` and `SARA` respectively.

Data Deletion Reports

The following tools and reports are available for deleting data:

`RPTXTPT`: Using the `DELETE` option deletes the data already transferred (stored in PA-tables) from the following interface tables:

- `PTEX2000`
- `PTEX2010`
- `PTEX2003GEN`
- `PTEX2003SPEC`

`RPWI4100`: Reorganizes interface table `LSHR` (Integration to Logistics).

Using Logical Paths and File Names to Protect Access to the File System

Personnel Time Management saves data in files in the local file system. Therefore, it is important to assign explicit access to the corresponding files in the file system without access to other directories or files (also called directory traversal). This is achieved by entering logical paths and file names in the system that are assigned to the physical paths and file names. This assignment is validated at runtime. If access to a directory is requested that does not correspond to a stored assignment, an error occurs.

The following lists show the logical file names and paths that are used by Personnel Time Management, and the reports for which these file names and paths are valid. The logical file names and logical file paths were created using transaction FILE to facilitate the validation of physical file names.

Logical File Names and Path Names Used in Personnel Time Management

Logical File Name	Reports That Use These Logical File Names	Logical File Path
HR_XX_DIR_RPTED000	RPTED000	HR_XX_DIR_RPTED000
HR_XX_DIR_RPTEUP00	RPTEUP00	HR_XX_DIR_RPTEUP00
HR_XX_DIR_RPTEUP10	RPTEUP10	HR_XX_DIR_RPTEUP10
HR_XX_DIR_RPTEZL00	RPTEZL00	HR_XX_DIR_RPTEZL00
HR_XX_DIR_RPTX2010	RPTX2010	HR_XX_DIR_RPTX2010
HR_XX_DIR_RPWI0000	RPWI0000	HR_XX_DIR_RPWI0000

13.3.6.2 Cross-Application Time Sheet (CA-TS)

13.3.6.2.1 User Administration and Authentication

The Cross-Application Time Sheet (CA-TS) uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the Application Server ABAP also apply to the Cross-Application Time Sheet (CA-TS). In addition to these guidelines, we include information about user administration and authentication that specifically applies to the Cross-Application Time Sheet (CA-TS) in the following topics:

- User Management
This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the Cross-Application Time Sheet (CA-TS).
- Integration into Single Sign-On Environments
This topic describes how the Cross-Application Time Sheet (CA-TS) supports Single Sign-On mechanisms.

13.3.6.2.1.1 User Management

User management for the Cross-Application Time Sheet (CA-TS) uses the mechanisms provided with the Application Server ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for the Cross-Application Time Sheet (CA-TS), see the sections below.

User Administration Tools

The table below shows the tools to use for user management and user administration with the Cross-Application Time Sheet (CA-TS).

User Management Tools

Tool	Detailed Description	Prerequisites
User and Role Maintenance (transaction PFCG)	You can use the Role Maintenance transaction PFCG to generate profiles for the Cross-Application Time Sheet (CA-TS) users. For more information, see User and Role Administration of AS ABAP .	
Technical Settings for User Management in Cross-Application Time Sheet (CA-TS)	For more information on user profiles and the roles, see Customizing for Time Sheet under Settings for All User Interfaces > Authorizations .	

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

The user types that are required for the Cross-Application Time Sheet (CA-TS) include:

- Individual users:
 - Dialog users are used to maintain, release, and approve working times. They are used for SAPGUI and WD ABAP Frontends
- Technical users:
 - System User: Background processing and communication within a system (such as RFC users for ALE, Workflow). They are used for transferring data to target components, to check data remotely, and to process workflow items.
 - Communication users are used for scenarios in which CATS BAPIs are called from external systems.

For more information on these user types, see [User Types](#) under [User Authentication](#) in the SAP NetWeaver Application Server for ABAP Security Guide.

Standard Users

We do not deliver standard users within Cross-Application Time Sheet (CA-TS).

13.3.6.2.1.2 Integration into Single Sign-On Environments

The most widely-used supported mechanisms are listed below. For a complete list, see the link provided below.

- **Secure Network Communications (SNC)**
SNC is available for user authentication and provides for a single sign-on (SSO) environment when using the SAP GUI for Windows or Remote Function Calls.
- **SAP logon tickets**
Cross-Application Time Sheet (CA-TS) supports the use of logon tickets for SSO when using a Web browser as the frontend client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.
- **Client certificates**
As an alternative to user authentication using a user ID and passwords, users using a Web browser as a frontend client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.
- **Security Assertion Markup Language (SAML) 2.0**
SAML 2.0 provides a standards-based mechanism for SSO. The primary reason to use SAML 2.0 is to enable SSO across domains.

The Cross-Application Time Sheet (CA-TS) supports the Single Sign-On (SSO) mechanisms provided by ABAP Platform. Therefore, the security recommendations and guidelines for user administration and authentication as described in the ABAP Platform Security Guide also apply to the Cross-Application Time Sheet (CA-TS).

For more information about the available authentication mechanisms, see [User Authentication and Single Sign-On](#).

13.3.6.2.2 Authorizations

Use

The Cross-Application Time Sheet (CA-TS) uses the authorization concept provided by the AS ABAP and AS Java. Therefore, the recommendations and guidelines for authorizations as described in the Application Server

ABAP Security Guide and SAP NetWeaver AS Security Guide Java also apply to the Cross-Application Time Sheet (CA-TS).

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP and the User Management Engine's user administration console on the AS Java.

i Note

For more information about how to create roles, see section *Role Administration* under the SAP Library for *SAP S/4 HANA Identity Management*.

The following section shows the typical scenarios, the relevant roles and the authorization objects that Cross-Application Time Sheet (CA-TS) uses. These are:

Enter Working Times in Time Sheet

Approve Working Times

Transfer Working Times to Target Components

Role and Authorization Concept for Cross-Application Time Sheet (CA-TS)

Enter Working Times

Standard Roles

The table below shows the standard roles that are used by the Cross-Application Time Sheet (CA-TS).

Role	Description
SAP_HR_PT_TIME-ADMINISTRATOR	Time Administrator: The Time Administrator role is performed by employees in the individual departments of a company, such as secretaries and foremen. Their duties include entering employees' documents in the system and reacting to messages from time evaluation.
SAP_EMPLOYEE_WDA_1 (This includes single role SAP_EMPLOYEE_XX_ESS_WDA_1 containing authorizations for CATS)	Employee Self-Service (WD ABAP): You need this role if you want to enable all your company's employees to record their working times.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by the Cross-Application Time Sheet (CA-TS).

Authorization Object	Field	Value	Description
P_PERNR	AUTHC	E, R	Used to assign users different authorizations for accessing their own personnel number. P_PERNR is relevant for Self Service Scenarios (Role SAP_EMPLOYEE)
P_PERNR	INFTY	0000, 0001, 0002, 0007, 0315, 0316, 2001, 2002, 2003, 2010	Needed infotypes
P_ORGIN	AUTHC	E, R	Used during the authorization check for HR infotypes. P_ORGIN is relevant for Administrator Scenarios (Role AP_HR_PT_TIME-ADMINISTRATOR, SAP_ISR_RETAIL_STORE)
P_ORGIN	INFTY	0000, 0001, 0002, 0007, 0315, 0316, 2001, 2002, 2003, 2010	Needed infotypes
P_PCLX	AUTHC	R	Relevant for both Self Service and Administrator Scenarios, used when attendance/absence types are recorded and to display target hours.
P_PCLX	RELID	B2, PC	Needed clusters

Approve Working Times

Standard Roles

The table below shows the standard roles that are used by the Cross-Application Time Sheet (CA-TS).

Role	Description
SAP_HR_PT_TIME-SUPERVISOR	<p>The <i>Time Supervisor</i> role is performed by executive employees in the individual departments of a company, such as those with personnel responsibility, department heads, project managers, or foremen.</p> <p>The Time Supervisor plans and approves leave and alterations to working times. He or she orders overtime as required, and regularly monitors the amount of overtime worked in the department. He or she checks and approves employees' activity reports, and monitors absence times.</p>

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by the Cross-Application Time Sheet (CA-TS).

Authorization Object	Field	Value	Description
P_ORGIN	AUTHC	D, R	Authorization object that is used during the authorization check for HR infotypes.
P_ORGIN	INFTY	0328, 2001, 2002	Needed infotypes

Transfer Working Times to Target Components

Standard Roles

The table below shows the standard roles that are used by the Cross-Application Time Sheet (CA-TS).

Role	Description
SAP_HR_PT_TIME-MGMT-SPECIALIST	<p>The time management specialist is responsible for the smooth operation of the time management system. He or she is familiar with the technical side of the SAP System. The time management activities for this role include controlling the transfer of data to other SAP applications, such as the transfer of data from the <i>SAP Cross-Application Time Sheet</i>.</p>

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by the Cross-Application Time Sheet (CA-TS).

Authorization Object	Field	Value	Description
P_ORGIN	No proposal	No proposal	
P_PERNR	No proposal	No proposal	
PCLX	No proposal	No proposal	

13.3.6.2.3 Session Security Protection

To prevent access in javascript or plug-ins to the SAP logon ticket and security session cookie(s), we recommend activating secure session management.

We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

To prevent access in javascript or plug-ins to the SAP logon ticket and security session cookie(s) (SAP_SESSIONID_<sid>_<client>), activate secure session management. With an existing security session, users can then start applications that require a user logon without logging on again. When a security session is ended, the system also ends all applications that are linked to this security session.

Use the transaction SICF_SESSIONS to specify the following parameter values shown in the table below in your AS ABAP system:

Session Security Protection Profile Parameters

Profile Parameter	Recommended Value	Comment
icf/set_HTTPOnly_flag_on_cookies	0	Client-Dependent
login/ticket_only_by_https	1	Not Client-Dependent

For more information and detailed instructions, see [Activating HTTP Security Session Management on AS ABAP](#) in the AS ABAP security documentation.

13.3.6.2.4 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level), or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, there is no way for intruders to compromise

the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for the Cross-Application Time Sheet (CA-TS) is based on the topology used by the ABAP Platform. Therefore, the security guidelines and recommendations described in the ABAP Platform Security Guide also apply to the Cross-Application Time Sheet (CA-TS). Details that specifically apply to the Cross-Application Time Sheet (CA-TS) are described in the following topics:

- **Communication Channel Security**
This topic describes the communication paths and protocols used by the Cross-Application Time Sheet (CA-TS).
- **Network Security**
This topic describes the recommended network topology for the Cross-Application Time Sheet (CA-TS). It shows the appropriate network segments for the various client and server components, and where to use firewalls for access protection. It also includes a list of the ports needed to operate the Cross-Application Time Sheet (CA-TS).
- **Communication Destinations**
This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the ABAP Platform Security Guide:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

13.3.6.2.4.1 Communication Channel Security

The table below shows the communication channels used by the Cross-Application Time Sheet (CA-TS), the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client that uses SAP GUI for Windows for the application server	DIAG	All customizing data, application data entered by Non-WD applications	Passwords
Front-end client that uses a Web browser for the application server	RFC, HTTP(S) We recommend you use HTTPS.	Application data entered by WD applications and Web Services	Passwords

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

i Note

We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, see Transport Layer Security in the ABAP Platform Security Guide.

13.3.6.2.4.2 Network Security

You can operate Cross-Application Time Sheet (CA-TS) in different ways. You can run the Cross-Application Time Sheet (CA-TS) and the HR system and or cProject system integrated on one system, or on different instances.

Firewall Settings

For more information, see Using Firewall Systems for Access Control in the SAP NetWeaver Security Guide.

For more information, see Using Multiple Network Zones in the ABAP Platform Security Guide.

Ports

The Cross-Application Time Sheet (CA-TS) runs on SAP NetWeaver and uses the ports from the AS ABAP.

For more information, see the topic for AS ABAP Ports in the corresponding ABAP Platform Security Guides.

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see <https://help.sap.com/viewer/ports>.

13.3.6.2.4.3 Communication Destinations

Use

The table below shows an overview of the communication destinations used by the Cross-Application Time Sheet (CA-TS).

Destination	Delivered	Type	User, Authorizations	Description
Cross-Application Time Sheet (CA-TS) to Human Resources Management	No	RFC	Anonymus dialog user specified in connections between both systems	Customizing: <i>Time Sheet → Settings for All User Interfaces → Data Transfer for Distributed Systems (ALE)</i>

Destination	Delivered	Type	User, Authorizations	Description
Cross-Application Time Sheet (CA-TS) to cProjects	No	RFC	Anonymus dialog user specified in connections between both systems	Customizing: Time Sheet → Settings for All User Interfaces → Data Transfer for Distributed Systems (ALE)
WD Java Frontend to Cross-Application Time Sheet (CA-TS)	Yes	RFC/JCo	See Customizing	Customizing: Integration with Other SAP Components → Business Packages / Functional Packages → Manager Self Service (mySAP ERP) .
External consumer/external Web UI to Cross-Application Time Sheet (CA-TS)	No	HTTP(S) and SOAP messages	Specific dialog user	Cross-Application Time Sheet (CA-TS) acts as service provider.

13.3.6.2.5 Data Storage Security

The Cross-Application Time Sheet (CA-TS) data is saved in databases of the SAP system as follows:

Data	Location
Application Data	CATSDB
Attachments and user-defined texts	SAPScript storage
Templates	CATS_TEMP
Transfer data for HR	PTEX2000, PTEX2010, PTEXDIR
Transfer data for CO	CATSCO
Transfer data for PS	CATSPS
Transfer data for PM	CATSPM
Transfer data for MM-SRV	CATSMM
Transfer data for cPro	DPR_CONF_LI

13.3.6.2.6 Enterprise Services Security

The following chapters in the SAP NetWeaver Security Guide and documentation are relevant for all enterprise services delivered with Cross-Application Time Sheet (CA-TS):

- [Web Services Security](#)
- [Recommended WS Security Scenarios](#)
- [SAP Process Integration Security Guide](#)

13.3.6.2.7 Security-Relevant Logging and Tracing

Cross-Application Time Sheet (CA-TS) relies on the logging and tracing mechanisms from ABAP Platform:

- Auditing and Logging
- Tracing and Logging

13.3.6.2.8 Services for Security Lifecycle Management

The following services are available from Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWatch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.
In this case, analyze and implement the identified notes, if possible. If you cannot implement the notes, the report should be able to help you decide on how to handle the individual cases.
- Whether an accumulation of critical basis authorizations has been identified.
In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation okay, you should still check for any significant changes compared to former EWA reports.
- Whether standard users with default passwords have been identified on your system.
In this case, change the corresponding passwords to non-default values.

Security Optimization Service (SOS)

The Security Optimization Service can be used for a more thorough security analysis of your system, including:

- Critical authorizations in detail
- Security relevant configuration parameters
- Critical users
- Missing security patches

This service is available as a self service within the SAP Solution Manager or as a remote or on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation of a system audit.

Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance to predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers configuration parameters, but it also covers critical security properties like the existence of a non-trivial Gateway configuration or making sure standard users do not have default passwords.

Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

More Information

For more details on these services see

- EarlyWatch Alert: <https://support.sap.com/en/offerings-programs/support-services/earlywatch-alert.html>
- Security Optimization Service / Security Notes Report: <https://support.sap.com/en/offerings-programs/support-services/security-optimization-services-portfolio.html>
- Comprehensive list of Security Notes: <https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html>
- Configuration Validation
- SAP Activate Methodology Roadmaps: <https://support.sap.com/en/offerings-programs/methodologies/implement.html>

13.4 Manufacturing

13.4.1 Production Planning

13.4.1.1 Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

Production Planning and Detailed Scheduling saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The data storage security of SAP NetWeaver and components installed on the base is described in the ABAP Platform Security Guide. All business data in SAP PP/DS is stored in the system database. If SAP LiveCache is used, some business data is also stored there. This business data is protected by the authorization concept of SAP NetWeaver and SAP PP/DS. In some special cases, business-relevant data is stored in another location, such as a file system. The special case is listed below:

Logical File Names Used

The following logical file name has been created in order to enable the validation of physical file names:

- SAP SCM Optimizer

Logical Path Names Used

The logical file names listed above all use the following logical file paths:

- <drive>:\usr\SAP\<SID>\<Gxx>\log (for Windows)
- \usr\sap\<SID>\<Gxx>\log (for Linux)

<SID>: Gateway ID on the SAP SCM Optimizer server

<Gxx>: Gateway number

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see about data storage security, see the respective chapter in the ABAP Platform Security Guide.

13.4.2 Manufacturing Execution for Discrete Industries

13.4.2.1 Authorizations for Just-in-Time-Processing

Just-in-Time Processing (JIT) uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
C_AUTO_JIT	ISAUTO_JIT: Sequenced JIT Calls (seqJC)
C_JIT_CALL	PP-FLW JIT Calls
C_JIT_OUT	IS-A-JIT: JIT Outbound Calls
JIT_S2P	JIT Supply to Production: Authorizations for JIT Calls

Authorization Object	Description
JIT_S2P_CC	JIT Supply to Production: Authorization for Control Cycles

13.4.2.2 Authorizations for Production Backflush

Production Backflush uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
C_BCKFLUSH	Automotive: Production backflush
C_APO_PPC	APO Authorization Object: Production Backflush

13.4.2.3 Deletion of Personal Data

Related Information

[Deletion of Personal Data \(Just-in-Time-Processing\) \[page 479\]](#)

[Deletion of Personal Data \(Production Backflush\) \[page 481\]](#)

[Deletion of Personal Data \(Production Order\) \[page 481\]](#)

13.4.2.3.1 Deletion of Personal Data (Just-in-Time-Processing)

Use

Just-in-Time-Processing (IS-A-JIT) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Just-in-Time Supply to Customer

Application	Provided Deletion Functionality
Just-in-Time-Processing (IS-A-JIT)	Archiving Object
	JIT_SJCAL
	JITO_CALL
	ILM Object
	JIT_SJCALL
	JITO_CALL
	Report
	DELETE_JIT_VENDOR_CUSTOMER

Just-in-Time Supply to Production

Application	Provided Deletion Functionality
Just-in-Time-Processing (IS-A-JIT)	Archiving Object
	• NJIT_OCALL
	• NJIT_OCGRP
	ILM Object
	• NJIT_OCALL
	• NJIT_OCGRP

Just-in-Time Supply to Customer

Application	Provided Deletion Functionality
Just-in-Time-Processing - Supply to Customer (LE-JIT)	Archiving Object NJIT_ICALL ILM Object NJIT_ICALL Reports NJIT_I_DEL (Delete) NJIT_I_READ_AR_SEQUENTIAL (Read) NJIT_I_WRI (Write)

Just-in-Time Supply to Production

Application	Provided Deletion Functionality
Just-in-Time-Processing - Supply to Production (LE-JIT)	<ul style="list-style-type: none"> • Archiving Object <ul style="list-style-type: none"> • NJIT_OCALL • NJIT_OCGRP • ILM Object <ul style="list-style-type: none"> • NJIT_OCALL • NJIT_OCGRP • Reports <ul style="list-style-type: none"> • NJIT_O_DEL (Delete) • NJIT_O_DEL_COMMUNICATION_GRP(Delete) • NJIT_O_READ_AR_SEQUENTIAL (Read) • NJIT_O_READ_COMMUNICATION_GRP(Read) • NJIT_O_WRI (Write) • NJIT_O_COMMUNICATION_GRP(Write)

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Just-in-Time-Processing (IS-A-JIT)	WUC	Checks tables JITCU

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for [Cross-Application Components→Data Protection](#).

13.4.2.3.2 Deletion of Personal Data (Production Backflush)

Use

Production Backflush might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Production Backflush (IS-A-PPC)	Archiving Object PP_CONF

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components*→*Data Protection*.

13.4.2.3.3 Deletion of Personal Data (Production Order)

Use

Production orders might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Production Order (ERP_PP_SFC)	<p>When a production order is created with reference to a sales order, the customer details are copied over from the sales order.</p> <p>In addition, the supplier data is taken from the purchasing data of the material.</p> <p>For externally processed operations, the supplier data can also be maintained in the operation.</p>	<p>Archiving Object</p> <p>PP_ORDER</p> <p>ILM Object</p> <p>PP_ORDER</p>

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Production Order (ERP_PP_SFC)	End of Purpose (EoP) check	

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of customer master/supplier master in Customizing for [► Cross-Application Components ► Data Protection ► Blocking and Unblocking of Data ►](#).

13.4.2.4 Data Archiving in Just-In-Time Supply to Customer

Use

You archive data to remove from the database data that the system no longer needs, but which must still be accessible.

You use a specific archiving object to archive specific data.

Features

It may be possible to display archived data. For more information, see the descriptions of the individual archiving objects.

Activities

You can carry out archiving using the **Manage Archiving Variants** app.

13.4.2.4.1 Archiving Just-In-Time Call Data Using NJIT_ICALL

You can use archiving object NJIT Call Inbound (NJIT_ICALL) to archive NJIT calls.

The following programs are available for NJIT_ICALL:

- Write program: NJIT_I_WRI
- Delete program: NJIT_I_DEL
- Read program: NJIT_I_READ_AR_SEQUENTIAL

You can find the following information:

- Tables - NJIT_CALL_D_HDR, NJIT_CALL_D_CGRP, NJIT_CALL_D_CMAT, NJIT_CALL_D_DREF, and NJIT_CALL_D_RTXT
- Archiving Object - NJIT_ICALL

Checks

The following checks are carried out on JIT calls before they can be archived:

- The Write program can select only archivable NJIT calls, that is to say, for those which lifecycle status is completed.

Prerequisites

JIT calls must be in a completed state to archive related data.

13.4.2.4.2 Archiving Just-In-Time Inbound Packaging Units Data Using NJIT_IPKGU

You can use archiving object NJIT Inbound Packaging Units (NJIT_IPKGU) to archive NJIT inbound packaging units.

The following programs are available for NJIT_IPKGU:

- Write program: NJIT_PKGU_I_WRI
- Delete program: NJIT_PKGU_I_DEL
- Read program: NJIT_PKGU_I_READ_AR_SE

You can find the following information:

- Tables - NJIT_D_PG_HDR, NJIT_D_PG_CNSMPN, NJIT_D_PG_ITM, and NJIT_D_PG_ITMREF
- Archiving Object - NJIT_IPKGU

Checks

The following checks are carried out before NJIT inbound packaging units can be archived:

- The Write program can select only archivable NJIT inbound packaging units, that is to say, those for which the package group status is set to *Delivered*.

Prerequisites

Package groups must be in a *Delivered* state to archive related NJIT inbound packaging unit data.

13.4.2.4.3 ILM-Based Information for the Archiving Object

You must create policies and rules for the related ILM object NJIT Call Inbound (`NJIT_ICALL`) using the Retention Management functions of SAP Information Lifecycle Management (SAP ILM).

To define retention rules using ILM policies (Using ILM Policies app), you can use the following condition fields and time references (start time for determining the retention period and residence period).

Available Condition Fields:

- Plant (`WERKS_D`)

Available Time References:

- Last Changed On (`LAST_CHANGE_DATE`)

13.4.2.4.4 Business Partner End Of Purpose (EoP) Check in Just-In-Time Supply to Customer

Just-In-Time Supply to Customer provides an end of purpose (EoP) check to determine whether business partner data is still relevant for business activities in the application or can be blocked.

Technical Details

The EoP check evaluates retention policies and data for ILM object `NJIT_ICALL`.

The end of business for a JIT-relevant customer is reached when no JIT calls for that customer are active or in use. In other words, all their JIT calls must be set to a completed state. Execute transaction `CVP_PRE_EOP` to check if these conditions are met.

The EoP check for Just-In-Time Supply to Customer supports the use of application rule variants based on ILM rule groups. If you want to define differing residence and retention periods for business partner data depending on area-specific condition fields, you can use the following configuration apps to define and assign rule variants:

Assign Rule Variants and *Groups for the Customer EoP Check*: Both apps are used to assign the rule groups used in the ILM retention policies of an area-specific ILM object to the rule variants, which are used in combination with the area name to maintain the required residence and retention policies for the BP-related ILM objects (`FI_ACCRECV`).

You can set up the rule groups for an ILM object in configuration app *Manage ILM Object Groups*.

13.4.2.4.5 Information Retrieval Framework in Just-In-Time Supply to Customer

The information retrieval feature supports you to comply with the relevant legal requirements for data protection by allowing you to search for and retrieve all personal data of a specified data subject.

While creating Purpose, you need to provide the ILM object name (NJIT_ICALL).

13.4.2.5 Data Archiving in Just-in-Time Supply to Production

Use

You archive data to remove from the database data that the system no longer needs, but which must still be accessible. For more information, see [Introduction](#).

You use a specific archiving object to archive specific data.

For information about archiving objects in general, see [The Archiving Object](#).

Features

It is possible to display archived data.

Activities

You can archive using the **Manage Archiving Variants** application. For more information, see [Manage Archiving Variants](#).

See Also

- [Archiving Procedure](#)

Related Information

[Archiving Just-In-Time Call Data Using NJIT_OCALL \[page 486\]](#)

[Archiving Just-In-Time Communication Group Data Using NJIT_OCGRP \[page 487\]](#)

[ILM Based Information for Archiving Object \[page 488\]](#)

[Business Partner End of Purpose \(EoP\) Check in Just-In-Time Supply to Production \[page 488\]](#)

[Information Retrieval Framework in Just-In-Time Supply to Production \[page 489\]](#)

13.4.2.5.1 Archiving Just-In-Time Call Data Using NJIT_OCALL

You can use archiving object NJIT Outbound Call (**NJIT_OCALL**) to archive NJIT calls.

The following are the available programs:

- **Write:** NJIT_O_WRI
- **Delete:** NJIT_O_DEL
- **Read:** NJIT_O_READ_AR_SEQUENTIAL

You can find the following information:

- **Tables**
 - NJIT_CALL_D_HDR
 - NJIT_CALL_D_CGRP
 - NJIT_CALL_D_CMAT
 - NJIT_CALL_D_DREF
 - NJIT_CALL_D_RTXT
- **Archiving Object**
 - NJIT_OCALL

Checks

The required check on JIT calls before archiving them is:

- The **write** program can select only archivable NJIT calls, that is, for those which lifecycle status is completed

Prerequisite

- JIT calls must be completed to archive related data.

Related Information

[Data Archiving in Just-in-Time Supply to Production \[page 485\]](#)

13.4.2.5.2 Archiving Just-In-Time Communication Group Data Using NJIT_OCGRP

You can use archiving object NJIT communication group, **NJIT_OCGRP** to archive NJIT communication group data.

The available programs for **NJIT_OCGRP** are, as below:

- **Write:** NJIT_O_WRI_COMMUNICATION_GRP
- **Delete:** NJIT_O_DEL_COMMUNICATION_GRP
- **Read:** NJIT_O_READ_COMMUNICATION_GRP

You can find the following information:

- **Tables**
 - NJIT_COMM_GRP
 - NJIT_MSG_PTNR
- **Archiving Object**
 - NJIT_OCGRP

Checks

The required check must be performed before NJIT communication group is archived:

- The **write** program can select only archivable NJIT communications groups, that is, for those for which the supplier and communication group status is set to **Blocked**.

Prerequisites

- Communication group must be in **Blocked** status to archive related NJIT communication group data.

Related Information

[Data Archiving in Just-in-Time Supply to Production \[page 485\]](#)

13.4.2.5.3 ILM Based Information for Archiving Object

You must create policies and rules for the related ILM object NJIT Call Outbound (**NJIT_OCALL**) using the retention management functions of SAP Information Lifecycle Management (SAP ILM).

To define retention rules using ILM policies (Using ILM Policies application), you can use the following condition fields and time references (start time for determining the retention period and residence period).

Available Condition Fields

- Plant (**WERKS_D**)

Available Time Preferences

- Last Changed On (**LAST_CHANGE_DATE**)

Related Information

[Data Archiving in Just-in-Time Supply to Production \[page 485\]](#)

13.4.2.5.4 Business Partner End of Purpose (EoP) Check in Just-In-Time Supply to Production

Just-In-Time Supply to Production provides an end of purpose (EoP) check to determine whether business partner data is still relevant for business activities in the application or can be blocked.

Technical Details

The end of purpose (EoP) check evaluates retention policies and data for ILM object, **NJIT_OCALL**. The end of business for a JIT-relevant supplier or business partner is reached when no JIT calls for that supplier or business partner are active or in use. In other words, all their JIT calls must be set to completed. Execute transaction **CVP_PRE_EOP** to check if the conditions are met.

The EoP check for Just-In-Time supply to production supports the use of application rule variants based on ILM rule groups. If you want to define differing residence and retention periods for business partner data depending on area-specific condition fields, you can use the following configuration apps to define and assign rule variants:

Assign Rule Variants and Groups for Supplier/Business PartnerCustomer EoP Check

Both applications are used to assign the rule groups used in the ILM retention policies of an area-specific ILM object to the rule variants, which are used in combination with the area name to maintain the required residence and retention policies for the BP-related ILM objects (**FI_ACCRECV**).

You can set up the rule groups for an ILM object in configuration application, *Manage ILM Object Groups*. For more information, see [Manage ILM Object Groups](#).

Related Information

[Data Archiving in Just-in-Time Supply to Production \[page 485\]](#)

13.4.2.5.5 Information Retrieval Framework in Just-In-Time Supply to Production

The information retrieval feature supports you to comply with the relevant legal requirements for data protection by allowing you to search for and retrieve all personal data of a specified data subject.

While creating purpose, you need to provide the ILM object name ([NJIT_OCALL](#)).

For information on relevant BAdI, refer [Information Retrieval Framework \(IRF\)](#).

Related Information

[Data Archiving in Just-in-Time Supply to Production \[page 485\]](#)

13.4.2.6 Data Aging for Just-In-Time Inbound/Outbound (DAAG_NJIT_I)

Data aging enables you to move large volumes of data within a database so as to gain more working memory. The data is moved from the current area (hot area) to the historical area (cold area).

You can use data aging for your inbound and outbound Just-In-Time calls (Data aging object DAAG_NJIT_I).

Data aging can only be applied to completed JIT calls.

The standard residence time is 100 days. Once the JIT calls have been moved to the historical area, you can no longer access them.

13.4.2.7 Input Sanitization for Just-In-Time Processing Applications

Input sanitization attempts to prevent malicious data by validating input content. The free text input fields in applications of Just-In-Time Supply to Customer and Just-In-Time Supply to Production support alphanumeric characters and selected special characters only.

13.4.3 Manufacturing Execution for Process Industries

13.4.3.1 Deletion of Personal Data (Process Orders)

Use

Process orders might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Process Order (ERP_PP_SFC)	When a process order is created with reference to a sales order, the customer details are copied over from the sales order.	Archiving Object PR_ORDER
	In addition, the supplier data is taken from the purchasing data of the material.	ILM Object PR_ORDER
	For externally processed operations, the supplier data can also be maintained in the operation.	

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Process Order (ERP_PP_PI)	End of Purpose (EoP) check	

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of customer master/supplier master in Customizing for ► [Cross-Application Components](#) ► [Data Protection](#) ► [Blocking and Unblocking of Data](#) ►.

13.4.4 Project Manufacturing Management and Optimization

13.4.4.1 Deletion of Personal Data

Use

Project Manufacturing Management and Optimization processes user ID information (personal data) that is subject to the data protection laws applicable in specific countries/regions. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Project Manufacturing Management and Optimization	<p>The BAdI implementation PMMO_USER_DELETED_STE deletes the entries pertaining to the deleted user in the following tables:</p> <ul style="list-style-type: none">• PMMO_RTM_HEADER• PMMO_RTM_ITEM• TPMMO_TOGGLE• TPMMO_CUSTSUBCL <p>It updates the following tables:</p> <ul style="list-style-type: none">• PMMO_REPORT_DFLT• PMMO_MIGRATION	<p>To delete the user ID, the component PMMO has implemented BADI_IDENTITY_BOR_DELETED via the BAdI implementation PMMO_USER_DELETED_STE in the class CL_PMMO_USER_DELETED.</p>

Application	Detailed Description	Provided Deletion Functionality
	The method <code>DELETE_APP_DATA_FOR_USER</code> of the class <code>CL_PMMO_PEGGING_USER_DELETED</code> deletes entries in the table <code>SPERS_OBJ</code> . (In the PMMO application log, choose the pushbutton Change Tree Hierarchy. This data is stored in the <code>SPERS_OBJ</code> .)	To delete the user ID, the component PMMO has implemented <code>BADI_IDENTITY_BOR_DELETED</code> via the BAdI implementation <code>PMMO_USER_DELETED</code> in the class <code>CL_PMMO_PEGGING_USER_DELETED</code> .

13.4.5 Quality Management

13.4.5.1 Communication Channel Security

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

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Communication with Supplier Network Collaboration	SOAP	Quality notification data	
Communication with the Quality Inspection Engine (QIE) of the Extended Warehouse Management (EWM)	SOAP, RFC	Inspection lot data	
Communication exchange of quality certificates with external partner	IDoc	Quality certificates	

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Quality master data replication	IDoc	Master inspection characteristics Master inspection methods Codes Inspection plan Inspection setup data in material master	
Communication with external subsystem for inspection	RFC, SOAP	Inspection lot data Inspection results	
Communication with external subsystem for inspection planning	SOAP	Inspection plan, Master inspection characteristic	
Communication with external subsystem for quality notifications	SOAP	Quality notification data	
Communication with external subsystem for statistical process control (SPC)	RFC	Inspection lot data Inspection results	
Communication with SAP Manufacturing Execution (ME)	RFC, IDoc	Inspection lot data Inspection results	

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

i Note

We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, see Transport Layer Security and Web Services Security in the ABAP Platform Security Guide.

13.4.5.2 Deletion of Personal Data

The Quality Management application might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note 1825544.

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. The Quality Management application uses SAP ILM to support the deletion of personal data as described in the following sections.

SAP delivers an end of purpose check for the Quality Management application.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases.

- Phase one: The relevant data is actively used.
- Phase two: The relevant data is actively available in the system.
- Phase three: The relevant data needs to be retained for other reasons.
For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- Display: The system does not display blocked data.
- Change: It is not possible to change a business object that contains blocked data.
- Create: It is not possible to create a business object that contains blocked data.
- Copy/Follow-Up: It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- Search: It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see the Process Flow.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
Inspection Lot	<p>The EOP check considers partners (customers or suppliers):</p> <ul style="list-style-type: none"> that are stored directly in the inspection lot (table QALS) that are available in the worklist of the transfer table for subsystems (QIWL) that are assigned to a multiple specification (QAOBJMS) <p>Each inspection lot is checked if the customer or supplier is still relevant. If a customer or supplier is used in several objects, he is relevant as long as only one object is not completed. An object is completed if</p> <ul style="list-style-type: none"> an inspection lot is canceled an inspection lot has status <i>All inspections completed</i>, an usage decision was made and stock postings are completed if the inspection lot is stock-relevant. <p>The following data is relevant for calculating the retention rules and residence rules (taking the latest date):</p> <ul style="list-style-type: none"> Last change date <p>You can start report QM_CVP_EOP_SORT_ARC_CONTROL to select all data that has already been archived (background job due to performance).</p>	Archiving object QM_CONTROL

Application Object	Detailed Description	Provided Deletion Functionality
Sample Records	<p>Partners are assigned to the drawing of material samples.</p> <p>Material samples are only considered if there are not part of an order, an inspection lot or a notification since these material samples are considered as separate business operations and are checked during the EoP check for the corresponding object (e.g. notification). Only 'independent' material samples are checked.</p> <p>The assigned partners are no longer relevant, if the material sample is marked for deletion or marked as no longer existent. Then the latest change date is taken as basis for the calculation of the retention and residence rules.</p> <p>You can start report QM_CVP_EOP_SORT_ARC_SAMPLE to select all data that has already been archived (background job due to performance).</p>	Archiving object QM_SAMPLE
Quality Notification	<p>Suppliers and customers are relevant.</p> <p>The end of business is reached when the quality notification has status <i>Completed</i>.</p> <p>You can start report RQARCQMS to select all data that has already been archived.</p>	Archiving object QM_QMEL

Application Object	Detailed Description	Provided Deletion Functionality
Quality Certificate	<p>Only suppliers are relevant. Suppliers are entered directly in the certificate.</p> <p>A certificate is completed if it has one of the following statuses:</p> <ul style="list-style-type: none"> • <i>Certificate filed and inspected</i> • <i>Certificate receipt canceled</i> <p>If you want to send or receive the quality data of a certificate using EDI, and the inspection characteristics to be sent have different descriptions in the supplier and the customer system you can set up a partner-specific identification and assignment of the respective characteristics (characteristic mapping). The communication partners are defined by Partner Type and Partner Number.</p> <p>For the deletion of the partner-specific settings and characteristic mappings you have to run deletion report RDEL_PARTNER_CHAR.</p>	Archiving object QM_CERT
Failure Mode and Effects Analysis	<p>Only business partners on header level are checked. Business partners entered for actions are not checked.</p> <p>It is checked that the FMEA has status <i>Completed</i>, <i>To Be Archived</i>, or <i>Archived</i>.</p> <p>You can start report PLM_FMEA_EOP_AUD_ARC_EXTRACT to select all data that has already been archived.</p>	Archiving object QM_FMEA
Audit Plans/Audits	<p>It is checked that the Audit has status <i>Completed</i>, <i>To Be Archived</i>, or <i>Archived</i>.</p> <p>Only audits are taken into account in the check, but not audit plans or question lists.</p> <p>You can start report PLM_AUDIT_EOP_AUD_ARC_EXTRACT to select all data that has already been archived.</p>	Archiving object PLM_AUD

Application Object	Detailed Description	Provided Deletion Functionality
Quality Info Records in Procurement	The system checks the residence times that were entered under Quality Management > Environment > Central Functions > Organize Archiving .	Archiving object QM_QINF
Quality Info Records in Sales	The system checks the residence times that were entered under Quality Management > Environment > Central Functions > Organize Archiving .	Archiving object QM_QVDM

Relevant Application Areas and Available EoP Functionality

Application	Implemented Solution	Further Information
Quality Management	EoP check	This includes the business in areas of: <ul style="list-style-type: none"> Quality Planning (QM-PT) Quality Inspection (QM-IM) Quality Notification (QM-QN) Audit Management (CA-AUD)

Process

- Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
- You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
- You do the following:
 - Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA).
 - Run transaction BUPA_PRE_EOP to enable the end of purpose check function for the central business partner
 - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and supplier master (ILM objects: FI_ACCPAYB, FI_ACCRECV; for ILM objects in QM see archiving objects above)
 - Run transaction CVP_PRE_EOP to enable the end of purpose check function for the customer master and supplier master.
- Business users can request unblocking of blocked data by using the transaction BUP_REQ_UNBLK.
- If you have the needed authorizations, you can unblock data by running the transaction BUPA_PRE_EOP and CVP_UNBLOCK_MD.
- You delete data by using the transaction ILM_DESTRUCTION for the ILM objects of Quality Management.

13.4.6 Maintenance Operations

13.4.6.1 Authorizations in Plant Maintenance

Standard Roles

SAP delivers business role templates which follow the naming convention SAP_BR_*. The delivered business role templates are designed to cover typical activities of business users with a certain job profile.

Example

The delivered business role template SAP_BR_MAINTENANCE_TECHNICIAN is designed for maintenance technicians. The role contains business catalogs which cover all the functions that a maintenance technician requires to carry out their work effectively and safely.

Another example business role template SAP_BR_MAINTENANCE_PLANNER is designed for maintenance planners. The role contains business catalogs which cover a broad range of functions necessary for planning and executing maintenance activities.

Each business catalog contains one or more applications and is designed to support segregation of duty.

i Note

For more information about how to create roles, see [Role Administration \[page 13\]](#).

13.5 R&D / Engineering

13.5.1 Product Compliance

13.5.1.1 Service Role and User for SAP Business Workflow

The SAP_WFRT user with the *SAP Business Workflow Service User* (SAP_BC_BMT_WFM_SERV_USER) role is delivered with the SAP S/4HANA system. This user is required and responsible for executing the SAP Business

Workflow functions. In the context of Product Compliance, this user calls the program that executes the Product Compliance Event Processing in the background.

The ABAP platform authorization concept is based on assigning authorizations to users based on roles. To maintain roles for ABAP technology, you use the profile generator (transaction `PF03`).

Note

For more information about how to create roles, see [Role Administration \[page 13\]](#).

The following table displays the security-relevant authorization objects that the technical user `SAP_WRF1` needs to execute Product Compliance Event Processing in the background:

Authorization Object	Field	“From” Authorization Value	Description
S_PROGNAM	P_ACTION	BTCSUBMIT	Schedule programs for background processing
		SUBMIT	Execute ABAP program
	P_PROGNAM	R_EHFND_PCEP_EVT_QUEUE_WORKER	A program that processes all production compliance events and tasks
S_PROGRAM	P_ACTION	BTCSUBMIT	Schedule programs for background processing
		SUBMIT	Execute ABAP program
	P_GROUP	WF_ADMIN	Workflow Administration

13.5.1.2 Data Destruction in Product Compliance

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

Product Compliance uses *SAP ILM* to support the deletion of data as described in the following sections.

Relevant Application Objects and Available Deletion Functionality

The following table shows the application objects and the appropriate deletion functionality that is provided in Product Compliance.

Application Objects	Provided Deletion Functionality
Supplier Raw Materials	Data destruction object <code>EHFND_CSM</code>

Deletion Report and Job Dependencies

You can set a supplier raw material to *Outdated* in the app. The retention date is calculated by ILM and a destruction report (`R_EHFND_CSM_DES`) then deletes the datasets.

You can create and set up a job to carry out the deletion report R_EHFND_CSM_DES on a daily basis.

This report persistently deletes all outdated supplier raw materials and their assignments to their corresponding raw materials. A material is outdated when its retention date (RETENTION_DATE) has passed.

13.5.2 Product Safety and Stewardship

13.5.2.1 Product Compliance for Discrete Industries

13.5.2.1.1 User Administration and Authentication

Product Compliance for Discrete Industries uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the ABAP Platform Security Guide also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG).

For more generic information see [User Administration and Authentication \[page 10\]](#) in the *Introduction* section

13.5.2.1.1.1 User Management

The table below shows the standard users that are necessary for operating *Product Compliance for Discrete Industries*. For more generic information, see [User Management \[page 10\]](#) in the *Introduction* section.

User ID	Type	Password	Description
Business processing user	Dialog user	To be entered	Business user of <i>Product Compliance</i>
E-mail inbound processing user	Communication user	Not needed	User to process the incoming e-mails of <i>Product Compliance</i>
Workflow engine batch user	Background user	Not needed	User for the background processing of workflows in <i>Product Compliance</i>

You need to create users after the installation. Users are not automatically created during installation. In consequence, there is no requirement to change user IDs and passwords after the installation.

i Note

Several business processes within *Product Compliance for Discrete Industries* use SAP Business Workflow and e-mail inbound and outbound processing. It is not recommended that you grant the corresponding

system users (such as WF_BATCH for Workflow System or SAPCONNECT for e-mail inbound processing) all authorizations of the system (SAP_ALL).

13.5.2.1.2 Network and Communication Security

Your network infrastructure is important for protecting your system. Therefore, your network must support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit known bugs and security holes in network services on the server machines.

The network topology for *Product Safety and Stewardship* is based on the topology used by the ABAP Platform. Therefore, the security guidelines and recommendations described in the ABAP Platform Security Guide also apply here. Details that specifically apply to *Product Safety and Stewardship* are described in the following sections:

- [Communication Channel Security \[page 509\]](#)
This topic describes the communication paths and protocols.
- [Network Security \[page 510\]](#)
This topic describes the recommended network topology. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports required.
- [Communication Destinations \[page 510\]](#)
This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the *ABAP Platform Security Guide*:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

13.5.2.1.2.1 Communication Destinations

The table below shows an overview of the communication destinations used by *Product Compliance for Discrete Industries*. For more generic information, see in corresponding chapter in the *Introduction* section.

Destination	Delivered	Type	Description
<PM system>	No	RFC	Connection to plant maintenance system
<BuPa system>	No	RFC	Connection to business partner system

Destination	Delivered	Type	Description
<AC system>	No	RFC	Connection to accounting system
<EHS system>	No	RFC	Connection to <i>SAP Product Safety and Stewardship</i> as part of <i>SAP ERP</i> system

Note

The user in the remote AC system needs to have all authorizations as proposed by the respective EHS user roles.

For *SAP EHS Management* as part of *SAP ERP*, Product Compliance for Discrete Industries does not provide any authorizations.

For detailed information about communication destinations, see Customizing for *Environment, Health, and Safety* under ► *Foundation for EHS* ► *Integration* ► *Specify Destinations for Integration* ►.

13.5.2.1.3 ICF Security in Product Safety and Stewardship

To use an app in Product Safety and Stewardship, you have to activate the internet communication framework (ICF) service that is needed for this app.

For general information, see [ICF Security \[page 21\]](#) in the *Introduction* section.

Product Compliance for Discrete Industries

To use *Product Compliance for Discrete Industries* apps, proceed as follows:

- In your back-end system, open transaction SICF. Under `/default_host/sap/bc/webdynpro/sap/`, activate the following Web Dynpro services:
 - that start with EHFND
 - that start with EHPRC
 - POWL
 - IBO_WDA_INBOX
 - WDR_CHIP_PAGE

13.5.2.1.4 Data Storage Security

Using Logical Path and File Names to Protect Access

In *Product Compliance for Discrete Industries*, several applications save data in files in the file system. The International Material Data System (IMDS) uses the file system to store downloaded files temporarily, before

they are imported. Additionally, it is possible for users to upload files to the application server manually prior to further processing. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime, and, if access is requested to a directory that does not match a stored mapping, an error occurs.

The following lists show the logical file names and paths used by *Product Compliance for Discrete Industries* and for which programs these file names and paths apply:

Logical File Names Used

The following logical file names have been created in order to enable the validation of physical file names:

- EHPRC_IMPORT_DIR
- EHPRC_ERROR_DIR
- EHPRC_ARCHIVE_DIR

For more information, see the Customizing activity *Set Up Directory Structure for IMDS*.

Logical Path Names Used

The logical file names listed above all use the logical file path EHPRC_HOME_PATH.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information about data storage security, see the respective chapter in the ABAP Platform Security Guide.

13.5.2.1.5 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that *Product Safety and Stewardship for Discrete Industries* provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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 given system landscape and the applicable legal requirements.

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.

13.5.2.1.5.1 Deletion of Personal Data

Product Safety and Stewardship for Discrete Industries might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use *SAP Information Lifecycle Management (SAP ILM)* to control the blocking and deletion of personal data in *Product Safety and Stewardship for Discrete Industries*.

More Information

- For general information about the blocking and deletion of data for customers, vendors and business partners, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.
- For more information about the deletion of customer and vendor master data, see the Security Guide for SAP ERP on the SAP Help Portal at <http://help.sap.com/erp> under ► *SAP ERP Central Component Security Guide* ► *Data Protection* ► *Deletion of Personal Data* ►.
- For more information about simplified blocking and deletion of customer and vendor master data, see Customizing under ► *Logistics - General* ► *Business Partner* ► *Deletion of Customer and Vendor Master Data* ►.
- For more information about simplified blocking and deletion of central business partner master data, see Customizing for Cross-Application Components under ► *Data Protection* ► *Blocking and Unblocking* ► *Business Partner* ►.

13.5.2.1.5.1.1 Deletion of Personal Data for Product Compliance for Discrete Industries

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

Product Compliance for Discrete Industries uses *SAP ILM* to support the deletion of personal data as described in the following sections.

Relevant Application Objects and Available Deletion Functionality

The following table shows the application objects and the appropriate deletion functionality that is provided in *Product Compliance for the Discrete Industries*.

Application Objects	Provided Deletion Functionality
Worklists for compliance assessment	Archiving object EHPRC_WLCA
Worklists for regulatory changes	Archiving object EHPRC_WLRC
Intenational Material Data Sheets (IMDS)	Archiving object EHPRC_MDS
Compliance data records	Archiving object EHPRC_COD
Campaigns	Archiving object EHPRC_CMP
E-mail assignments	Archiving object EHPRC_PSA
Assessments and BOM transfers	Archiving object EHPRC_PBB

Deletion Report and Job Dependencies

Product Compliance provides the deletion report *R_EHPRC_DPP_CLEANUP* which verifies if any CDOs that are marked as end of business are used in any composition or supplier listing. If this is the case, it changes the lifecycle status to *Active* which prevents the CDO from being archived.

The report needs to be run as a periodic job. Schedule report *R_EHPRC_DPP_CLEANUP* with option *CDOs check Out of Business*, every time before you run the preprocessing and the write program.


For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *R&D / Engineering* ► *Product Safety and Stewardship* ► *Product Compliance (EHS-MGM-PRC)* ► *Data Protection in Product Compliance* ►.

13.5.2.1.5.1.2 Logging Changes

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to track the changes that have been made to this data. When these changes are logged, you should be able to check which employee made which changes, the date and time, the previous value, and the current value.

It is also possible to analyze errors in this way.

See Also

- Go to https://help.sap.com/s4hana_op_2020, enter *Services for Application Developers* into the search bar, press `Enter`, open the search result with that title, and navigate to *Change Documents*.
- Go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press `Enter`, open the search result with that title, and navigate to *Auditing and Logging*.
- See [2125662](#)  for more information about superfluous data change logging defined for database tables.

13.5.2.1.6 Virus Scanning

The interactive forms of *Product Compliance for Discrete Industries* can contain JavaScript. Therefore, JavaScript must be enabled in Adobe Acrobat Reader. In addition, e-mails with PDF attachments that contain JavaScript must not be filtered out in the e-mail inbound and outbound process.

For more generic information see [Virus Scanning \[page 24\]](#) in the *Introduction* section.

13.5.2.2 Product Safety and Stewardship for Process Industries

This section contains information that is valid for:

- Basic Data and Tools
- Product Safety
- Global Label Management
- Dangerous Goods Management

13.5.2.2.1 Technical System Landscape

Product Safety

Expert is a registering Remote Function Call (RFC) server that reads and writes specification data through RFC from the SAP system.

Windows Wordprocessor Integration (WWI) is a registering RFC server that generates and prints reports.

Report shipping can be determined centrally in the product safety system, or product safety document data can be distributed by ALE/IDOC to logistics systems. These logistics systems use their own *WWI* generation servers (*WWI* servers) to print documents.

Dangerous Goods Management

If you use separate logistics systems, dangerous goods data can be transferred to logistics systems by ALE/IDOC.

Global Label Management

The technical system landscape for Global Label Management consists of the following elements:

- *WWI* is a registering RFC server. It can contain its own database that is used as a document cache and data cache.
- Option 1: Label printing is possible with a printer that is connected to a local PC. *WWI* servers are hosted on a central *WWI* server farm. Printing is executed by the SAP spool system or a printer that is connected to a local PC.
- Option 2: Label printing is executed through print requests. *WWI* servers are decentralized. Therefore, the data of the print requests is sent directly to the printer, or the print requests are printed through the SAP spool system.
- Option 3: Label printing is possible via an extraordinary, distributed approach for product safety. In this case, plants host their own SAP systems. Document data is maintained centrally and distributed by ALE. Printing is determined directly or through the SAP spool system.

13.5.2.2.2 User Administration and Authentication

Product Safety and Stewardship for Process Industries uses the administration and authentication mechanisms provided with the *SAPNet Weaver* platform.

For more generic information see [User Administration and Authentication \[page 10\]](#) in the *Introduction* section.

13.5.2.2.3 Network and Communication Security

Your network infrastructure is important for protecting your system. Therefore, your network must support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit known bugs and security holes in network services on the server machines.

The network topology for *Product Safety and Stewardship* is based on the topology used by the ABAP Platform. Therefore, the security guidelines and recommendations described in the ABAP Platform Security Guide also

apply here. Details that specifically apply to *Product Safety and Stewardship* are described in the following sections:

- [Communication Channel Security \[page 509\]](#)
This topic describes the communication paths and protocols.
- [Network Security \[page 510\]](#)
This topic describes the recommended network topology. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports required.
- [Communication Destinations \[page 510\]](#)
This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the *ABAP Platform Security Guide*:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

13.5.2.2.3.1 Communication Channel Security

The following table lists the communication paths used by *Product Safety and Stewardship for Process Industries*, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP PS&S for Process Industries Application Server to SAP BP Application Server	RFC	Business Partner	-
SAP PS&S for Process Industries Application Server to SAP PM Application Server	RFC	Plant Maintenance	-
SAP Logistics Application Server to SAP PS&S for Process Industries Application Server	RFC	Logistics data for Report Shipping Logistics data for Substance Volume Tracking	-
SAP PS&S for Process Industries Application Server to SAP Logistics Application Server	ALE /IDOC	Application data Dangerous Goods data and Reports can be transferred to logistics systems	-
SAP Application Server to Expert Server	RFC	Application data	Substance data may contain corporate secrets such as recipes.

SAP Application Server to WWI generation server (WWI server)	RFC	Application data, documents	Usually MSDS or label data is transferred. Depending on the process, incident reports that contain personal data or corporate secrets may also be transferred.
SAP PS&S for Process Industries Application Server to SAP Logistics Application Server	RFC	Application data: For Global Label Management, material data is transferred from logistics system to the Product Safety system	-
Only for Global Label Management systems with many WWI servers: WWI server to SQL database server	TCP/IP DB-specific protocol	Label data	Usually no sensitive data, depending on the usage of the label.

i Note

Protect RFC connections with *Secure Network Communications* (SNC).

Use secure protocols (SSL, SNC) whenever possible.

13.5.2.2.3.2 Network Security

Ports

WWI generation servers (WWI servers) and Expert servers use Remote Function Call (RFC).

For more information, see <https://help.sap.com/viewer/ports>.

13.5.2.2.3.3 Communication Destinations

The table below lists the communication destinations that are used by *Product Safety and Stewardship for Process Industries*.

For a description of the purpose of the RFC destinations, see the Customizing activities mentioned for *Product Safety and Stewardship for Process Industries*.

Destination	Delivered	Type	User, Authorizations	Description
-------------	-----------	------	----------------------	-------------

[▶▶ Basic Data and Tools ▶](#)
[Basic Settings ▶](#)
[Specify Environment Parameters ▶](#)
 Environment parameter DEST_BU

[▶▶ Basic Data and Tools ▶](#)
[Basic Settings ▶](#)
[Specify Environment Parameters ▶](#)
 Environment parameter DEST_HR

[▶▶ Basic Data and Tools ▶](#)
[Basic Settings ▶](#)
[Specify Environment Parameters ▶](#)
 Environment parameter DEST_PM

[▶▶ Basic Data and Tools ▶](#)
[Basic Settings ▶](#)
[Specify Environment Parameters ▶](#)
 Environment parameter DEST_SRE_DS

[▶▶ Basic Data and Tools ▶](#)
[Basic Settings ▶](#)
[Specify Environment Parameters ▶](#)
 Environment parameter SVT_EHS_RFCDDEST

<p>▶▶ Basic Data and Tools ▶ Basic Settings ▶ Specify Environment Parameters ▶</p> <p>Environment parameter WWI_GENSERWER_SYN_DEST</p>	No	RFC	Calling user	Synchronous generation of reports
<p>▶▶ Basic Data and Tools ▶ Report Definition ▶ Window Wordprocessor Integration (WWI) ▶ Configuration of Generation PCs ▶ Configuration of Generation Servers ▶ Manual Configuration of Generation Servers ▶ Specify Generation Servers ▶</p> <p>Maintain the destination</p>	No	RFC	Configured Background Job user See Customizing activity Start WWI Dispatcher in Background	Background generation of reports
<p>▶▶ Global Label Management ▶ Prerequisites for Global Label Management ▶ Define WWI Settings ▶ Configure WWI Server for Print Request Generation ▶</p>	No	RFC	Calling User	Print and preview tables in Global Label Management

▶ Global Label Management ▶ Prerequisites for Global Label Management ▶ Define WWI Settings ▶ Configure WWI Server for Print Request Generation ▶	No	RFC	Calling User or Configured background job user	Process print requests in Global Label Management See Customizing activity Background Jobs for Processing Print Requests
▶ Basic Data and Tools ▶ Basic Settings ▶ Manage User Exits ▶	No	RFC	Calling User	Determine secondary data for specifications with Expert
▶ Basic Data and Tools ▶ Basic Settings ▶ Specify Environment Parameters ▶	No	RFC	Calling User	Mass change of specification data with Easy Expert

Note

The WWI servers and the Expert servers are registering RFC servers.

For more information about setting up RFC destinations, see the Customizing for [Product Safety and Stewardship](#) under [▶ Basic Data and Tools ▶ Tools ▶ Expert ▶ Set Up RFC Destination. ▶](#)

13.5.2.2.4 Application-Specific Virus Scan Profile (ABAP)

SAP provides an interface for virus scanners to prevent manipulated or malicious files from damaging the system. To manage the interface and to find out which file types are checked or blocked, use the virus scan profiles. Some applications rely on default profiles, while others rely on application-specific profiles.

To use a virus scanner with the SAP system, you must activate and set up the virus scan interface. During this process, you also set up the default behavior. Here, SAP also provides the following default profiles:

Application	Profile	Allowed MIME Types	Blocked MIME Types
Product Safety and Stewardship for Process Industries	/CBUI/WWI_REPORT_GEN	*	-
Global Label Management	/CBGLMP_API/ WWI_GET_CONTENT	*	-

When the application-specific virus scan profile is activated, this profile has the following impact:

- Documents generated by the *WWI* generation server (*WWI* server) are scanned for viruses
- Documents imported into *Product Safety and Stewardship for Process Industries* are scanned for viruses

13.5.2.2.5 Data Storage Security

i Note

When you exchange data between systems, there is a risk that files or file paths are accessed by unauthorized source. To prevent this directory traversal, you have to specify logical file names in the transactions `SFILE` or `SF01`.

For more information, see [File System Access Security \[page 23\]](#) and SAP Note [1497003](#).

For importing or exporting data between two SAP systems or an SAP system and an external system, *Product Safety and Stewardship for Process Industries* uses transfer files.

After generating a transfer file either by exporting data or uploading a transfer file from a PC file system, the transfer file is stored on the application server. If the export is started again or a new file is uploaded from a PC file system, the transfer file that is stored on the application server will be overwritten.

i Note

The transfer file of imported specification data is stored in file `substance.dat` on the application server. The transfer file path is configured in logical path `EHS_IMP_SUBSTANCES_PATH_2`.

Using Logical Path and File Names to Protect Access

When importing or exporting data, *Product Safety and Stewardship for Process Industries* saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used when importing or exporting data, and for which programs these file names and paths apply:

Logical File Names Used in Export and Import

The following logical file names have been created in order to enable the validation of physical file names:

Logical File Names	Programs Using these Logical File Names
EHS_EXP_PHRASES_2	Export of Phrase Libraries
EHS_EXP_PROPERTY_TREE_2	Export of Property Tree
EHS_EXP_SOURCES_2	Export of Sources
EHS_EXP_SUBSTANCES_2	Export of Specification Master Data
EHS_EXP_TEMPLATE_2	Export of Report Templates
EHS_IMP_PHRASES_2	Import of Phrase Libraries
EHS_IMP_PROPERTY_TREE_2	Import of Property Tree
EHS_IMP_SOURCES_2	Import of Sources
EHS_IMP_SUBSTANCES_2	Import of Specification Master Data
EHS_IMP_TEMPLATE_2	Import of Report Templates
EHS_IMP_REPORT_2	Import of Reports
EHS_FTAPPL_2	Upload File; Download File

Logical Path Names Used During Export and Import

These logical file names use the following logical file path:

Logical File Names	Logical Path Names
EHS_EXP_PHRASES_2	EHS_EXP_PHRASES_PATH_2
EHS_EXP_PROPERTY_TREE_2	EHS_EXP_PROPERTY_TREE_PATH_2
EHS_EXP_SOURCES_2	EHS_EXP_SOURCES_PATH_2
EHS_EXP_SUBSTANCES_2	EHS_EXP_SUBSTANCES_PATH_2

EHS_EXP_TEMPLATE_2	EHS_EXP_TEMPLATE_PATH_2
EHS_FTAPPL_2	EHS_FTAPPL_PATH_2
EHS_IMP_PHRASES_2	EHS_IMP_PHRASES_PATH_2
EHS_IMP_PROPERTY_TREE_2	EHS_IMP_PROPERTY_TREE_PATH_2
EHS_IMP_REPORT_2	EHS_IMP_REPORT_PATH_2
EHS_IMP_SOURCES_2	EHS_IMP_SOURCES_PATH_2
EHS_IMP_SUBSTANCES_2	EHS_IMP_SUBSTANCES_PATH_2
EHS_IMP_TEMPLATE_2	EHS_IMP_TEMPLATE_PATH_2

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log (transaction `SM19`).

Relevant audit log numbers:

- DUA – EHS-SADM: Service &A on client &B created
- DUB – EHS-SADM: Service &A on client &B started
- DUC – EHS-SADM: Service &A on client &B stopped
- DUD – EHS-SADM: Service &A on client &B stopped
- DUE – EHS-SADM: Configuration of service &A on client &B was changed
- DUF – EHS-SADM: File &A from client &B transferred
- DUG – EHS-SADM: File &A transferred to client &B

13.5.2.2.5.1 Data Storage on WWI Servers and Expert Servers

Windows Wordprocessor Integration (WWI) and Expert read data from the SAP system using Remote Function Call (RFC), process data, and store the results in the database of the SAP system. That is, the WWI generation server (WWI server) and the Expert server save configuration data and cached data locally.

i Note

Make sure that only as few users as possible can access the Windows servers that run the WWI server and the Expert server.

To apply access permissions in Windows, execute the following steps for the following folders.

For more information on access control and on security auditing, see the Windows Help.

To configure access control for a local file or folder, proceed as follows:

1. Start the *Windows Explorer*.
2. In the context menu of the file or the folder that you want to audit, choose *Properties*, and go to the *Security* tab page.
3. Choose *Edit*.
4. Add or remove the user names and set the permissions for each user.

i Note

To improve data storage security, you can apply Windows file system encryption to the folders that hold sensitive data.

Expert Cache

If you use the specification data cache of Expert, it stores copies of the specification data locally in the Expert server file system. The root folder of the cache is determined in the registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TechniData\EHS-AddOns\CacheRoot`.

To protect data, make sure that you set appropriate access permissions on the configured root folder of the cache. Grant read or write access only to `LocalSystem`, to administrators and to selected users.

Expert Rules

Apply access permissions to the Expert rules directory. Expert rules are programs that are executed by Expert altering specification data. Make sure that the rules are not altered by unauthorized users.

The rules are usually stored in the Rules folder of the Expert installation, but each rule can be configured separately in the Windows Registry. For more information on the paths to the rules files, see `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TechniData\EHS-AddOns\Instances`.

Set appropriate access permissions on the Expert rules folder. Grant access only to `LocalSystem`, to administrators and to selected users.

WWI Root Directory

WWI temporarily stores data in the Windows file system to process data in the WWI root directory.

If an error occurs, the temporary files might remain in the root directories. We recommend cleaning up the folder regularly.

The path that indicates the WWI root directory depends on the process. For more information about the path, check the Customizing settings for *Product Safety and Stewardship for Process Industries*.

- For synchronous generation, check the environment parameter `WWI_GENSERVER_SYN_ANCHOR` under [Basic Data and Tools](#) > [Basic Settings](#) > [Specify Environment Parameters](#) >
- For background generation, check the WWI root under [Basic Data and Tools](#) > [Report Definition](#) > [Windows Wordprocessor Integration \(WWI\)](#) > [Configuration of Generation PCs](#) > [Configuration of Generation Servers](#) > [Manual Configuration of Generation Servers](#) > [Specify Generation Servers](#) >
- For Global Label Management, check the temporary directory for synchronous WWI server under [Global Label Management](#) > [Set Basic Data and Tools for Global Label Management](#) > [Make Settings for Basic Data](#) >
- For print request processing in Global Label Management, check `HKEY_CLASSES_ROOT\WWIDOCUMENT\AnchorRoot` in the Windows registry.

Grant access on the WWI root folders only to `LocalSystem`, to administrators and to selected users.

WWI Print Request Cache for Global Label Management

WWI caches templates and generated labels in the Windows file system.

The path that indicates the Windows file system is configured in the WWI.INI file under `[DMS]`. Set the appropriate access permissions on the WWI root directories. Grant read or write access only to the WWI user, to the `LocalSystem`, to administrators and to selected users.

The database file or database connection is configured under `dbConnection` in the WWI.INI file: Set appropriate access permissions on the database file or in the configured database management system. Grant access only to the WWI user, to `LocalSystem`, to administrators and to selected users.

13.5.2.2.6 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that *Product Safety and Stewardship for Process Industries* provides to support compliance with the relevant requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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 given system landscape and the applicable legal requirements.

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.

13.5.2.2.6.1 Deletion of Personal Data

Product Safety and Stewardship for Process Industries might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use *SAP Information Lifecycle Management (SAP ILM)* to control the blocking and deletion of personal data in *Product Safety and Stewardship for Process Industries*.

More Information

- For general information about the blocking and deletion of data for customers, vendors and business partners, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.
- For more information about the deletion of customer and vendor master data, see the Security Guide for SAP ERP on the SAP Help Portal at <http://help.sap.com/erp> under ► *SAP ERP Central Component Security Guide* ► *Data Protection* ► *Deletion of Personal Data* ►.
- For more information about simplified blocking and deletion of customer and vendor master data, see Customizing under ► *Logistics - General* ► *Business Partner* ► *Deletion of Customer and Vendor Master Data* ►.
- For more information about simplified blocking and deletion of central business partner master data, see Customizing for Cross-Application Components under ► *Data Protection* ► *Blocking and Unblocking* ► *Business Partner* ►.
- For more information about simplified blocking and deletion of customer and vendor master data in other applications, see Customizing of the application under ► *Data Protection* ►.
- For more information about settings for authorization management, see Customizing of the application under ► *Data Protection* ► *Authorization Management* ►.

13.5.2.2.6.1.1 Deletion of Personal Data for Substance Volume Tracking

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

Substance Volume Tracking uses *SAP ILM* to support the deletion of personal data as described in the following sections.

Process Flow: Data Destruction

1. Before deleting data in *Substance Volume Tracking*, define the retention periods in *SAP Information Lifecycle Management* in transaction *ILM Policies* (IRMPOL) for the following ILM objects:
 - EHS_SVT_SOLDQ_DESTRUCTION
 - EHS_SVT_OR_DESTRUCTION
2. To destroy data, proceed as described in the documentation of the data destruction objects in *Substance Volume Tracking*.
See section *Relevant Application Objects and Available Deletion Functionality* for the relevant data destruction objects in *Substance Volume Tracking*.

For more information, see SAP Note [2320353](#) (Simplified data deletion based on SAP ILM in substance volume tracking).

Relevant Application Objects and Available Deletion Functionality

The following table shows the application objects and the appropriate deletion functionality that is provided in *Substance Volume Tracking*.

Application	Provided Deletion Functionality
Assignment of External Business Partners or External Only Representatives to Regulatory Lists	Data destruction object to check the assignment of external business partners or external only representatives to regulatory lists. Destroys those assignments that are no longer relevant once the retention period expires.
Property <i>Sold Quantities</i>	Data destruction object to destroy data of the property <i>Sold Quantities</i> that is assigned to business partner numbers and that is no longer relevant once the retention period expires.

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *R&D / Engineering* ► *Product Safety and Stewardship* ► *Product Safety (EHS-SAF)* ► *Data Destruction in Product Safety* .

Integration: EoP Check for Customer Master and Vendor Master

In addition to deleting data of substance volume tracking processes, *Substance Volume Tracking* provides an end of purpose (EoP) check to support the blocking and deletion of personal data of customer master (customer master data) and vendor master (vendor master data) that have been entered in *Substance Volume Tracking*.

The EoP check for *Substance Volume Tracking* is integrated in the following ILM objects of *SAP ERP*:

- FI_ACCRECV (customer master data)
- FI_ACCPAYB (vendor master data)

EoP Check for Customer Master and Vendor Master

The end of purpose (EoP) check that has been implemented in *Substance Volume Tracking* determines whether a certain **customer master** or a certain **vendor master** is used in **one** of the following tables:

- CCRCT_OR (*EHS: Inc./Acc. Log - Data for Person Affected (Event)*)
- CCRCT_CU (*EHS: Customer List - Header Data*)
- CCRCT_SO (*EHS: Confirmed Sold Quantities*)
- CCRCT_SOPL (*EHS: Planned Sold Quantities*)

Furthermore, the EoP check determines whether this business partner is still relevant for the business activities in *Substance Volume Tracking*.

If a customer master or a vendor master is assigned to a material as an external only representative or as an external customer, the system checks whether the business purpose has ended or is still in process. The EoP check then reports the status message *No Business*, *Ongoing Business*, or *Business Complete* to the customer master or the vendor master.

Process Flow: EoP Check for ERP Customer Master and ERP Vendor Master

You can determine the EoP check for ERP Customer Master and ERP Vendor Master that are used in *Substance Volume Tracking* as follows:

- Run transaction *ILM Policies* (IRMPOL) and enter the required residence policies for the customer master data and the vendor master data (ILM objects FI_ACCPAYB and FI_ACCRECV).
- Run transaction *Block Customer & Vendor Master Data* (CVP_PRE_EOP) to enable the end of purpose check function for the ERP customer master and the ERP vendor master (ERP_CUST and ERP_VEND).

For more information about the deletion of customer and vendor master data, see the Security Guide for SAP ERP on the SAP Help Portal at <http://help.sap.com/erp> under ► *SAP ERP Central Component Security Guide* ► *Data Protection* ► *Deletion of Personal Data* ►.

13.5.2.2.6.1.2 Deletion of Personal Data for Report Shipping

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

Report Shipping uses *SAP ILM* to support the deletion of personal data as described in the following sections.

Process Flow: Data Blocking and Data Destruction

1. Before blocking and deleting data in *Report Shipping*, define the residence times and retention periods in *SAP Information Lifecycle Management* in transaction *ILM Policies* (IRMPOL) for the EHS_PS_REPHIS_DESTRUCTION ILM object.

- To block data that match the residence times, run the program RC1_REPHIS_BLOCK to block report shipping orders of status *Historical*, *Archived*, or *Rejected*.
For more information, see the documentation of this program in the *ABAP: Program Execution* (transaction SA38).
- To destroy data, proceed as described in the documentation of the data destruction object in *Report Shipping*.
See section *Relevant Application Objects and Available Deletion Functionality* for the relevant data destruction objects in *Report Shipping*.

Relevant Application Objects and Available Deletion Functionality

The following table shows the application object and the appropriate deletion functionality that is provided for *Report Shipping*.

Application	Provided Deletion Functionality
Report Shipping	Data destruction object to destroy report shipping orders with the status <i>Historical</i> , <i>Archived</i> , or <i>Rejected</i> that are no longer relevant once the retention period expires.

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *R&D / Engineering* ► *Product Safety and Stewardship* ► *Product Safety (EHS-SAF)* ► *Data Destruction in Product Safety* ►.

Integration: EoP Check for Customer Master and Vendor Master

In addition to blocking and deleting data of report shipping processes, *Report Shipping* provides an end of purpose (EoP) check to support the blocking and deletion of personal data of customer master (customer master data) and vendor master (vendor master data) that have been entered in *Report Shipping*.

The EoP check for *Report Shipping* is integrated in the following ILM objects of *SAP ERP*:

- FI_ACCRECV (customer master data)
- FI_ACCPAYB (vendor master data)

EoP Check for Customer Master and Vendor Master

The end of purpose (EoP) check that has been implemented in *Report Shipping* determines whether a certain **customer master** or **vendor master** is used in table CVDDEH (*EHS: Report shipping orders*) and is therefore still relevant for business activities in *Report Shipping*.

If a customer master or a vendor master is used as a recipient in a report shipping order, the system checks whether the business purpose has ended or is still in process. The EoP check then reports the status message *No Business*, *Ongoing Business*, or *Business Complete* to the **customer master** or the **vendor master**.

Process Flow: EoP Check for ERP Customer Master and ERP Vendor Master

You can determine the EoP check for ERP Customer Master and ERP Vendor Master that are used in *Report Shipping* as follows:

- Run transaction *ILM Policies* (IRMPOL) and enter the required residence policies for the customer master data and the vendor master data (ILM objects FI_ACCPAYB and FI_ACCRECV).
- Run transaction *Block Customer & Vendor Master Data* (CVP_PRE_EOP) to enable the end of purpose check function for the ERP customer master and the ERP vendor master (ERP_CUST and ERP_VEND).

For more information about the deletion of customer and vendor master data, see the Security Guide for SAP ERP on the SAP Help Portal at <http://help.sap.com/erp> under ► *SAP ERP Central Component Security Guide* ► *Data Protection* ► *Deletion of Personal Data* ►.

13.5.2.2.6.1.3 Deletion of Personal Data for Report Management

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

Report Management uses *SAP ILM* to support the deletion of personal data as described in the following.

Process Flow: Data Blocking and Data Destruction

1. Before blocking and deleting data in *Report Management*, define the residence times and retention periods in *SAP Information Lifecycle Management* in transaction *ILM Policies* (IRMPOL) for the EHS_PS_REPMAN_DESTRUCTION ILM object.
2. To block data that match the residence times in *Report Management*, run program RC1_REPHIS_BLOCK to block the report shipping orders of a certain status.
For more information, see the documentation of this program in the *ABAP: Program Execution* (transaction SA38).
3. To destroy data, proceed as described in the documentation of the data destruction object in *Report Management*.
See section *Relevant Application Objects and Available Deletion Functionality* for the relevant data destruction objects in *Report Management*.

Relevant Application Objects and Available Deletion Functionality

The following table shows the application object and the appropriate deletion functionality that is provided for *Report Management*.

Application	Provided Deletion Functionality
Report Management	Data destruction object to destroy inbound-reports with the status <i>Historical</i> or <i>Archived</i> that are no longer relevant once the retention period expires.

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *R&D / Engineering* ► *Product Safety and Stewardship* ► *Product Safety (EHS-SAF)* ► *Data Destruction in Product Safety* ►.

13.5.2.2.6.1.4 Deletion of Personal Data for Global Label Management

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

Global Label Management uses *SAP ILM* to support the deletion of personal data as described in the following.

The data destruction for *Global Label Management* is integrated in the FI_ACCRECV (*customer master data*) ILM object of *SAP ERP*.

You use BAdI method IF_EX_FI_ACCRECV_WRITE~DELETE of BAdI implementation EHS_LABELING_DPP to delete customer-specific labels in table CCGLT_CLBL (*EHS: Customer-Specific Labels*) that are related to the customer master and the vendor master to be deleted.

Additionally, you have to set up program *Reorganize Print Requests and Change Documents* (RCBGL_PRINTREQUEST_REORG) to delete the relevant entries in tables CCGLT_PRTREQ_HDR (*EHS: Print Request Header Table*) and CCGLT_PRTREQ_PAR (*EHS: Print Request Parameters*).

More Information

SAP Note [2327810](#) (Simplified data deletion based on SAP ILM in Global Label Management)

For more information about the deletion of customer and vendor master data, see the Security Guide for SAP ERP on the SAP Help Portal at <http://help.sap.com/erp> under ► *SAP ERP Central Component Security Guide* ► *Data Protection* ► *Deletion of Personal Data* ►.


13.5.2.2.6.2 Logging Changes

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to track the changes that have been made to this data. When these changes are logged,

you should be able to check which employee made which changes, the date and time, the previous value, and the current value.

It is also possible to analyze errors in this way.

See Also

- Go to https://help.sap.com/s4hana_op_2020, enter *Services for Application Developers* into the search bar, press `Enter`, open the search result with that title, and navigate to *Change Documents*.
- Go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press `Enter`, open the search result with that title, and navigate to *Auditing and Logging*.
- See [2125662](#)  for more information about superfluous data change logging defined for database tables.

13.5.2.2.6.2.1 Change Logging in Substance Volume Tracking

Setting Up Change Logs for Substance Volume Tracking

Substance Volume Tracking processes personal data of only representatives for external and internal business partners. If any changes are made regarding these internal and external business partners, the system logs the following information on personal data:

- The user who has changed data
- Date and time of the change
- Change type
- Transaction of the data change
- Data origin
- Internal and external only representatives whose data have been changed
- Internal and external business partners whose data have been changed

You can set up the change logging for external and internal business partners in transaction *Maintain Profile Parameters* (RZ10) as follows:

1. Enter the name of the start profile or the system profile to be edited and select *Extended Maintenance* under *Edit Profile*.
2. Change the profile by entering the following:
 - *Parameter Name*: `rec/client`
 - *Parameter Value*: Enter the client of the system in which you want to log data.
3. Save and activate the profile.
4. Restart the application server.

The system now logs all changes of internal and external business partners, and internal and external only representatives that are made in table `CCRCT_OR` (*Material Business Partner Only Representative Assignment*) of *Substance Volume Tracking*.

All changes are logged in table DBTABLOG.

Displaying Change Logs in Substance Volume Tracking

You can call up the change logs in transaction *Table History* (SCU3).

For more information see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *R&D / Engineering* ► *Product Safety and Stewardship* ► *Product Safety (EHS-SAF)* ► *Data Protection in Product Safety* ► *Logging Changes in Substance Volume Tracking* ►

More Information

- For more information on logging changes in *Substance Volume Tracking*, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *R&D / Engineering* ► *Product Safety and Stewardship* ► *Product Safety (EHS-SAF)* ► *Data Protection in Product Safety* ►
- See [2125662](#) 📄 for more information about superfluous data change logging defined for database tables.

13.5.2.2.7 Dispensable Functions with Impacts on Security

You can compile and display system information for Windows Wordprocessor Integration (WWI) as follows:

- You can display system information in the *WWI Monitor* (transaction CG5Z): In the menu, choose ► *Utilities* ► *Test Server* ►
- In WWI.INI, under [Global], enter as *DisableWwiServerInfo* the value 1. This prevents external access to the WWI system information (through the *WWI Server Monitor*, for example). The default value is 0.

13.5.2.2.8 Security for Additional Applications

Windows Authorization for Windows Wordprocessor Integration

Windows Wordprocessor Integration (WWI) requires a Windows user account that is used to run the WWI generation server services. This is because many printer settings and settings for Microsoft Word are user-specific.

As an abbreviation, the user account is called *WWI user*.

- Create a new Windows user. This user is used to execute the WWI generation server (WWI server). The user can be a local user or a domain user. We recommend creating a local user, for example, `WWI-USER`. Assign this user to the *Main users* group or the *Users* group. Use a password that does not expire.
- In Microsoft Windows Vista, in Microsoft Windows Server 2008 and higher releases, assign the WWI user to the administrators group.
- If the user is a domain user, ensure that the profile of the user is `local`.
- Check the security settings for the user that is used to execute the WWI server:
 - The user must have the *Log on as a service* authorization. In Microsoft Windows XP, Microsoft Windows Server 2003 and higher releases, also set this authorization for users of the administrators group. You can find this authorization in the Control Panel under ► *Administrative Tools* ► *Local Security Policy* ▾. Navigate to ► *Local Policies* ► *User Rights Assignment* ▾. Here, you assign the user privileges to the guideline *Log on as a service*.
 - Check the DCOM start authorization and access authorization for Microsoft Word using the `DCOMCNFG.EXE` configuration program. For more information, see the SAP Note [580607](#) 📄.
 - Ensure that the user has write (change) authorization for the WWI root directory. We recommend using a local directory. The WWI work directory is configured in the *Specify Generation Servers* Customizing activity.
 - Make sure that the Microsoft Windows TEMP directory exists. The TEMP directory is configured in Microsoft Windows under ► *Control Panel* ► *System* ► *Advanced* ► *Environment Variables* ▾. There, check the user variables and system variables TMP and TEMP.
 - Ensure that the user has write (change) authorization for the Microsoft Windows TEMP directory.

For further information, see SAP Note [580586](#) 📄.

Windows Authorization for Expert

The Expert server service is run as a local system account.

Windows Authorization for Administration Management Server

The Administration Management Server service is run as a local system account.

13.5.2.2.9 Security-Relevant Logging and Tracing

Windows Wordprocessor Integration (WWI) and Expert log all processing information in the Windows Application Event Log. A separate Security Log for WWI and Expert does not exist. For security relevant information from Windows, check the Windows Security Event Log.

For more information on maintaining a secure environment in Windows servers, check the *Microsoft Windows Security Guide* and the *Microsoft Security Compliance Manager*.

Tracking Configuration Changes

To track configuration changes of WWI and Expert Server Administration that are executed by *WWI and Expert Server Administration* (transaction CGSADM), enable the security audit log in the *Security Audit* (transaction SM19).

Relevant audit log numbers:

- DUA – EHS-SADM: Service &A on client &B created
- DUB – EHS-SADM: Service &A on client &B started
- DUC – EHS-SADM: Service &A on client &B stopped
- DUD – EHS-SADM: Service &A on client &B stopped
- DUE – EHS-SADM: Configuration of service &A on client &B was changed
- DUF – EHS-SADM: File &A from client &B transferred
- DUG – EHS-SADM: File &A transferred to client &B

For more information on configuration changes, change documents are used. Creating change documents in *WWI and Expert Server Administration* is enabled by default. To switch off the creation of change documents, set the environment parameter CGSADM_NO_CHANGE_DOCS in the *Specify Environment Parameters* Customizing activity to X.

To display change documents, start the program RSSCD110 (Display change documents (cross-client)) and choose object class ESSADM.

Tracking Configuration with Windows Features

To track WWI and Expert configuration changes, enable auditing in the Windows file system. For more information on Access Control and Security Auditing, see the Windows Help.

Before setting up auditing for files and folders, enable object access auditing by defining auditing policy settings for the object access event category.

To define or modify auditing policy settings for an event category for your local computer, proceed as follows:

1. Choose ► *Control Panel* ► *Administrative Tools* ► *Local Security Policy*. ►
2. In the console tree, go to ► *Local Policies* ► *Audit Policy*. ►
3. In the results pane, choose *Audit object access* to enable the auditing policy settings.

To configure auditing settings for a local file or folder, proceed as follows:

1. Open *Windows Explorer*.
2. In the context menu of the file or folder that you want to audit, choose *Properties* and go to the *Security* tab page.
3. Choose *Edit*, and then choose *Advanced*.
4. In the *Advanced Security Settings* go to the *Auditing* tab page.

To configure auditing settings for a registry key:

1. Open *Registry Editor*.
2. Go to the registry key.

3. In the context menu of the registry key that you want to audit, choose *Permissions*.
4. On the *Security* tab page, choose *Advanced*.
5. In the *Advanced Security Settings*, choose the *Auditing* tab page.

Windows Wordprocessor Integration (WWI)

For WWI, the following files and folders must be covered by change auditing:

- WWI.INI
- SAPRFC.INI
- GRAPHICS
- Registry key: HKEY_CLASSES_ROOT\WWIDOCUMENT

Expert

For Expert, the following files and folders must be covered by change auditing:

- SAPRFC.INI
- RULES
- Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TechniData\EHS-AddOns\Instances

For 32bit systems, omit Wow6432Node

- Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TechniData\EHS-AddOns\System

For 32bit systems, omit Wow6432Node

13.5.3 Enterprise Portfolio and Project Management

13.5.3.1 Project System

13.5.3.1.1 Deletion of Personal Data

Use

The `Project System` might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Project System (PS)	The archiving objects are used for archiving and deleting operative objects and standard networks in the Project System	Archiving Objects: <ul style="list-style-type: none">• PS_PROJECT• PS_PLAN

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Project System (PS)	EoP	An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. This check is determined based on the date on which the network activity is set to the closed status. For more information, refer to sections Process Flow and Configuration: Simplified Blocking and Deletion .

Application	Implemented Solution (EoP or WUC)	Further Information
Project System (PS)	WUC	<p>A where-used check is a simple check to ensure data integrity in case of potential blocking. The WUC in application Project System checks whether any dependent data exists for:</p> <ul style="list-style-type: none"> • A certain customer in RSADD, VRSADD_CN, COFP, COER, QMSM, QMUR, QMEL, IHPA. • A certain vendor in RSADD, VRSADD_CN, AFVC, VSAFVC_CN, RESB, VS_RESB_CN, COFP, QMSM, QMUR, QMEL, IHPA. • A certain contact person in QMSM, QMUR, IHPA. • A certain cBP in ADO1DLI, PSACL_TAB. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>i Note</p> <p>If dependent data exists, that is, if the data is still required for business activities, the system does not block the corresponding customer, vendor, or cBP. If you still want to block data, the dependent data must be deleted by using the existing archiving and deletion tools or by using any other customer-specific solution.</p> </div>

Process Flow

1. Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
3. You do the following:
 - Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA).
 - Run transaction BUPA_PRE_EOP to enable the end of purpose check function for the central business partner.
 - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and vendor master (ILM objects: FI_ACCPAYB, FI_ACCRECV, FI_ACCKNVK).
 - Run transaction CVP_PRE_EOP to enable the end of purpose check function for the customer master and vendor master.

4. Business users can request unblocking of blocked data by using the transaction `BUP_REQ_UNBLK`.
5. If you have the needed authorizations, you can unblock data by running the transaction `BUPA_PRE_EOP` and `CVP_UNBLOCK_MD`.
6. You delete data by using the transaction `ILM_DESTRUCTION` for the ILM objects of PS.

For information about how to configure blocking and deletion for PS, see [Configuration: Simplified Blocking and Deletion](#).

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for `Cross-Application Components` under `Data Protection`.

- Define the settings for authorization management under [Data Protection > Authorization Management](#). For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for [Cross-Application Components](#) under [Data Protection > Blocking and Unblocking of Data > Business Partner](#).
- You configure the settings related to the blocking and deletion of customer and vendor master data in Customizing for:
 - [Logistics - General > Business Partner > Deletion of Customer and Supplier Master Data](#)

13.5.3.2 Commercial Project Management

13.5.3.2.1 Authorizations

The following section provides an overview of the authorizations that apply to Commercial Project Management.

Based on your business needs, you can choose one of the following component combinations as a deployment option:

Deployment Option	Project Workspace	Project Cost and Revenue Planning	Project Issue and Change Management	SAP BusinessObjects Analysis for Microsoft Office
Option 1	x	x	x	x
Option 2	x	x		x
Option 3	x		x	x
Option 4	x			x

The following standard roles can be used as templates to build your own roles, based on the option you have deployed.

Standard Roles

Commercial Project Management

Role	Description
SAP_BPR_CPD_USER_1	Provides <i>Display</i> authorizations for Commercial Project Management.

Project Workspace

Role	Description
SAP_SR_CPD_PWS_USER_1	Provides <i>Display</i> authorizations for Commercial Project Management.
SAP_SR_CPD_PM_1	Allows the creation, change, and display of commercial projects and financial plans and provides authorizations to users working as project managers.
SAP_SR_CPD_PICM_PM_1	Provides <i>Create</i> , <i>Change</i> , and <i>Display</i> authorizations for objects in Project Issue and Change Management.
SAP_BR_PRJTEAMMEMBER_COMMPRJ	Allows team members to use the following Fiori app: <ul style="list-style-type: none">Commercial Projects: Activities
SAP_BR_PROJECTMGR_COMMPRJ	Allows project managers to use the following Fiori apps: <ul style="list-style-type: none">Commercial Projects: ActivitiesCommercial Projects: Multiproject OverviewCommercial Projects: Single-Project OverviewCommercial Projects: Billing and Receivables OverviewCommercial Projects: Procurement Overview

Project Cost and Revenue Planning

Role	Description
SAP_SR_CPD_PFP_USER_1	Provides <i>Display</i> authorizations for objects relevant to Project Cost and Revenue Planning.
SAP_SR_CPD_PM_1	Allows the creation, change, and display of commercial projects and financial plans. The role provides authorizations to users working as project managers.
SAP_SR_CPD_PICM_PM_1	Provides <i>Create</i> , <i>Change</i> , and <i>Display</i> authorizations for objects in Project Issue and Change Management.

Project Issue and Change Management

Role	Description
SAP_SR_CPD_PICM_USER_1	Provides <i>Display</i> authorizations for objects in Project Issue and Change Management.
SAP_SR_CPD_PICM_PM_1	Provides <i>Create</i> , <i>Change</i> , and <i>Display</i> authorizations for objects in Project Issue and Change Management.

13.5.3.2.2 Data Storage Security

In Commercial Project Management, the header data of the financial plan is stored in the database tables of Project Cost and Revenue Planning.

- Data is saved in the database tables of Project Cost and Revenue Planning when the user explicitly chooses the Save pushbutton on the financial planning screen.
- The planning data is stored in the BW InfoCube and can be transferred to the S4CORE database tables by the user.
- Data is saved in the BW InfoCube when the user explicitly chooses the *Save Data* pushbutton in the Analysis Office workbook.
- Data is saved in S4CORE database tables when the user explicitly chooses the *Transfer Data* pushbutton on the financial planning screen.

13.5.3.2.3 Data Archiving

13.5.3.2.3.1 Archiving Commercial Projects

You can use *Archiving Object for Commercial Projects* (/CPD/PWS_M) to archive commercial projects that are no longer needed. Archiving allows you to reduce the load on your database.

Structure

Tables

Tables for Commercial Projects

Table	Description
/CPD/S_MP_HDR_K	Commercial Project Header
/CPD/D_MP_HDR_S	Commercial Project Header Short Text
/CPD/D_MP_ITEM	Commercial Project Structure Elements
/CPD/D_MP_MEMBER	Project Member
/CPD/D_MP_REP_AT	Reporting Attribute Node
/CPD/D_MP_RESP	Responsibility Node
/CPD/D_MP_STATUS	Status Header
/CPD/D_MP_ST_ARV	Table for Status Area Version
/CPD/D_MP_ST_HRA	Status Header Area
/CPD/D_MP_ST_VHR	Status Versions

Table	Description
/CPD/D_MP_TEAM	Team
/CPD/D_MP_TEAM_M	Team Member Subnode
/CPD/D_MP_TEAM_R	Team Role Subnodes

Programs

The following programs are available for /CPD/PWS_M:

- Preprocessing: /CPD/PWS_ARCH_MP_PRE
This program makes the following checks for commercial projects:
If both these conditions are satisfied, the program sets the archiving status of the commercial project to Archiving in Process (O2).
- Write: /CPD/PWS_ARCH_MP_WRITE
This program checks if an object has the status Archiving in Process (O2). If the status is O2, the program archives the object to the archive file.
- Delete: /CPD/PWS_ARCH_MP_DELETE
This program verifies archived files against the data in the database, and deletes all objects in the database that have been successfully archived.

Information Lifecycle Management (ILM)

Information Lifecycle Management (ILM) allows you to define rules for storing archived business data, set legal holds on stored data, and destroy the data in adherence to legal requirements.

The ILM object CPD_PWS_M is available for commercial projects and this ILM object allows you to model retention rules based on the following fields:

- Condition Fields
 - Archiving Status
 - Commercial Project Type
 - Organization
- Time Reference Fields
 - End Date

You can use the transaction IRMPOL to define policies and rules for ILM.

Prerequisites

The prerequisites for *Retention Management* are:

- You have activated the business function ILM
- You have assigned the following objects to an audit area:
 - CPD_PWS_M

More Information

To change the residence time, you can make settings in Customizing for *Cross-Application Components* under [▶ Processes and Tools for Enterprise Applications](#) > [Reusable Objects and Functions for BOPF Environment](#) > [Archiving Adapter](#) > [Maintain BO-Specific Residence Periods](#) >

13.5.3.2.3.2 Archiving Financial Plans

You can use *Archiving Object for Financial Plans* (/CPD/PFP_P) to archive financial plans that are no longer needed. Archiving allows you to reduce the load on your database.

Structure

Tables

Tables for Financial Plans

Table	Description
/CPD/D_PFP_PH	Plan Header
/CPD/D_PFP_PV	Plan Version
/CPD/D_PFP_PS	Plan Structure
/CPD/D_PFP_PER	Plan Exchange Rate
/CPD/D_PFP_PHTXT	Plan Header Text
/BOBF/D_ATF_RT	Attachment Root
/BOBF/D_ATF_DO	Attachment Document
/BOBF/D_TXCROOT	Text Collection Root
/BOBF/D_TXCTXT	Text Collection Text
/BOBF/D_TXCCON	Text Collection Text Content

Programs

The following programs are available for /CPD/PFP_P:

- Preprocessing: /CPD/PFP_ARCH_PH_PRE
This program checks whether a financial plan is ready for archiving. A financial plan is ready for archiving when:
 - Related financial plan versions have a status that indicates completion.
 - All related change requests and change request alternatives are ready for archiving, with the status as Archiving in Process (02). This is only applicable if you are also using *Project Issue and Change Management*.
 - The financial plan has a status that indicates completion.

If the object is ready, this program sets the status as Archiving in Process (02) in the database.

i Note

After the preprocessing program has run, the objects marked for archiving are no longer made available on the UI. The program also deletes corresponding data from the real-time InfoCube (/CPD/PFP_R01) and transfers the data into the InfoCube for archiving (/CPD/PFP_C01).

- Write: /CPD/PFP_ARCH_PH_WRITE

This program checks if an object has the status Archiving in Process (O2). If the status is O2, the program archives the object to the archive file.

- Delete: /CPD/PFP_ARCH_PH_DELETE
This program verifies archived files against the data in the database; and deletes all objects in the database that have been successfully archived.

Information Lifecycle Management (ILM)

Information Lifecycle Management (ILM) allows you to define rules for storing archived business data, set legal holds on stored data, and destroy the data in adherence to legal requirements.

The ILM object CPD_PFP_P is available for financial plans and this ILM object allows you to model retention rules based on the following fields:

- Condition Fields
 - Plan Scenario ID
 - Plan Type ID
 - Archiving Status
- Time Reference Fields
 - End Date

You can use the transaction IRMPOL to define policies and rules for ILM.

Prerequisites

The prerequisites for *Retention Management* are:

- You have activated the business function ILM
- You have assigned the following objects to an audit area:
 - CPD_PFP_P

More Information

To change the residence time, you can make settings in Customizing for *Cross-Application Components* under [▶ Processes and Tools for Enterprise Applications](#) > [Reusable Objects and Functions for BOPF Environment](#) > [Archiving Adapter](#) > [Maintain BO-Specific Residence Periods](#) >.

13.5.3.2.3.3 Archiving Issues and Change Requests

You can use *Archiving Object for Issues and Change Requests* (/PICM/BO_I) to archive issues and change requests that are no longer needed. Archiving allows you to reduce the load on your database.

Structure

Tables

Tables for Issues and Change Requests

Table	Description
/BOBF/D_ATF_DO	Document node of attachment folder

Table	Description
/BOBF/D_ATF_RT	Root nodes of attachment folder
/BOBF/D_TXCCON	Text content
/BOBF/D_TXCROOT	Root node of text collection
/BOBF/D_TXCTXT	Text
/IAM/D_I_ATT	Attachment
/IAM/D_I_DATE	Date
/IAM/D_I_DESC	Description node
/IAM/D_I_DESC_TX	Language-dependent description text node
/IAM/D_I_OBJ_REF	Issue reference node
/IAM/D_I_OREF_DT	Language-dependent, reference, description text node
/IAM/D_I_PARTY	Party node
/IAM/D_I_QTY	Quantity
/IAM/D_I_ROOT	Root node

Programs

The following programs are available for /PICM/BO_I:

- Preprocessing: /PICM/ARCH_ISSUE_CR_ROOT_PRE
This program checks if an object is ready for archiving by verifying the following conditions:
 - The adherence to the specified residence time
 - The availability of activities for the object
If the object is ready, this program sets the status as Archiving in Process (02) in the database. After the preprocessing program has run, the objects marked for archiving are no longer made available on the UI.
- Write: /PICM/ARCH_ISSUE_CR_ROOT_WRITE
This program checks if an object has the status Archiving in Process (02). If the status is 02, the program archives the object to the archive file.
- Delete: /PICM/ARCH_ISSUE_CR_ROOT_DEL
This program verifies archived files against the data in the database; and deletes all objects in the database that have been successfully archived..

More Information

To change the residence time, you can make settings in Customizing for [Cross-Application Components](#) under [► Processes and Tools for Enterprise Applications](#) ► [Reusable Objects and Functions for BOPF Environment](#) ► [Archiving Adapter](#) ► [Maintain BO-Specific Residence Periods](#) ►.

13.5.3.2.3.4 Archiving Activities

You can use *Archiving Object for Activities* (/PICM/BO_A) to archive activities that are no longer needed. Archiving allows you to reduce the load on your database.

Structure

Tables

Tables for Activities

Table	Description
/BOBF/D_ATF_DO	Document node of attachment folder
/BOBF/D_ATF_RT	Root nodes of attachment folder
/BOBF/D_TXCCON	Text content
/BOBF/D_TXCROOT	Root node of text collection
/BOBF/D_TXCTXT	Text
/IAM/D_ACT_ATT	Attachment
/IAM/D_ACT_DATE	Date
/IAM/D_ACT_DESC	Description node
/IAM/D_ACT_DTXT	Language-dependent description text node
/IAM/D_ACT_FOA	Follow-up action
/IAM/D_ACT_FOA_P	Follow-up action parameter
/IAM/D_ACT_OBJ_RF	Object reference
/IAM/D_ACT_OREF_DT	Language-dependent description texts
/IAM/D_ACT_PARTY	Party
/IAM/D_ACT_QTY	Activity quantity

Programs

The following programs are available for /PICM/BO_A:

- **Preprocessing:** /PICM/ARCH_ACTIVITY_ROOT_PPROC
This program checks if an object is ready for archiving by verifying the adherence to the specified residence time. If the object is ready, this program sets the status as Archiving in Process (02) in the database. After the preprocessing program has run, the objects marked for archiving are no longer made available on the UI.
- **Write:** /PICM/ARCH_ACTIVITY_ROOT_WRITE
This program checks if an object has the status Archiving in Process (02). If the status is 02, the program archives the object to the archive file.

- Delete: /PICM/ARCH_ACTIVITY_ROOT_DEL
This program verifies archived files against the data in the database; and deletes all objects in the database that have been successfully archived.

More Information

To change the residence time, you can make settings in Customizing for *Cross-Application Components* under [► Processes and Tools for Enterprise Applications](#) ► [Reusable Objects and Functions for BOPF Environment](#) ► [Archiving Adapter](#) ► [Maintain BO-Specific Residence Periods](#) ►.

13.5.3.2.3.5 Archiving Checklists Headers and Items

You can use the archiving objects *Checklist Headers* (/CPD/MC_H) and *Checklist Items* (/CPD/MC_I) to archive checklist headers and items that are no longer needed. Archiving allows you to reduce the load on your database.

Structure

Tables

Tables for Checklist Headers

Table	Description
/BOBF/D_ATF_DO	Document node of attachment folder
/BOBF/D_ATF_RT	Root nodes of attachment folder
/BOBF/D_TXCCON	Text content
/BOBF/D_TXCROOT	Root node of text collection
/BOBF/D_TXCTXT	Text
/IAM/D_I_ATT	Attachment
/IAM/D_I_DATE	Date
/IAM/D_I_DESC	Description node
/IAM/D_I_DESC_TX	Language-dependent description text node
/IAM/D_I_OBJ_REF	Issue reference node
/IAM/D_I_OREF_DT	Language-dependent, reference, description text node
/IAM/D_I_PARTY	Party node
/IAM/D_I_QTY	Quantity
/IAM/D_I_ROOT	Root node

Tables for Checklist Items

Table	Description
/BOBF/D_ATF_DO	Document node of attachment folder
/BOBF/D_ATF_RT	Root nodes of attachment folder
/BOBF/D_TXCCON	Text content
/BOBF/D_TXCROOT	Root node of text collection
/BOBF/D_TXCTXT	Text
/IAM/D_ACT_ATT	Attachment
/IAM/D_ACT_DATE	Date
/IAM/D_ACT_DESC	Description node
/IAM/D_ACT_DTXT	Language-dependent description text node
/IAM/D_ACT_FOA	Follow-up action
/IAM/D_ACT_FOA_P	Follow-up action parameter
/IAM/D_ACT_OBJ_RF	Object reference
/IAM/D_ACT_OREF_DT	Language-dependent description texts
/IAM/D_ACT_PARTY	Party
/IAM/D_ACT_QTY	Activity quantity

Programs

The following programs are available for /CPD/MC_H:

- Preprocessing: /CPD/ARCH_MC_HEADER_PRE
This program checks if an object is ready for archiving by verifying the following conditions:
 - The adherence to the specified residence time
 - The availability of activities for the object
 If the object is ready, this program sets the status as Archiving in Process (02) in the database. After the preprocessing program has run, the objects marked for archiving are no longer made available on the UI.
- Write: /CPD/ARCH_MC_HEADER_WRITE
This program checks if an object has the status Archiving in Process (02). If the status is 02, the program archives the object to the archive file.
- Delete: /CPD/ARCH_MC_HEADER_DELETE
This program verifies archived files against the data in the database; and deletes all objects in the database that have been successfully archived..

The following programs are available for /CPD/MC_I:

- Preprocessing: /CPD/ARCH_MC_ITEM_PRE

This program checks if an object is ready for archiving by verifying the adherence to the specified residence time. If the object is ready, this program sets the status as Archiving in Process (O2) in the database. After the preprocessing program has run, the objects marked for archiving are no longer made available on the UI.

- Write: /CPD/ARCH_MC_ITEM_WRITE
This program checks if an object has the status Archiving in Process (O2). If the status is O2, the program archives the object to the archive file.
- Delete: /CPD/ARCH_MC_IEM_DELETE
This program verifies archived files against the data in the database; and deletes all objects in the database that have been successfully archived.

Information Lifecycle Management (ILM)

Information Lifecycle Management (ILM) allows you to define rules for storing archived business data, set legal holds on stored data, and destroy the data in adherence to legal requirements.

The ILM objects CPD_MC_H and CPD_MC_I are available for checklist headers and items respectively, and these ILM objects allow you to model retention rules based on the following fields:

- Condition Field
 - APPLICATION
- Time Reference Fields
 - Last Changed On

i Note

The date of the last change of the checklist headers and items is considered in the time reference field.

i Note

When you create retention rules for a checklist item, ensure that the retention time specified does not exceed the retention time specified for the parent (checklist header).

You can use the transaction IRMPOL to define policies and rules for ILM.

Prerequisites

The prerequisites for *Retention Management* are:

- You have activated the business function ILM
- You have assigned the following objects to an audit area:
 - o CPD_MC_H
 - o CPD_MC_I

More Information

To change the residence time, you can make settings in Customizing for *Cross-Application Components* under [► Processes and Tools for Enterprise Applications](#) > [Reusable Objects and Functions for BOPF Environment](#) > [Archiving Adapter](#) > [Maintain BO-Specific Residence Periods](#) ►.

13.5.3.2.4 Deletion of Personal Data

The Commercial Project Management applications might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data.

Project Workspace

Relevant Application Objects and Available Deletion Function

Application	Detailed Description	Deletion Function
Project Workspace	Project Workspace stores personal information of business partners for the Team function.	The ILM-enabled deletion program for commercial projects: /CPD/PWS_ARCH_MP_DELETE

Relevant Function Modules

Application	Function Module	Description
▶ Project Workspace > Risk Management >	/CPD/BUPA_EOP_CHECK	You can use this API to check the retention period of business partners.
▶ Project Workspace > Risk Management >	/CPD/RM_BUPA_EVENT_ARCH1	You can use this API to archive business partners.
▶ Project Workspace > Risk Management >	/CPD/RM_BUPA_EVENT_DELETE1	You can use this API to delete business partners.
Project Workspace	/CPD/PWS_WS_BUPA_EOP_CHECK	You can use this function module for the end of purpose check.

Relevant Programs

Application	Program	Description
Project Workspace	/CPD/R_DPP_CONTACT_PERSON_S4H	<p>This program is relevant for contact persons who have been added using the <i>Create Contact</i> feature in the <i>Define Commercial Project Types</i> view in Customizing for ▶ Commercial Project Management > Master Data > Commercial Project > Make Settings for Commercial Projects >.</p> <p>When a contact person leaves a company, to comply with data privacy and protection rules, you can use this program to identify all the projects that this person is assigned to; and then</p>

Application	Program	Description
		proceed to delete the contact from all projects in one go.

Project Cost and Revenue Planning

The Project Cost and Revenue Planning application (CA-CPD-PP) does not use SAP ILM to support the deletion of personal data since the data required for transactional purposes is stored in a BW InfoCube.

Relevant Application Objects and Available Deletion Function

Application	Detailed Description	Deletion Function
Project Cost and Revenue Planning	Project Cost and Revenue Planning stores personal information of business partners only when resources are planned together with SAP Multiresource Scheduling (MRS). This information is then stored in a BW InfoCube, for real-time planning.	The deletion program /CPD/ PFP_EMP_DATA_CONSISTENCY checks the HR master and delete information from the InfoCube, for employee records that are not found in the HR master.

Project Issue and Change Management

Relevant Application Objects and Available Deletion Function

Application	Detailed Description	Deletion Function
Project Issue and Change Management	Project Issue and Change Management stores personal information of business partners for the Partner function.	<ul style="list-style-type: none"> The ILM-enabled deletion program for issues and change requests: /PICM/ ARCH_ISSUE_CR_ROOT_DEL The ILM-enabled deletion program for activities: /PICM/ ARCH_ACTIVITY_ROOT_DEL Function module to check (before deletion) if business partner is used in the application: /PICM/ BUPA_EVENT_DELE1

Relevant Function Modules

Application	Function Module	Description
Project Issue and Change Management	/PICM/BUPA_EOP_CHECK	You can use this function module for the end of purpose check.

13.5.3.2.5 Protection of Data Stored in BW InfoCube

Project Cost and Revenue Planning uses embedded BW technology and the BW InfoCube stores personal data of customers and employees.

The customer InfoObject (/CPD/CUSTOMER) is an attribute of the commercial project InfoObject (/CPD/MPID); and the commercial project is an attribute of the financial plan InfoObject (/CPD/FPOID). The master data of the customer InfoObject is updated from the transactional screens of Commercial Project Management. To address the exclusion of customers' personal data, which has been marked for End of Purpose (EoP), the HANA calculation view CV_CUSTOMER (package: sap.cpm4h.pfp) performs a join of the commercial project header and the customer master data table (KNA1) to ensure that masking is done using the CVP_XBLCK flag.

The master data of employees is used in the SAP BW InfoObject (/CPD/FPERID), from SAP HCM for SAP S/4HANA, using the HANA calculation view CV_EMPLOYEE. The business partner End of Purpose (EoP) is fetched from the CDS view I_EMPLOYEE to address the exclusion of employees' personal data that has been marked for End of Purpose. The system uses the BW InfoObject /CPD/EMP_ACTV to handle inactive employees so that they are not available with the financial planning application of Commercial Project Management.

You can use the report /CPD/PFP_PERSONAL_PROJECT_LIST to display to logged-in users the business objects (commercial projects and financial plans) where their individual personal data is used. The report allows employees to check usage of their own personal data across commercial projects.

For more information of the archiving concept and the objects that cover the erasure requirements of personal data, see the relevant chapters in Data Archiving.

i Note

You must configure the archiving concept and objects according to regional laws.

For more information, see Customizing for Commercial Project Management:

- [▶ Master Data ▶ Define End of Purpose for Personal Data ▶](#)
- [▶ Project Cost and Revenue Planning ▶ Information on Personal Data Protection ▶](#)
- [▶ Project Issue and Change Management ▶ Define End of Purpose for Personal Data ▶](#)

13.5.3.2.6 Logging of Changes

Commercial Project Management provides change logging to audit changes to key fields in the projects:

In Project Workspace, the system logs changes to certain information in master projects. Each log contains information such as the fields that were changed, the old and new values of the field, the user who changed the information, the type of change, and the time and date when the change was made.

You can now view change logs for the following:

- Master project header
- Contact person
- Risk
- Checklist activity

You can also control change logging using the Business Add-In BAdI: Control of Change Log Output. For more information, see Customizing for SAP Commercial Project Management --> Project Workspace --> Business Add-Ins.

Project Cost and Revenue Planning allows you to view the changes made in a financial plan. You can choose the Document History pushbutton, on the Financial Plan screen, to view this change log.

You can also control change logging using the Business Add-In BAdI: Control of Change Log Output. For more information, see Customizing for SAP Commercial Project Management --> Project Cost and Revenue Planning --> Business Add-Ins.

Project Issue and Change Management allows you to view the changes made in an issue or change request. You can choose the Document History pushbutton, on the Issue or Change Request screens, to view this change log.

You can also control change logging using the Business Add-In BAdI: Control of Change Log Output. For more information, see Customizing for SAP Commercial Project Management --> Project Issue and Change Management --> Business Add-Ins.

13.5.3.2.7 Security-Relevant Logging and Tracing

The Project Cost and Revenue Planning application of Commercial Project Management uses the tracing functions of SAP BusinessObjects Analysis for Microsoft Office (AO) to trace actions performed in the planning workbook (AO). You can also activate a trace file for Project Cost and Revenue Planning using the *Activate Tracing* button on the *Financial Planning* ribbon. Details of the items are recorded in the trace file (CACPDFP_TRACE_LOG.10g). Note that the file does not record user-specific personal information such as user name or IP address.

For information about tracing related to Analysis Office, see https://help.sap.com/viewer/p/SAP_BUSINESSOBJECTS_ANALYSIS_OFFICE ► *Installation, Configuration, Security and Administration* ► *Administrator Guide* ►.

13.5.3.2.8 Other Security-Relevant Information

Before you use the digitally-signed SAP BusinessObjects Analysis for Microsoft Office (AO) workbooks delivered by Commercial Project Management, you must follow these steps:

⚠ Caution

These settings are valid if you want to use the workbooks in a secure way by only enabling digitally-signed macros. However, if you use custom workbooks or make any changes and save it back to the standard, you must enable all macros.

1. Launch Microsoft Excel
 1. Go to ► *File* ► *Options* ► *Trust Center Settings* ► *Macro Settings* ►
 2. Choose *Disable all macros except digitally signed macros*
 3. Mark the *Trust access to the VBA project object model* checkbox
2. Launch the digitally-signed workbook and implement the following steps to add the certificate as a trusted publisher:
 1. A security warning is shown in ► *File* ► *Info* ► *Enable Control* ►
 2. Select *Advanced Options*
 3. In the next dialog box, select *Trust all documents from this publisher*

i Note

Adding the certificate is a one-time activity

3. Follow these steps to change the default system in the workbook:
 1. Go to ► [File](#) ► [Commercial Project](#) ► [Settings](#) ►
 2. In the dialog box, choose [Platform](#)
 3. Choose [Replace System](#)
 4. Choose your relevant system in the [Replace by System](#) column
 5. Save the workbook (with the correct standard workbook name) in the relevant system

13.5.3.3 SAP Portfolio and Project Management

13.5.3.3.1 Authorizations

Authorizations

In Project Management and Portfolio Management, authorizations are controlled in the following ways:

- ABAP authorization objects and roles
This is the standard method for controlling access to transactions and programs in an SAP ABAP system. Authorizations are combined in an authorization profile that is associated with a role. User administrators can then assign the corresponding roles via the user master record, so that the user can access the appropriate transactions for his or her tasks.
- Access control lists
These allow you to add another level of security by controlling authorization at object level. For example, you can control who has authorization to change a particular project definition. You can define the menu options in the navigation area using portal content adjustments or PFCG role Customizing.
- Roles for SAP Fiori apps
To use SAP Fiori Apps, users must be assigned to roles. These roles define which apps are displayed to the user.

In **Project Management only**, you can use the following additional authorization mechanisms:

- System administrators can grant access to objects by choosing ► [Portfolio and Project Administration](#) ► [Project Authorization Administration](#) ► in the application. This is an exception to the normal process and is only used if the administrator of the object is not available due to illness, for example. The system sends the “new” and “old” administrators an e-mail to inform them of the new authorization holder. For more information, see the [Granting Administration Authorization for an Object](#) section of the Configuration Guide for SAP Portfolio and Project Management.
- System administrators can assign PFCG roles in Customizing for SAP Portfolio and Project Management under ► [Common Functions](#) ► [Define Superuser Authorizations](#) ►. This ensures that the maintained PFCG roles with the selected authorization will be automatically assigned to the corresponding project definition.

Authorizations regarding BAPIs, reports, and (RFC-enabled) function modules:

In SAP Portfolio and Project Management, multiple BAPIs, reports and (RFC-enabled) function modules are available to create, read, change, edit, update, and delete the data of SAP Portfolio and Project Management.

Additionally, via (RFC-enabled) function modules and reports data is read from the SAP S/4HANA system. Therefore, using these BAPIs, reports, and function modules access to and manipulation of Portfolio and Project Management data as well as read access to SAP S/4HANA data is possible. Thus, the authorization for using these BAPIs, reports, and function modules (via transactions, for example), should be restricted to users who are intended to have these authorizations and the corresponding access to data.

Authorizations regarding search results

You can use the BAdI `BADI_DPR_SEARCH` to modify search results. You can filter the result set implementing this BAdI depending on the specified search helps which exist for each Portfolio and Project Management object. Thus, you can, for example, hide all results for which the user does not have read authorization from the result list. In the standard, these results are displayed in the result list, but the user cannot open or display these objects.

Use

SAP Portfolio and Project Management uses the authorization concept provided by ABAP Platform. Therefore, the recommendations and guidelines for authorizations as described in the Security Guide for ABAP Platform also apply to SAP Portfolio and Project Management.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF00`) on the AS ABAP.

You can maintain the following role authorizations in Project Management and Portfolio Management using the SAP Profile Generator.

The following `PF00` roles of SAP Portfolio and Project Management include authorizations to start the Web Dynpro ABAP applications (authorization check `S_START`) for Project Management and Portfolio Management:

- `SAP_CPR_USER`
- `SAP_XRPM_USER`

For details see the particular roles in transaction `PF00` and choose [▶ Authorizations ▶ Display Authorization Data ▶ Cross-application Authorization Objects ▶ Start Authorization Check for TADIR Objects ▶](#).

SAP recommends to adapt custom-specific roles accordingly.

Project Management Roles

The following single roles are delivered with Project Management:

Role	Authorization
<code>SAP_CPR_PROJECT_ADMINISTRATOR</code>	Create projects (project definitions).
<code>SAP_CPR_TEMPLATE_ADMINISTRATOR</code>	Create, change, read, and delete all templates in Project Management.

Role	Authorization
SAP_CPR_USER	Use Project Management, but no authorization to perform any activities in a particular project. To do this users need project-specific authorizations, which can be distributed either directly via ACLs or through their assignment to a role. This role must be included in every Project Management composite role.
SAP_CPR_BCV_USER	Project-Management-specific authorization for using BCV content in resource management.
SAP_BPR_PPM	SAP Portfolio and Project Management PFCG role for NW BC

The following composite roles are delivered with Project Management:

Role	Authorization
SAP_CPR_DECISION_MAKER	Decision maker in Project Management. Contains the role SAP_CPR_USER.
SAP_CPR_INTERESTED	Interested party in Project Management. Contains the role SAP_CPR_USER.
SAP_CPR_MEMBER	Team member in Project Management. Contains the role SAP_CPR_USER.
SAP_CPR_PROJECT_LEAD	Project manager in Project Management. Contains the role SAP_CPR_PROJECT_ADMINISTRATOR and SAP_CPR_USER
SAP_CPR_BCV_USER_COMP	Composite role containing the general role for using BCV (SAP_BCV_USER) and the Project Management specific role (SAP_CPR_BCV_USER).
SAP_CPR_TEMPLATE_RESPONSIBLE	Project Management template responsible. Contains the roles SAP_CPR_TEMPLATE_ADMINISTRATOR and SAP_CPR_USER
SAP_CPR_RESOURCE_MANAGER	Resource manager in Project Management. Contains the role SAP_CPR_USER.

You can use these SAP standard roles or create your own. For more information, see the [Activating Single Roles for Project Management](#) section and the [Creating Roles for the Project-Specific Authorization Checks](#) section of the Configuration Guide for SAP Portfolio and Project Management.

Portfolio Management Roles

For Portfolio Management, the following roles are available:

Roles	Authorization
SAP_XRPM_ADMINISTRATOR	Super user authorization in Portfolio Management. Used to create new portfolios. This role also provides the assigned user full access to all Portfolio Management business objects in the system.
SAP_XRPM_USER	General user in Portfolio Management. All users should be assigned this role. Has general authorizations to use Portfolio Management, but no specific object access. This access must be assigned to the user via ACLs.
SAP_RPM_BCV_USER	Portfolio Management specific authorization for BCV content in Portfolio Management
SAP_RPM_BCV_USER_COMP	Composite role containing the general role for using BCV (SAP_BCV_USER) and the Portfolio Management specific role (SAP_RPM_BCV_USER).
SAP_BPR_PPM	PFCG role for NWBC in SAP Portfolio and Project Management

You can use these SAP standard roles or create your own. For more information about roles in Portfolio Management, see the [Activating Single Roles for Portfolio Management \(PFCG\)](#) section and the [Creating Roles for the Portfolio-Specific Authorization Checks](#) section of the Configuration Guide for SAP Portfolio and Project Management.

SAP Fiori Roles

SAP Fiori roles (SAP_BR_*) need to be assigned on the front-end server on which the UIS4HOP1 software component is installed. You can find the roles in the implementation information for each application.

For more information and further implementation tasks on the front-end server,

In the back-end, you have to create roles in transaction PFCG and assign business catalogs to the roles. For more information, go to https://help.sap.com/s4hana_op_2020, enter *SAP Fiori Overview* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

13.5.3.3.2 Communication Channel Security

SAP Portfolio and Project Management Communication Channel Security

Communication Channel	Communication Technology	Data Transferred	Comment/Security Recommendation
SAP Portfolio and Project Management front-end (browser) to the Application Server ABAP (AS ABAP)	HTTP(S)	Files, metadata, and user data (passwords, user names)	
Project Management front-end (browser) to content or cache servers	HTTP(S)	Files	
Application Server ABAP to content or cache servers	HTTP(S)	Metadata, files	
Application Server ABAP to other application servers (for example, HR, CO)	RFC	Metadata, files	<p>SAP Portfolio and Project Management communicates with 3rd party or SAP S/4HANA systems to obtain or create information on object links between SAP Portfolio and Project Management and objects located in the 3rd party/SAP system. The communication to 3rd party systems has to be implemented at the customer site. The 3rd party/SAP system never calls back.</p> <p>For more information, see the Setting Up Object Links section of the Configuration Guide for SAP Portfolio and Project Management.</p>
SAP Portfolio and Project Management to Project System (PS) component on a separate system	RFC	Files, metadata	
SAP Portfolio and Project Management to SAP HCM on a separate system	SAP ALE RFC	Files, metadata	

i Note

In SAP Portfolio and Project Management, there is no fixed port for communication and the firewall settings described in the Application Server ABAP Security Guide.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for the Change and Transport System* into the search bar, press , and open the search result with that title.

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

→ Recommendation

We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *ABAP Platform Security Guide* into the search bar, press , open the search result with that title, and navigate to ► [Network and Communication Security](#) ► [Transport Layer Security](#) ►.

13.5.3.3.3 Network Security

SAP supports the installation of SAP Portfolio and Project Management within the intranet (for internal collaboration only).

Installation Scenarios

Scenarios A and B can be used for SAP Portfolio and Project Management:

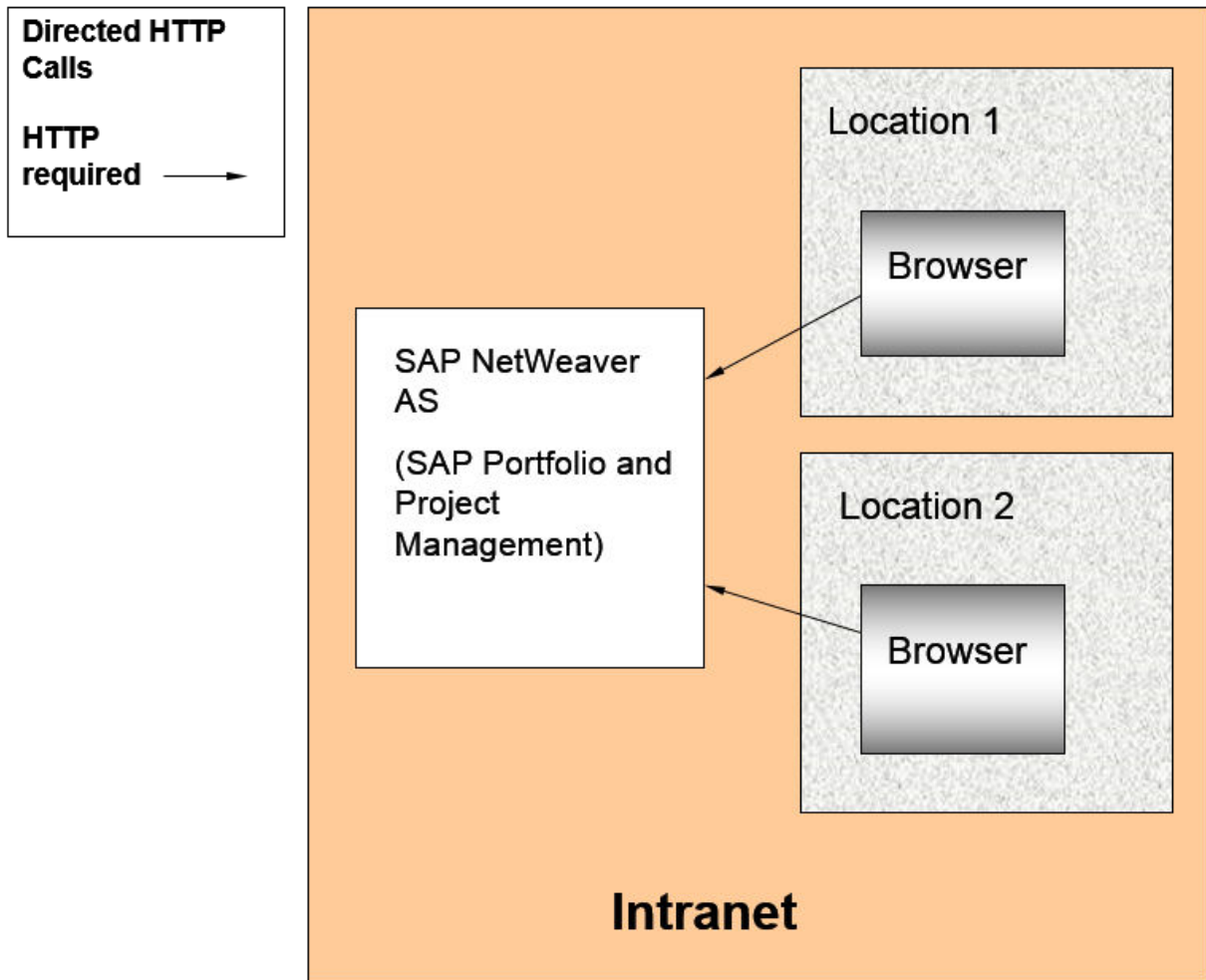
- Scenario A: **No content server**
- Scenario B: **One hidden content server**

Installation scenario B, with one hidden content server, is the installation scenario with the highest level of security.

Scenario A: No Content Server

In scenario A, the complete installation consists only of SAP Portfolio and Project Management server (AS ABAP).

The server is located in the intranet.

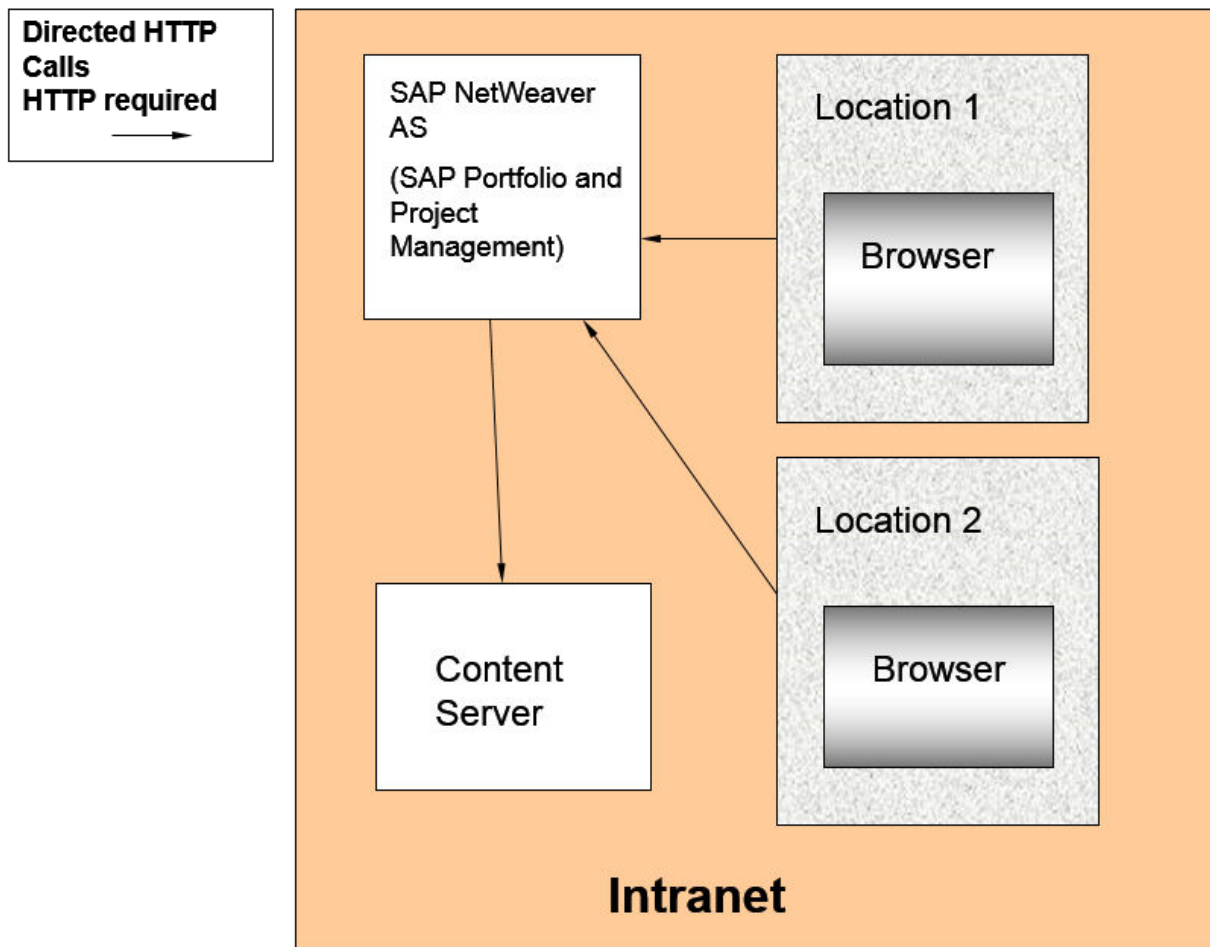


Scenario A: No Content Server

Scenario B: One Hidden Content Server

In the second type of installation, one content server is added to the network environment.

For SAP Portfolio and Project Management, the AS ABAP and the content server are both located in the intranet.



Scenario B: One Hidden Content Server

13.5.3.3.4 Communication Destinations

For the default SAP Portfolio and Project Management scenarios, no RFC destination pointing to external systems is required. However, if you are using the Project Management application programming interfaces (APIs) via the SOAP wrapper, the APIs consist of RFC function modules.

SAP Portfolio and Project Management

- FI/CO integration / Accounting Integration
- Adobe Document Services (ADS)
- Object links to e.g. SAP R/3, SAP ERP
- HR integration

In the following areas, Portfolio Management RFCs are called from an external application:

- Project integration

The Project Management APIs are required for:

- Portfolio Management Integration
- If a user needs to use the APIs they must have the basic RFC authorization for the relevant API function modules. The SOAP wrapper adheres to the authorization rules that apply if the RFC module is called directly. The function group name for Project Management is `CPR_API`.

To view the application-specific and basis authorization objects used in SAP Portfolio and Project Management, see [Authorizations \[page 547\]](#).

For more information about authorization objects and roles, go to https://help.sap.com/s4hana_op_2020, enter *AS ABAP Authorization Concept* into the search bar, press , and open the search result with that title.

13.5.3.3.5 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For more information about the services that are needed for SAP Portfolio and Project Management, see the [Activating Services](#) section of the Configuration Guide for SAP Portfolio and Project Management.

Use the transaction `SICF` to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Activating and Deactivating ICF Services* into the search bar, press , and open the search result with that title.

For more information about ICF security, go to https://help.sap.com/s4hana_op_2020, enter *RFC/ICF Security Guide* into the search bar, press , and open the search result with that title.

13.5.3.3.6 Data Storage Security

Data Storage

i Note

In the default setting for SAP Portfolio and Project Management, data is protected using the ACL concept already described in [Authorizations \[page 547\]](#). A Web browser is required for both scenarios. However, no cookies are used to store data on the front end.

Data Protection





In SAP Portfolio and Project Management, data is mainly stored on the Application Server ABAP (AS ABAP) database. An exception to this is when files are checked out for editing. In this case, files are stored locally on the user's hard drive and it is their responsibility to protect the files according to company security policy.

Depending on which installation scenario you have chosen for SAP Portfolio and Project Management, files might also be stored on content servers. For information about security measures to be taken in this case, see the [Network Security](#) chapter of this document.

For more information about data protection, see the [Data Protection](#) chapter of this document.

13.5.3.3.7 Deletion of Personal Data

Use

SAP Portfolio and Project Management might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at <http://help.sap.com/s4hana>  [Product Assistance](#)  [Cross Components](#)  [Data Protection](#) .

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Portfolio Management	For more information, see the Product Assistance documentation for SAP Portfolio and Project Management under Data Archiving in SAP Portfolio and Project Management .	Archiving Objects: <ul style="list-style-type: none"> • RPM_PORT (Portfolios) • RPM_BUCKET (Buckets) • RPM_ITEM (Items) • RPM_COLL (Collections) • RPM_INIT (Initiatives) • RPM_REVW (Reviews)
Project Management		Archiving Objects: <ul style="list-style-type: none"> • CDOCS_CONT (Documents) • CPROJECTS (Projects)
Portfolio and Project Management	Once a business partner is destructed using the central Business Partner application, all references of this particular business partner to objects in Portfolio Management and Project Management must be removed. Run the corresponding deletion program on a regular basis.	Deletion program PPM_DPP_DELETE

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented solution (EoP or WUC)	Further Information
Portfolio and Project Management	EoP	For more information, see the Product Assistance documentation for SAP Portfolio and Project Management under Blocking of Personal Data in SAP Portfolio and Project Management .

13.5.3.3.8 Security for Additional Applications

You can only (import or) export data to Microsoft Project if you have the required authorizations, see [Access Control Lists – Import and Export](#). The protection of this downloaded data is not part of the Project Management security model. When the user saves the project to his or her hard drive, the system does not perform an authorization check if somebody else opens the project again in Microsoft Project.

13.5.3.3.9 Other Security-Relevant Information

Import from Microsoft Excel

You can import projects from a Microsoft Excel file to Project Management. This enables you to transfer mass data in a quick and easy manner.

If you want to restrict the import function, you have to make sure that only allowed users receive authorization for transaction `DPR_DX_PROJECT` and report `DPR_DX_PROJECT`.

Moreover, you can import financial and/or capacity data from a Microsoft Excel file to financial and capacity planning in Portfolio Management. To use this function, you require an ERP system, an appropriate client, user, and password. This import is only allowed if the required authorization has been granted.

13.5.3.3.10 Security-Relevant Logging and Tracing

Floorplan Manager Message Logging to the Application Log

The Web Dynpro ABAP UI of SAP Portfolio and Project Management uses the Floor Plan Manager (FPM). The FPM Message Manager has a connection to the ABAP application log and offers the option to write error messages occurring in the FPM Message Manager also to the application log in the backend. To activate this feature, go to transaction `SAAB` and activate the check point group `FPM_RUNTIME_MESSAGES` for your user or for all users in the server.

For more information about FPM, see <http://www.sdn.sap.com/irj/sdn/nw-ui> under **Custom UI Development** > **Web Dynpro ABAP** > **Floorplan Manager (FPM)** > **Developer's Guide**.

For more information about security in the ABAP area, see

- Go to https://help.sap.com/s4hana_op_2020, enter *Application Server ABAP Security Guide* into the search bar, press , and open the search result with that title.
- Go to https://help.sap.com/s4hana_op_2020, enter *Security Guide: Web Dynpro for ABAP* into the search bar, press , and open the search result with that title.

Reports Logging to the Application Log

SAP Portfolio and Project Management logs application errors for background reports to transaction `SLG1`. Background reports are executed in the areas of financial integration, migration, import from Microsoft Excel, versioning, and replace user and resource. You can display these application logs via the objects `RPM_DOCUMENT`, `RPM_DX`, `RPM_INTEGRATION`, `RPM_MIGRATION`, `RPM_PLANNING`, `RPM_UC`, `RPM_VERSIONING`, `DPR_DX`, `DPR_REPLACE_USER_BP`.

Logon Attempts

For more information about logon attempts, go to https://help.sap.com/s4hana_op_2020, enter *The Security Audit Log* into the search bar, press , and open the search result with that title.

Change Document

You can use change document to track changes of objects of Project Management and Portfolio Management. If the function is active, the system also records changes to dependent objects. You can activate the change document function for the following objects:

- **Project Management**
 - Checklist templates
 - Project templates
 - Projects

You can activate this function in Customizing for *Project Management* under **Basic Settings** > **Activate Change Documents**.

If the function is active for one of these main objects, changes to dependent objects are also recorded. For example, if you select the indicator for the object category project, the system records all changes to the project as well as to the following objects:

- Project definitions
- Phases
- Tasks
- Mirrored tasks

- Checklists
- Checklist items
- Documents
- Object links
- Entity links
- Business partner favorites
- Business partner links
- Roles
- Approvals
- Qualifications
- Collaborations
- Templates

The system only records changes to database table `DPR_DOCUMENT`. This table contains unusable document attributes only.

The important attributes of the documents and files (such as name, location, and size) as well as the file content are saved to the KPro storage system without the support of a change document function.

Project Management supports versioning for files instead of the change document function. To track the changes, the user must always create a new document version. However, if he or she always overwrites the existing version, it is not possible to track the changes.

Project Management supports evaluations for the following objects:

- Project definitions
- Phases
- Tasks
- Mirrored tasks
- Checklists
- Checklist items
- Object links
- Entity links
- Business partner links
- Roles
- **Portfolio Management**
 - Portfolio
 - Bucket
 - Initiative
 - Item
 - Decision point
 - Review
 - Collection
 - What-if scenario
 - Relational associations of business objects
 - Financial and capacity category for bucket and item

In the standard system, this function is not activated.

You can activate this function in Customizing for *Portfolio Management* under ► *Global Customizing* ► *Process and Service Settings* ► *Activate Change Document* ►.

The system does not record changes to the following objects:

- **Project Management**
 - Documents
- **Portfolio Management**
 - Long texts
 - Comments/notes
 - Documents
 - Financial and capacity planning values

For more information:

- Go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press , open the search result with that title, and navigate to *Auditing and Logging*.
- Go to https://help.sap.com/s4hana_op_2020, enter *SAP NetWeaver Application Server for Java Security Guide* into the search bar, press , open the search result with that title, and navigate to *Tracing and Logging*.

13.5.4 Integrated Product Development for Discrete Industries

13.5.4.1 Classification Reuse UI Component

13.5.4.1.1 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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 given system landscape and the applicable legal requirements.

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.

Glossary

Term	Definition
Personal Data	Information about an identified or identifiable natural person.
Business 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	Deletion of personal data so that the data is no longer usable.
Retention period	The time period during which data must be available.
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

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

- **Access control:** Authentication features as described in section User Administration and Authentication.
- **Authorizations:** Authorization concept as described in section Authorizations.
- **Read access logging:** as described in section Read Access Logging.
- **Communication Security:** as described in section Network and Communication Security.
- **Availability control** as described in:
 - Section Data Storage Security
 - SAP NetWeaver Database Administration documentation
 - Go to https://help.sap.com/s4hana_op_2020, enter *SAP Business Continuity* into the search bar, press , and open the search result with that title.
- **Separation by purpose:** Is subject to the organizational model implemented and must be applied as part of the authorization concept

i Note

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped in Customizing for Cross-Application Components under Data Protection.

Additional industry-specific, scenario-specific or application-specific configuration might be required. For information about the application-specific configuration, see the application-specific Customizing in SPRO.

13.5.4.1.1.1 Data Privacy

The Classification Reuse UI Component must not process any sensitive personal data that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

Data Archiving and Deletion

Classification and characteristic data is dependent on the business object of the embedding application. You can only archive or delete classification and characteristic data with the business object of the embedding application, once the business object reaches its end of purpose. The embedding application is responsible for applying data protection and privacy rules.

Characteristics Containing Sensitive Personal Data

Characteristics are not intended for storing any sensitive personal data.

13.5.4.2 Advanced Variant Configuration

13.5.4.2.1 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific

legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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 given system landscape and the applicable legal requirements.

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.

Glossary

Term	Definition
Personal Data	Information about an identified or identifiable natural person.
Business 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	Deletion of personal data so that the data is no longer usable.
Retention period	The time period during which data must be available.
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

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

- **Access control:** Authentication features as described in section User Administration and Authentication.
- **Authorizations:** Authorization concept as described in section Authorizations.
- **Read access logging:** as described in section Read Access Logging.
- **Communication Security:** as described in section Network and Communication Security.

- **Availability control** as described in:
 - Section Data Storage Security
 - SAP NetWeaver Database Administration documentation
 - Go to https://help.sap.com/s4hana_op_2020, enter *SAP Business Continuity* into the search bar, press `[Enter]`, and open the search result with that title.
- **Separation by purpose:** Is subject to the organizational model implemented and must be applied as part of the authorization concept

i Note

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped in Customizing for Cross-Application Components under Data Protection.

Additional industry-specific, scenario-specific or application-specific configuration might be required. For information about the application-specific configuration, see the application-specific Customizing in SPRO.

13.5.4.2.1.1 Data Privacy

The Advanced Variant Configuration UI must not process any sensitive personal data that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

Data Archiving and Deletion

Characteristic data is dependent on the business object of the embedding application. You can only archive or delete characteristic data with the business object of the embedding application, once the business object reaches its end of purpose. The embedding application is responsible for applying data protection and privacy rules.

Characteristics Containing Sensitive Personal Data

Characteristics are not intended for storing any sensitive personal data.


13.5.4.3 Logging Changes

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to track the changes that have been made to this data. When these changes are logged,

you should be able to check which employee made which changes, the date and time, the previous value, and the current value.


It is also possible to analyze errors in this way.

See Also

- Go to https://help.sap.com/s4hana_op_2020, enter *Services for Application Developers* into the search bar, press `Enter`, open the search result with that title, and navigate to *Change Documents* .
- Go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press `Enter`, open the search result with that title, and navigate to *Auditing and Logging*.
- See [2125662](#)  for more information about superfluous data change logging defined for database tables.



13.5.4.3.1 Change Documents in Classification

Setting Up Change Documents for Classification

You can set up change documents for classification data by setting the *Change Docs* indicator for a class type in Customizing under [Cross-Application Components](#) > [Classification System](#) > [Classes](#) > [Maintain Object Types and Class Types](#) .

You can only set change documents if multiple objects are allowed to be classified in classes of the selected class type. When you first create a class type, you can set this parameter in Customizing manually. Once a class type has classified objects, you can only set this indicator by running report program RCCLUKA2, and you can only delete this indicator by running report program RMCLINOB.

More Information

- For more information on classification change documents, see [65124](#) .
- See [2125662](#)  for more information about superfluous data change logging defined for database tables.

13.5.4.4 Bill of Material

Standard Roles

Role	Description
SAP_BR_BOM_ENGINEER	You need this role to use the <i>Maintain Bill Of Material</i> and <i>Material where used list in BOMs</i> apps.

Standard Authorization Objects

Authorization Objects	Description
C_STUE_WRK	Authorization for CS BOM Plant (Plant Assignments)
C_STUE_BER	Authorization for CS BOM Authorizations

13.5.5 Product Lifecycle Management

13.5.5.1 Maintenance, Repair, and Overhaul

13.5.5.1.1 Authorizations (Specification 2000)

Specification 2000 (IS-ADEC-SPC) uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used:

Authorization Object	Description
C_ADSPCIP	Spec2000: Authorization object

13.5.5.1.2 Deletion of Personal Data (Specification 2000)

Use

Specification 2000 (IS-ADEC-SPC) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Specification 2000 (IS-ADEC-SPC)	Archiving Object ADS2KIP_AR ILM Object ADS2KIP_AR Report AD_SCIP_ILM_DEL_01

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Specification 2000 (IS-ADEC-SPC)	EoP	Checks tables EDP21, EDP13

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components*→*Data Protection*.

13.5.5.1.3 Deletion of Personal Data (Spare Parts Stock Calculation)

Use

Spare Parts Stock Calculation (IS-ADEC-SPSC) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Spare Parts Stock Calculation (IS-ADEC-SPSC)	Report AD_SPSC_ILM_DEL_01

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components*→*Data Protection*.

13.5.5.1.4 Authorizations (Manufacturer Part Number)

Manufacturer Part Number (MPN) uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used:

Authorization Object	Description
M_PIC_RIC	Authorization for MPN Restricted Interchangeability
ADPIC_RIC	Authorization object for MPN Restricted Interchangeability
M_PIC_EXCH	Authorization for material exchange

13.5.5.1.5 Deletion of Personal Data (MPN)

Use

Manufacturer Part Number (IS-ADEC-MPN) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Manufacturer Part Number (IS-ADEC-MPN)	EoP	Checks table MARA-MFRPN

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* → *Data Protection*.

13.5.5.1.6 Deletion of Personal Data (Sharing of Spare Parts and Customer Stock)

Sharing of Spare Parts and Customer Stock (IS-AD-SSP) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Customer Stock (IS-AD-SSP)	<p>Destruction Object</p> <p>MM_STO_SOBES_DEST</p> <p>ILM Object</p> <p>MM_STO_SOBES</p> <p>Report</p> <p>MM_STO_SOBES_DES</p>

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Customer Stock (IS-AD-SSP)	EoP check	Checks tables MSCD_MD, MCSS_MD, MSCD_MD, MSCS_MD

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for [Cross-Application Components→Data Protection](#).

13.5.5.1.7 Deletion of Personal Data (Subcontracting for MRO Processes)

[Subcontracting for MRO Processes](#) ((IS-AD-SUC) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Subcontracting for MRO Processes (IS-AD-SUC) - Special Stocks	<p>Destruction Object</p> <p>MM_STO_SOBES_DEST</p> <p>ILM Object</p> <p>MM_STO_SOBES</p> <p>Report</p> <p>MM_STO_SOBES_DES</p>

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Subcontracting for MRO Processes (IS-AD-SUC) - Special Stock	EoP check	Checks tables MSFS_MD, MSFD_MD, MSIS_MD, MSID_MD, MSRS_MD, MSRD_MD

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components*→*Data Protection*.

13.5.5.2 Attachment Service

Roles and Authorizations

For information on roles and authorizations for Attachment Service, goto https://help.sap.com/viewer/p/SAP_S4HANA_ON-PREMISE, and see under ► *Product Assistance* ► *Enterprise Business Applications* ► *R&D / Engineering* ► *Product Lifecycle Management (PLM)* ► *Attachment Service* ► *Technical Information for Consuming Application* ► *Roles and Authorizations* ►.

13.5.5.2.1 Deletion of Personal Data

End of Purpose Check

Consuming applications must adapt the BAdI `BADI_CV_ODATA_ATTACHMENTS_AUTH` to block the display or change of attachments once a business object has reached its end of purpose. The corresponding method in the BAdI is `CHECK_AUTHORIZATION`.

Moreover, to block access to the attachments with the Document Info Record (DIR) in Document Management, you must implement the BAdI `DOCUMENT_FILES01`, and its method `BEFORE_START_APPL`.

13.5.5.2.2 Read Access Logging

In Read Access Logging (RAL), you can configure which read-access information to log, and under what conditions.

To create the configurations for RAL, perform the steps as mentioned in the topic [► Data Protection and Privacy](#) > [Read Access Logging](#) in the current documentation guide. Also refer to the *Read Access Logging (RAL) and OData* information under the [More Information](#) section in the same topic.

Use the details mentioned in the following table when creating the RAL configurations:

Channel	OData Service / Application	Search Criteria	Fields to be Logged	Fields for Conditions	Business Context
SAP Gateway	CL_ODATA_CV_ATTACHMENT_API	Service ID - API_CV_ATTACHMENT_SRV	<ul style="list-style-type: none"> Under Channel Fields, log field Request URL Under Channel Fields > Entity Types > AttachmentContent log fields ARCHIVEDOCUMENTID, ARCHIVELINKREPOSITORY, FILENAME, and LOGICALDOCUMENT 	<ul style="list-style-type: none"> Condition name - CONDITION_ATTACHMENTCONTENTSET Expression name - EXPRESSION_ATTACHMENTCONTENTSET Fields - Under Channel Fields > Fields for Conditions > Requested Entity Set, drag and drop field AttachmentContentSet Sign - Inclusive Option - Equals Low/High Value - X 	Access to attachments from applications using attachment services.

Channel	OData Service / Application	Search Criteria	Fields to be Logged	Fields for Conditions	Business Context
SAP Gateway	API_CV_ATTACHMENT_SRV	Service ID - CV_ATTACHMENT_SRV	<ul style="list-style-type: none"> Under Channel Fields, log field Request URL Under Channel Fields Entity Types OriginalContent log fields APPLICATION_ID, FILENAME, and FILE_ID Under Channel Fields Entity Types OriginalContentArchiveLink log fields ARCHIVEDOCUMENTID and ARCHIVEREPOSITORYID 	<ul style="list-style-type: none"> Condition name - CONDITION_ORIGINALCONTENTSET Expression name - EXPRESSION_ORIGINALCONTENTSET <ul style="list-style-type: none"> Fields - Under Channel Fields Fields for Conditions Requested Entity Set drag and drop field OriginalContentSet Sign - Inclusive Option - Equals Low/High Value - X 	Access to attachments from applications using attachment service API.

Channel	OData Service / Application	Search Criteria	Fields to be Logged	Fields for Conditions	Business Context
KPro	Any access to attachment or files stored via KPro	PHIO Class - DMS_PCD1	<ul style="list-style-type: none"> Access Type PHIO Class PHIO ID 	Select the <i>Without Condition</i> checkbox in the log group attributes.	The KPro configuration logs any user accessing a DMS attachment.

i Note
For *Log Domain*, select **SAP / CUSTOMER**.

13.5.5.2.3 User Consent

The attachment service does not enforce user consent. The consuming application is responsible for enforcing user consent if required.

13.5.5.3 Document Management

For security-related information about Document Management, see the topics in this section.

13.5.5.3.1 Authorizations

The following authorization objects must be added to your respective business catalog role:

Authorization Object	Authorization Fields and Values	Remark
S_TCODE	TCD = CV01, CV02, CV03, CV01N, CV02N and CV03N	Add transactions to menu of roles, not to transaction SU22 data of services

Authorization Object	Authorization Fields and Values	Remark
C_DRAD_OBJ	DOKOB = <application specific values> STATUS = <application specific values> or "*" DOKAR = <application specific values>	Set object to "Yes, with Values" in transaction SU22 of the OData service (R3TR IWSV). Set DOKOB to the relevant values in SU22, but leave STAUS and DOKAR blank. Set STATUS and DOKAR in the business catalog roles only.
C_DRAW_DOK	DOKAR = <application specific values>	Set object to "Yes, without Values" in transaction SU22 of the OData service (R3TR IWSV). Set values in the business catalog roles only.
C_DRAW_TCD	DOKAR = <application specific values>	Set object to "Yes, without Values" in transaction SU22 of the OData service (R3TR IWSV). Set values in the business catalog roles only.
C_DRAW_TCS	STATUS = <application specific values> or "*" DOKAR = <application specific values>	Set object to "Yes, without Values" in transaction SU22 of the OData service (R3TR IWSV). Set values in the business catalog roles only.
C_DRAW_STA	STATUS = <application specific value> or "*" DOKAR = <application specific values>	Set object to "Yes, without Values" in transaction SU22 of the OData service (R3TR IWSV). Set values in the business catalog roles only.
DMS_DPP	ACTVT = <Change, Display or Execute>	Change and display of customizing transaction DMS_ACCESS. Execute is for running the deletion report.

For the above authorization objects, the Authorization field `ACTVT` could be assigned the value depending on the role created by the application.

13.5.5.3.2 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that Document Management (DMS) provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations regarding additional features that would be required in an environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

i Note

In most 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

13.5.5.3.2.1 Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped under customizing for *Cross-Application Components* under *Data Protection*.

Additional industry-specific, scenario-specific, or application-specific configurations might be required.

You can define or block access control to DIR data based on the personal data in the customizing *Maintain DIR Access Based on Personal Data* under ► *Cross-Application Components* ► *Document Management* ► *Control Data* ►. For more information, see the customizing documentation in the system.

13.5.5.3.2.2 Deletion of Personal Data

Document Management or CA-DMS might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in the SAP Note [1825544](#).

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. Document Management or CA-DMS uses SAP ILM to support the deletion of personal data as described in the following sections.

13.5.5.3.2.2.1 End of Purpose (EoP) Check

The End of Purpose check for a DIR (DRAW) object cannot be ascertained as there is no specific flag, field, or status that indicates this.

13.5.5.3.2.2.2 Handling Blocked Personal Data for a Blocked Business Partner in Document Management Application

Let's consider a customer or vendor master that is directly associated with a document info record (DIR), and that object has been blocked. In this case, Document Management application provides a customizing, based on which the access to a DIR and sections of a DIR can be decided by the users.

You can define or block access control to DIR data based on the personal data in the customizing [Maintain DIR Access Based on Personal Data](#) under [Cross-Application Components > Document Management > Control Data](#). For more information, see the customizing documentation in the system. The authorization object DMS_DPP must be assigned to your role to perform this customizing. For more information, see [Authorizations \[page 576\]](#).

- **Blocking of DIR:** When a user tries to display a DIR that has a reference to a blocked customer or vendor, the application checks the customizing, and decides whether the DIR should be opened in display or change mode. If it is allowed, then the relevant rules for file access and classification apply. The navigation to the respective applications via double-click operation is also blocked. The user cannot attach (object link) the blocked customer or vendor object as the search help of these applications do not display the blocked objects.
- **Blocking of Files and Classification:** When a DIR is accessed, the files and classification details are not displayed if the associated customer or vendor is blocked.

The Document Management BAPI's (Business Application Programming Interface) that are used to create, change, and display DIRs are adjusted to follow the customizing with respect to personal data. ALE scenarios are also considered here.

13.5.5.3.2.2.3 Handling Deleted Business Partner

For a DIR, it is not possible to determine the End of Business, and the End of Purpose of the associated customer or vendor. Hence, it is possible that the customer or vendor associated with a DIR can be blocked and later destroyed.

If the linked customer or vendor object is destroyed, the DMS application provides a deletion report that displays the usage of destroyed customers or vendors in the corresponding document info records. However, until the deletion report is run, the link is still displayed. For more information about the deletion report, see [Deletion Report \[page 580\]](#).

13.5.5.3.2.2.4 Deletion Report

The linked customer or vendor object may reach retention time and can be archived and destroyed. In this scenario, the document would still retain the link to this object, and while displaying this link, the link is masked.

The deletion report `DMS_BLOCKED_REF_DELETE` accepts document type and object type as mandatory inputs, and lists the documents that are associated with destroyed customer or vendor object. The user can choose the documents from the list, and delete the links for the same.

A new authorization object `DMS_DPP` is created to control the access to this report (same as the one for controlling access to customizing data).

13.5.5.3.2.2.5 Archiving or Destroying Business Data

The archiving and destruction of business data in Document Management takes place in accordance with the retention rules, and the option chosen while running the reports `DVSARCH1` and `DVSARCH2` respectively.


13.5.5.3.2.2.6 ILM Archiving for a DIR Including Files, Classification, and Object Links

Before archiving data, you must define the residence time, and retention periods in SAP Information Lifecycle Management (ILM).

You must decide whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.

You must do the following:

- Run transaction `IRMPOL` to maintain the required residence and retention policies for the document info record (ILM object: `CV_DVS`).
- For information about setting up the archiving object `CV_DVS`, go to https://help.sap.com/s4hana_op_2020, enter *Archiving Document Info Records (CA-DMS)* into the search bar, press , and open the search result with that title.

For information about how to configure blocking and deletion for Document Management, CA-DMS, refer to the customizing documentation for the following SPRO activity: [Cross-Application Components](#) > [Data Protection](#) > [Authorization Management](#) > [Business Partner: Blocking and Deletion](#) .

13.5.5.3.3 Read Access Logging

In Read Access Logging (RAL), you can configure which read-access information to log, and under which conditions.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Configuration	Logged for Service / Application	Fields Logged	Business Context
IDEA_DMS_PCD1_KPRO.xml	Any access to attachment or files stored via KPro	User Timestamp Access Type PHIO Class PHIO ID	The KPro configuration logs any user accessing a DMS attachment.

For more information about Read Access Logging, go to https://help.sap.com/viewer/p/SAP_S4HANA_CLOUD, and see under ► *Product Assistance* ► *Generic Information* ► *General Functions for the Key User* ► *Read Access Logging* ►.

13.5.6 Product Development for Discrete Industries

13.6 Sales

Standard Authorization Objects

The following table explains where you can find the standard authorization objects available for line of business *Sales* and related functionality (transaction *SU21*):

Class	Description
SD	<i>Sales and Distribution</i>
LE_T	<i>Logistics Execution - Transportation</i>
LE_V	<i>Logistics Execution - Shipping</i>
WG	For Global Trade Management (GTM): <i>Retailing</i> <ul style="list-style-type: none"> • <i>Trading Contract: Authorization for Organizational Data</i> (W_WBHK_ORG) • <i>Trading Contract: Authorization for Trading Contract Type</i> (W_WBHK_TCT)

13.6.1 Sales Force Support

13.6.1.1 Activity Management and Visit Planning

You can use Activity Management and Visit Planning to manage all activities undertaken by the employees of your company.

Activities such as interaction logs and appointments keep a record of any interaction that has taken place between your company and its customers. Tasks provide a way for your employees to manage their own workload and to record reminders.

User Management and Authentication

This application uses the user management and authentication mechanisms provided by the ABAP platform, in particular, the security features of the AS ABAP. For more information about the applicable security recommendations and guidelines for user administration and authentication, go to SAP Help Portal at <https://help.sap.com/s4hana>, choose the relevant release and search for *Application Server ABAP Security Guide*.

User Management

Tool	Description
User and role administration with AS ABAP: <i>User Maintenance</i> (SU01) transaction and the profile generator (PFPG) transaction	For more information about user and role administration, see and [page 10] Business Roles [page 598] .

User Types

You must create the following user:

User	Delivered?	Type	Default Password	Description
End user	No	Dialog user	No	Mandatory user who can access Activity Management applications and Customizing for Activity Management. Created by a system administrator.

Authorizations

Activity Management uses authorizations provided by the AS ABAP. For more information, go to SAP Help Portal at <https://help.sap.com/s4hana>, choose the relevant release and search for *Application Server ABAP Security Guide*.

The AS ABAP authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (PFCG) transaction on the AS ABAP.

The following table details the authorization objects for Activity Management:

Authorization Object	Field	Description
CRM_ORD_OP	PARTN_FCT (partner function) PARTN_FCTT (partner function category) ACTVT (Activity)	Own documents
CRM_ORD_LP	CHECK_LEV PR_TYPE ACTVT (Activity)	Visibility in the organizational model
CRM_ACT	ACTVT (Activity)	Authorization Object Order-Business Object Activity
CRM_ORD_PR	PR_Type (transaction type) ACTVT (Activity)	Business Transaction Type
CRM_ORD_OE	SALES_ORG (sales organization) SERVICE_OR (service organization) DIS_CHANNE (distribution channel) SALES_OFFI (sales office) SALES_GROU (sales group) ACTVT (activity)	Allowed organizational units
CRM_TXT_ID	TEXTOBJECT (texts: application object) TEXTID (text ID) ACTVT (Activity)	Display and edit texts
CRM_FLDCHK	ACTVT AUGRP (Authorization Group) LEVEL1 (Authorization Level)	Order Authorization Object-Field Check

Network and Communication Security

The network topology of this application is based on the ABAP platform. For information about the applicable security guidelines and recommendations, see the [Application Server ABAP Security Guide](#) and the section [Network and Communication Security \[page 19\]](#).

Communication Channel Security

For more information about communication channel security, see [Communication Channel Security \[page 19\]](#). The available communication paths, protocols used, and type of data transferred are listed in the following table:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive data such as customer data
Front-end client using a Web browser	HTTP/HTTPS	All application data	Passwords, all sensitive data such as customer data

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the above section [Communication Channel Security](#):

Destination	Delivered?	Type	User, Authorizations	Description
AS ABAP	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of AS ABAP. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No additional data storage security is required.

13.6.1.2 Opportunity and Pipeline Management

You can use Opportunity and Pipeline Management to control your presales process. It provides a framework for tracking the progress of sales projects from the very outset.

User Management and Authentication

This application uses the user management and authentication mechanisms provided by the ABAP platform, in particular, the security features of the AS ABAP. For more information about the applicable security recommendations and guidelines for user administration and authentication, go to SAP Help Portal at <https://help.sap.com/s4hana>, choose the relevant release and search for *Application Server ABAP Security Guide*.

User Management

Tool	Description
User and role administration with AS ABAP: <i>User Maintenance</i> (SU01) transaction and the profile generator (PF00) transaction	For more information about user and role administration, see User Administration and Authentication [page 10] and Business Roles [page 598] .

User Types

The following users must be created for Opportunity and Pipeline Management:

User	Delivered?	Type	Default Password	Description
End user	No	Dialog user	No	Mandatory user who can access the opportunity management application and Customizing for opportunity management. Created by a system administrator.

Authorizations

Opportunity and Pipeline Management uses authorizations provided by the AS ABAP. For more information, go to SAP Help Portal at <https://help.sap.com/s4hana>, choose the relevant release and search for *Application Server ABAP Security Guide*.

The AS ABAP authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (PF00) transaction on the AS ABAP.

The following table details the authorization objects for Opportunity and Pipeline Management:

Authorization Object	Field	Description
CRM_ORD_OP	PARTN_FCT (partner function) PARTN_FCTT (partner function category) ACTVT(Activity)	Own documents

Authorization Object	Field	Description
CRM_ORD_LP	CHECK_LEV	Visibility in the organizational model
	PR_TYPE	
	ACTVT (Activity)	
CRM OPP	ACTVT (Activity)	Authorization Object Order-Business Object Opportunity
CRM_ORD_PR	PR_Type (Transaction type)	Business Transaction Type
	ACTVT (Activity)	
CRM_ORD_OE	SALES_ORG (Sales organization)	Allowed organizational units
	SERVICE_OR (Service organization)	
	DIS_CHANNE (Distribution channel)	
	SALES_OFFI (Sales office)	
	SALES_GROU (Sales group)	
	ACTVT (Activity)	
CRM_TXT_ID	TEXTOBJECT (texts: application object)	Display and edit texts
	TEXTID (text ID)	
	ACTVT (Activity)	
CRM_FLCHK	ACTVT	Order Authorization Object-Field Check
	AUGRP (Authorization Group)	
	LEVEL1 (Authorization Level)	

Network and Communication Security

The network topology of this application is based on the ABAP platform. For information about the applicable security guidelines and recommendations, see the [Application Server ABAP Security Guide](#) and the section [Network and Communication Security \[page 19\]](#).

Communication Channel Security

For more information about communication channel security, see [Communication Channel Security \[page 19\]](#). The available communication paths, protocols used, and type of data transferred are listed in the following table:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive data such as customer data
Front-end client using a Web browser	HTTP/HTTPS	All application data	Passwords, all sensitive data such as customer data

Network Security

For more information about network security, see [Network and Communication Security \[page 19\]](#).

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the section above [Communication Channel Security](#):

Destination	Delivered?	Type	User, Authorizations	Description
AS ABAP	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of AS ABAP. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

13.6.1.3 Sales Documents

Sales Force Support provides a user interface to view and edit sales documents (such as sales orders or sales order quotations).

For this scenario, you require one of the following PFCG roles:

Role	Description
SAP_S4C_UIU_SLS_PRO	Sales Professional
SAP_S4C_UIU_SLS_EMP	Sales Employee

13.6.1.4 Deletion of Personal Data in Sales Force Support

Use

Business objects in *Sales Force Support* might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Service* ► *Basic Functions* ► *Information Lifecycle Management* ►.

Relevant Business Objects and Available Deletion Functionality

Business Objects	Provided Deletion Functionality
Activity	Archiving object CRM_ACT_ON
Lead	Archiving object CRM_LEAD
Opportunity	Archiving object CRM_OPPT

Relevant Business Objects and Available EoP Functionality

Business Objects	Implemented Solution (EoP or WUC)	Further Information
<i>Pre-Sales and Sales</i> (CRM-S4-SLS)	EoP check	This EoP check includes business in the areas of the following: <ul style="list-style-type: none">• Sales• Service• Billing• Pricing• Procurement• Logistics

More Information

- For more information about data protection, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Service* ► *Basic Functions* ► *Data Protection* ►.
- For more information about archiving business objects that belong to completed business processes, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Business Applications* ► *Service* ► *Basic Functions* ► *Data Archiving* ►.

13.6.2 Order and Contract Management

13.6.2.1 Deletion of Personal Data in Order and Contract Management

Use

Applications in the business area *Order and Contract Management* might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Sales documents	Archiving object SD_VBAK
Billing documents	Archiving object SD_VBRK
Self-billing	Archiving object SBWAP_TRN
Empties management: Archiving of monthly empties stock	Archiving object BEV1_EMBD
Empties management: Archiving of empties update	Archiving object BEV1_EMFD

Application	Provided Deletion Functionality
Agreements	Archiving object SD_AGREEM
Condition records	Archiving object SD_COND
Customer master data	Archiving object FI_ACCRECV
Deliveries	Archiving object RV_LIKP
Shipment documents	Archiving object SD_VTTK
Shipment cost documents	Archiving object SD_VFKK
Advanced Returns Management data	Archiving object MSR_TRC
Trading contracts	<ul style="list-style-type: none"> • Archiving object WB2 • Report WB2_UPDATE_EOP_FROM_ARCHIVE (transaction SE38)
Sales plans	Data destruction object SD_SALESPLAN_DESTRUCTION
Campaigns	Data destruction object SD_CAMPAGN_DESTRUCTION
Destroying material listing and exclusions	Data destruction object SD_MAT_LIST_EXCL_DESTRUCTION
Destroying material determinations	Data destruction object SD_MAT_DETERM_DESTRUCTION
Destroying free goods determinations	Data destruction object SD_FREE_GOODS_DESTRUCTION
Destroying product proposals	Report SD_PRODUCT_PROPOSAL_DES (transaction SE38)

Relevant Application Objects and Available EoP Functionality

Application	Implemented Solution (EoP or WUC)	Further Information
<ul style="list-style-type: none"> • Sales & Distribution (ERP_SD) 	EoP check	<p>This EoP check includes business in the areas of the following:</p> <ul style="list-style-type: none"> • Sales • Billing • Delivery

Application	Implemented Solution (EoP or WUC)	Further Information
<ul style="list-style-type: none"> <i>Empties Management in SD</i> (ERP_SD_BIL_EM) 	EoP check	<p>This EoP check includes business in the areas of the following:</p> <ul style="list-style-type: none"> Supplier Empties data from invoice receipt Customer Empties account for customers
<ul style="list-style-type: none"> <i>Global Trade Management Position Management</i> (LO_GT_PM) <i>Global Trade Management Trading Contract</i> (LO_GT_TC) <i>Global Trade Management Trading Expenses</i> (LO_GT_TE) <i>Global Trade Management TEW</i> (LO_GT_TEW) 	EoP check	<p>This EoP check includes business in <i>Global Trade Management</i> (LO-GT).</p>

More Information

- For information about deleting personal data related to the *Order-to-Cash Performance* app, see [Deletion of Personal Data in Process Observer \[page 739\]](#).
- For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under [▶ Product Assistance ▶ Enterprise Business Applications ▶ Sales ▶ Order and Contract Management ▶ Data Management in Order and Contract Management ▶](#).

13.6.2.2 Global Trade Management

13.6.2.2.1 Network and Communication Channel Security

The information below shows the communication channels used, the protocol used for the connection, and the type of data transferred.

Connection to a SAP FSCM System

For Global Trade Management, you have the option to use an external SAP FSCM system to create forward exchange transactions. If you install SAP FSCM on a separate system, you require an RFC connection. If you install SAP FSCM together with Global Trade Management on one system, no RFC connection is necessary.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP S/4HANA system - SAP FSCM system (Financial Supply Chain Management)	RFC	Application data	n/a

RFC connections can be protected using *Secure Network Communications (SNC)*. For more information about setting up the RFC connection, and the prerequisites (authorizations), see Customizing for SAP S/4HANA under [Logistics General > Global Trade Management > Currency Hedging > Maintain RFC Destination of CFM System](#).

Connection to an External Global Trade Services System

You can connect Global Trade Management to an external Global Trade Services (GTS) system in order to check whether the contract data for Global Trade Management adheres to the prevailing legal requirements (import/export controls, global trade data).

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP S/4HANA system – GTS system	RFC	Application data	n/a

All users in the SAP S/4HANA system can call the functions on the GTS server using an RFC entry. In this RFC entry, you specify a user that is used uniquely for communication with GTS. Assign this communication user to the following roles for SAP Compliance Management.

Roles for Compliance Management

Role	Description
/SAPSL/LEG_ARCH GTS	Archiving
/SAPSL/LEG_LCE_APP GTS	Legal Control Export: Specialist
/SAPSL/LEG_LCI_APP GTS	Legal Control Import: Specialist
/SAPSL/LEG_SPL_APP GTS	Sanctioned Party List: Specialist

Role	Description
/SAPSSL/LEG_SYS_COMM GTS	(Technical) System Communication

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

i Note

We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, see Transport Layer Security and Web Services Security in the ABAP Platform Security Guide.

13.7 Service

13.7.1 Master Data

13.7.1.1 Accounts and Contacts

Why Is Security Necessary?

Security within account, contact, and employee processing in the master data area is necessary because these areas access sensitive customer and personal data, such as private address data, payment cards, bank details, and so on. This data is accessed from one central point that is integrated into the different systems. Therefore, you should restrict access to this data.

User Administration and Authentication

User Management

System	User	Delivered?	Type	Default Password	Description
SAP S/4HANA Service	Personal user	No	Dialog user	No	User who can access service transactions. To be maintained by a system administrator.
SAP S/4HANA Service	Technical user	No	System user	No	User who can process background tasks. To be maintained by a system administrator.

User Management Tools

Tool	Description
User Maintenance (transaction SU01)	For more information, see User Administration and Authentication [page 10] .

User Types

The personal user type is used to create users such as the following:

- Dialog users
- Background users

You must create the following users:

- Individual users so that they can use the standard processes that are delivered
- Initial identification parameters, such as the password and certificate for the users

Authorizations

Account, contact, and employee processing uses the authorization technique provided by the ABAP platform. Therefore, the recommendations and guidelines for authorizations as described in the [ABAP Platform Security Guide](#) also apply to the application.

The authorization concept is based on the assignment of authorizations to users based on roles. For role administration, use the profile generator (transaction PFCG). For more information, see [Role Administration \[page 13\]](#).

For a description of the authorization procedure used in master data processing in SAP S/4HANA Service, see the component-specific sections of this security guide.

The following authorization objects and authorization fields are used for account, contact, and employee processing:

Standard Authorization Objects

Authorization Object	Authorization Fields
B_BUPA_FDG (Business Partner: Field Groups)	ACTVT FLDGR (Field group for authorization)
B_BUPA_GRP (Business Partner: Authorization Groups)	ACTVT BEGRU (Authorization group)
B_BUPA_RLT (Business Partner: BP Roles)	ACTVT RLTYP (BP role)
B_BUPR_BZT (Business Partner Relationships: Relationship Categories)	ACTVT RELTYP (Business partner relationship category)
B_CARD_SEC (Authorization Encryption Card Master)	ACTVT
B_CCARD (Payment Cards)	ACTVT
UIU_COMP (UIU: Component Access Authorization Check)	COMP_NAME (Component Name) COMP_WIN (Component window name) COMP_PLUG (Inbound plug)
CRM_BPROLE (Business Partner: BP Roles)	ACTVT BPROLE (BP role)
CRMS4_PBDL (Authorization Check for Product Bundle)	ACTVT MTART (Material type)
S_USER_GRP (User Master Maintenance: User Groups)	CLASS (User group in user master maintenance) ACTVT

Additional Authorization Checks

Enhanced authorization check capabilities related to the secured processing of sensitive data of accounts, contacts, and employees in SAP S/4HANA Service are provided by the [Authorization Checks](#) (BADI_CRM_BP_UIU_AUTHORITY) Business Add-In (BAI). For more information, see the BAI system documentation.

Network and Communication Security

The network topology for master data is based on the topology used by the ABAP platform. The security guidelines and recommendations described in the [ABAP Platform Security Guide](#) and the corresponding component-specific sections of this security guide also apply to master data in SAP S/4HANA Service.

For more information, see [Network and Communication Security \[page 19\]](#).

Communication Channel Security

The following communication channels are used:

- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to SAP S/4HANA Service server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive service data such as payment card information, customer data, and employee data
Front-end client using a Web browser to SAP S/4HANA Service server	HTTP/HTTPS	All application data	Passwords, all sensitive service data such as payment card information, customer data, and employee data

Data Storage Security

The data is stored in database tables owned by SAP S/4HANA and the ABAP platform. Depending on the user, rights such as read, write, change, and delete are required. There is no need for you to adopt any other dedicated measures for data storage security.

13.7.1.2 Organizational Management

Organizational Management in SAP S/4HANA Service is a flexible tool to display your company's task-related, functional organizational structure. When using the service solution, you can simply display the organizational units that are relevant for your processes.

Organizational Management uses the ABAP platform.

User Management and Authentication

Users

System	User	Delivered?	Type	Default Password
SAP S/4HANA Service	Normal user	No	Dialog user	Arbitrary

Authorization Objects

There are several authorization objects, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Authorization Object	Description
PLOG	Controls authorization check for personal development data

Network and Communication Security

The network topology for this application is based on the ABAP platform. For information about the applicable security guidelines and recommendations, see the [ABAP Platform Security Guide](#) and the section [Network and Communication Security \[page 19\]](#).

Communication Channel Security

For more information about communication channel security, see [Network and Communication Security \[page 19\]](#). The available communication paths, protocols used, and type of data transferred are listed in the following table:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive data such as customer data
Front-end client using a Web browser	HTTP/HTTPS	All application data	Passwords, all sensitive data such as customer data

Network Security

For more information about network security, see [Network and Communication Security \[page 19\]](#).

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the above section [Communication Channel Security](#):

Destination	Delivered?	Type	User, Authorizations	Description
ABAP Platform	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of ABAP platform. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No additional data storage security is required.

13.7.2 Business Roles

In SAP S/4HANA Service, you can define business roles so that they can do the following:

- Assign function profiles, including the navigation bar profile
- Deactivate work centers
- Make work-center group links visible in the menu and in work center pages
- Make direct group links visible in the menu
- Assign an appropriate authorization role using the profile generator (transaction `PFCCG`)

SAP S/4HANA Service comes with a set of pre-defined business roles. For information about using a pre-defined role or copying an existing role and adjusting it to your needs, see the Customizing for [Service](#) under [UI Framework > Business Roles > Overview](#).

If you want to create a business role from scratch, use the following activities in Customizing for [Service](#):

Setting	Path to Customizing Activity
Configuration key	UI Framework > Technical Role Definition > Define Role Configuration Key
Authorization role	UI Framework > Business Roles > Define Authorization Role
Business role	UI Framework > Business Roles > Define Business Role
Logical links, work-center link groups, direct link groups, and navigation bar profiles	UI Framework > Technical Role Definition > Define Navigation Bar Profile

13.7.3 Internet Communication Framework Security (ICF) in Service

Get information on the services required to use apps in Service.

WebClient UI Apps

To use apps based on the WebClient UI framework, you need to activate the services listed below.

If your deployment has WEBCUIF applications embedded in the SAP Fiori Launchpad (FLP Integrated Mode), activate the following services:

```
/default_host/sap/bc/bsp/sap/bsp_dlc_frmcp  
/default_host/sap/bc/bsp/sap/bsp_wd_base  
/default_host/sap/bc/bsp/sap/bspwd_basics  
/default_host/sap/bc/bsp/sap/crm_ui_frame  
/default_host/sap/bc/bsp/sap/crm_ui_start  
/default_host/sap/bc/bsp/sap/crm_ui_sysmsg  
/default_host/sap/bc/bsp/sap/crm_thtmlb_util  
/default_host/sap/bc/bsp/sap/thtmlb_styles  
/default_host/sap/bc/bsp/sap/thtmlb_scripts  
/default_host/sap/bc/bsp/sap/wcf_jquery  
/default_host/sap/webcuif/uif_callback  
/default_host/sap/webcuif/uif_export_tab
```

If your deployment has standalone WEBCUIF applications, in addition to the services for the embedded release, activate the following services:

```
/default_host/sap/bc/bsp/sap/crm_bsp_frame  
/default_host/sap/bc/bsp/sap/gsbirp  
/default_host/sap/bc/bsp/sap/crmcmp_hdr  
/default_host/sap/bc/bsp/sap/crmcmp_hdr_std  
/default_host/sap/bc/bsp/sap/uicmp_ltx  
/default_host/sap/bc/bsp/sap/ic_base  
/default_host/sap/webcuif/uif_feed  
/default_host/sap/webcuif/uif_flex_data  
/default_host/sap/webcuif/wcf_fct
```

In-House Repair

To use apps in in-house repair, activate the following services:

```
UI_MANAGEINHREPAIRS  
UI_PERFORMPRECHECKS
```

UI_PLANREPAIRS
 UI_PERFORMREPAIRS
 UI_PREPAREFORBILLG

Only activate those services that you need for the applications running in your system. Use the transaction `SICF` to activate these services.

If your firewall(s) use URL filtering, you need to adjust your firewall settings accordingly.

For general information, see [ICF Security \[page 21\]](#) in the *Introduction* section of this guide.

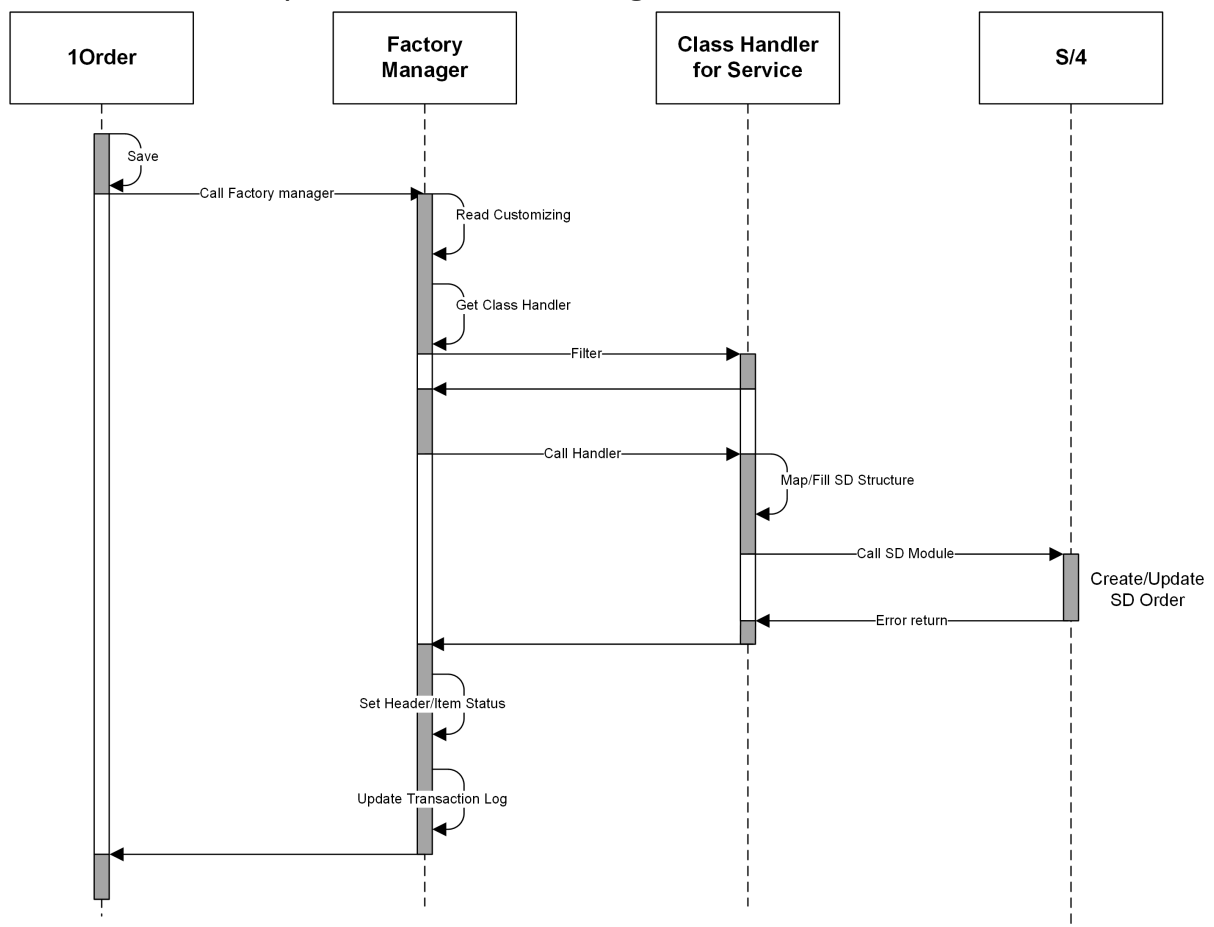
13.7.4 Service Processes

Service order processing in SAP S/4HANA Service enables you to process service requests, service order quotations, service orders, and service confirmations.

Security Aspects of Data Flow and Processes

The following figure shows the data flow in service order processing.

Overview of Process Steps for Service Order Processing



The following table shows the security aspects to be considered for the process step and what mechanism applies:

Step	Description	Security Measure
1	User creates order in SAP S/4HANA Service	<ul style="list-style-type: none"> User type: Dialog user with assignment to business role <code>SERVICEPRO</code> and corresponding PFCG role Communication protocol HTTP/HTTPS
2	User saves data in SAP S/4HANA Service	Not applicable
3	System creates or updates sales order in SAP S/4HANA Sales	Not applicable

Business Roles

Business Role	PFCG Role	Description
S4C_SRV_PRO	SAP_S4C_UIU_SRV_PRO	Service Professional
S4C_SRV_EMP	SAP_S4C_UIU_SRV_EMP	Service Employee

User Administration and Authentication

User Management

System	User	Delivered?	Type	Default Password	Description
SAP S/4HANA Service	Personal user	No	Dialog user	No	User who can access service transactions. Maintained by a system administrator.
SAP S/4HANA Service	Technical user	No	System user	No	User who can process background tasks. Maintained by a system administrator.

User Management Tools

Tool	Description
User Maintenance (SU01) transaction	For more information, see User Administration and Authentication [page 10] .

User Types

The personal user type is used to create users such as the following:

- Dialog users
- Background users

Customers must create the following users:

- Individual users to use with the standard processes that are delivered
- Initial identification parameters, such as the password and certificate for the users

i Note

SAP does not provide any default users.

Network and Communication Security

The network topology for master data is based on the topology used by the ABAP platform. The security guidelines and recommendations described in the [ABAP Platform Security Guide](#) and the corresponding component-specific sections of this security guide also apply to all service processes.

Communication Channel Security

The following communication channels are used:

- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to Fiori front-end	HTTP/HTTPS	URLs	Passwords, all sensitive data such as credit card information, customer data, and conditions
Front-end client using a Web browser	HTTP/HTTPS	All application data	Passwords, all sensitive data such as credit card information, customer data, and conditions

13.7.4.1 Service Core

Using the core service functions, you can process service order quotations, service orders, and service confirmations.

Business Roles

Depending on your requirements, you use either the *Service Professional* or the *Service Employee* business role for all core service transactions:

Business Role	PFCG Role	Description
S4C_SRV_PRO	SAP_S4C_UIU_SRV_PRO	<i>Service Professional</i>
S4C_SRV_EMP	SAP_S4C_UIU_SRV_EMP	<i>Service Employee</i>

Authorizations

SAP S/4HANA Service provides PFCG roles with authorization proposals for the above business roles.

13.7.4.2 Surveys

A survey is a type of questionnaire for gathering information from specific users.

Surveys are specialized forms that can be integrated into websites or sent as attachments in personalized e-mails to customers. The answers submitted are collected on a server and, depending on the business scenario, the results are either stored in a database or condensed beforehand. Later, the results are evaluated and can be used for making strategic decisions.

Surveys are an important means of gaining information from known and unknown users. For example, you could use a survey to gather feedback on customer satisfaction. The results collected from surveys can play an important role in making strategic business decisions, for example, when planning a new product launch or when making improvements for future products.

User Management and Authentication

Surveys use the user management provided by the ABAP platform and require dialog users.

Users

System	User	Delivered?	Type	Default Password
SAP S/4HANA Service	Normal user	No	Dialog user	Arbitrary

Authorization Objects

The following authorization object is used for survey processing:

Authorization Object	Authorization Field
CRM_SVY	ACTVT

Access checks are done based on PFCG roles. Currently, surveys are enabled in the Interaction Center for the *Service Professional* role.

Network and Communication Security

Communication Channel Security

Communication Path	Protocol Used	Type of Data Transferred
Internet	TCP/IP(SSL)	General data

For more information about communication channel security, see [Network and Communication Security \[page 19\]](#).

Network Security

For information about network security, see [Network and Communication Security \[page 19\]](#).

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the [Communication Channel Security](#) section above:

Destination	Delivered?	Type	User, Authorizations	Description
ABAP Platform	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of the ABAP platform. Depending on the user, no special data storage security measures are required. Surveys are a dependent application, so the leading application storage security applies to survey read or edit rights.

Checklist

Feature	Check	How to Check
View or maintain surveys	Does the PFCG role allow access to the survey application?	Role assignment
View or maintain surveys	Leading object checks for read or edit rights for surveys	Leading object (for example, an opportunity or lead)

13.7.4.3 Service Professional

Related Security Guides

Application	Guide
AS ABAP	Application Server ABAP Security Guide

Why Is Security Necessary?

Security is necessary to prevent attacks from the Internet and to protect data.

The Service Professional business role can perform functions such as broadcasting messages to agents or configuring alerts. For this reason, care must be taken that the Service Professional is assigned only to very specific persons. Otherwise, misleading information could be broadcast to agents, or critical information could be stolen.

User Administration and Authentication

User Management

User management for the Service Professional uses the mechanisms provided by the AS ABAP, for example, tools, user types, and password policies.

User Management Tools

Tool	Description
User Maintenance (SU01) transaction	N/A
Profile generator (PF0G) transaction	You use the profile generator to create roles and assign authorizations to users in ABAP-based systems.

No standard users are delivered.

You must create a user for SAP S/4HANA Service. If users want to access Service Professional functions, we recommend that the system administrator creates users and assigns them to `SAP_S4C_UIU_SRV_PRO` (for more information, see the [Authorizations](#) section below). All functions for the Service Professional are defined in this role.

Users

System	User	Delivered?	Type	Description
SAP S/4HANA Service	End user	No	Dialog	Created by an SAP system administrator

i Note

The default password for the SAP S/4HANA Service system is necessary when creating a new user in this systems. When you create new users with an initial password, we recommend that the new users log on to the backend system to change the initial password.

User Data Synchronization

All data is stored in SAP S/4HANA. There is no user data synchronization.

Integration with Single Sign-On Environments

The application accepts SAP logon tickets.

The application does not accept X.509 digital certificates.

Authorizations

The Service Professional uses the standard for authorizations provided by SAP S/4HANA Service.

The backend role `SAP_S4C_UIU_SRV_PRO` is delivered with the Service Professional.

The following table shows the security-relevant authorization objects used in the Service Professional scenario:

Standard Authorization Objects

Authorization Object	Field	Value	Description
CRM_BM	ACTVT: Activity	16	Only users with this authorization in their user profile can start the broadcast messaging server application.
CRM_ERMS_P	ACTVT	01, 02, 03, 43	This authorization object defines which rule policies the Service Professional is allowed to work with and what activities within them are permitted.
	ERMS_CTXT	Any context defined in Customizing (transaction CRMC_ERMS_REPOSITORY)	
	ERMS_AUGR	Any authorization group defined in Customizing (transaction CRMC_ERMS_REPOSITORY)	

Network and Communication Security

Communication Channel Security

The application runs in the web browser and it needs to communicate with the backend SAP S/4HANA server. An HTTP(S) communication channel is required for this.

- Broadcast messaging
 - HTTP(S) communication from browser to SAP S/4HANA server
 - HTTP(S) communication between SAP S/4HANA servers for sending messages to agents

Data Storage Security

No temporary data is stored. This is a web-based application.

Broadcast messaging uses cookies to store certain UI favorites on the client side. This data is retained until it is manually deleted. No sensitive data is stored in the cookie, so there are no specific measures to protect the cookie.

Checklist

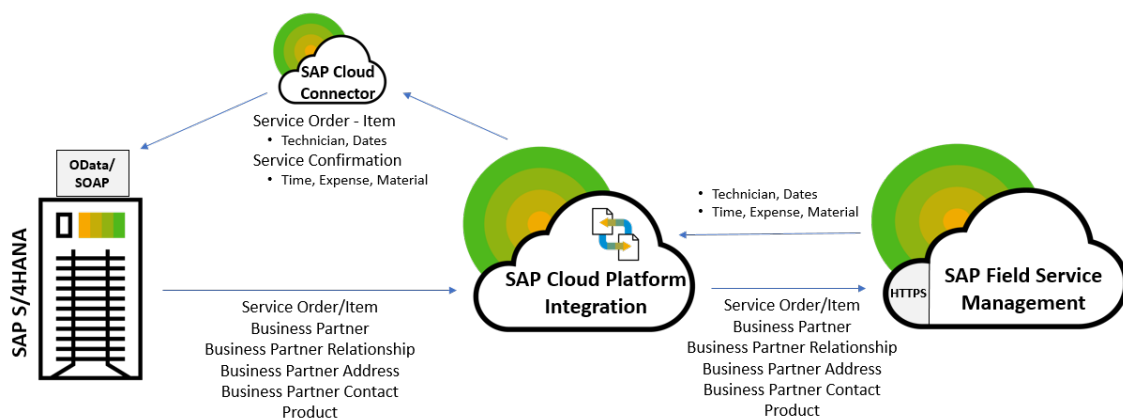
Feature	Check	How to Check
Broadcast messaging for supervisors	For authorization object CRM_BM, check that field ACTVT has a value of 16	In the profile generator (PFCG) transaction, enter role SAP_S4C_UIU_SRV_PRO or any role used to create supervisors, and choose <i>Display</i> . On the <i>Authorizations</i> tab, choose <i>Display Authorization Data</i> . Choose Utilities > Technical names on

13.7.5 Field Service Management Integration

SAP S/4HANA Service supports the integration with SAP Field Service Management.

SAP Field Service Management is integrated with SAP S/4HANA Service using SAP Cloud Platform Integration and SAP Cloud Connector. The following diagram provides an overview of the integration.

Overview of SAP Field Service Management Integration with SAP S/4HANA



For details on the installation and configuration steps, and security information, required for the integration of SAP Field Service Management, see the product assistance for SAP S/4HANA on SAP Help Portal at <http://help.sap.com/s4hana>. Search for *Integration with SAP Field Service Management*.

For more information about security and data protection in SAP Field Service Management, see the documentation for SAP Field Service Management on SAP Help Portal at http://help.sap.com/viewer/product/SAP_FIELD_SERVICE_MANAGEMENT. Search for *Security and Data Protection*.

For additional security information, see SAP Help Portal at <http://help.sap.com> and search for the following:

- *ABAP Platform Security Guide*
- *SAP Cloud Platform Connectivity (Cloud Connector Security)*
- *SAP Cloud Platform Integration Security Guide*

13.7.6 In-House Repair

In-House Repair supports companies that offer a repair and maintenance service performed in-house at repair centers. The in-house repair process consists of core activities such as prechecking, planning, repairing, and triggering billing for repair objects.

User Management

In-House Repair uses the user management of SAP NetWeaver AS and requires dialog users.

Users

System	User	Delivered?	Type	Default Password	Description
SAP Fiori front-end	Dialog user	No	Dialog user created in user maintenance (SU01) transactions	No	Used for Fiori applications

SAP Fiori Business Roles

The following business roles are used for the In-House Repair Fiori apps:

Business Role	System	Purpose
SAP_BR_CUST_SRVC_REP_REPA	Fiori front-end	Customer Service Representative - Manage In-House Repairs
SAP_BR_CUST_SRVC_MGR_REPA	Fiori front-end	Customer Service Manager - Plan In-House Repairs
SAP_BR_CUST_SRVC_TEC_REPA	Fiori front-end	Service Technician - Perform In-House Repairs

For information on creating back-end users for In-House Repair, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title.

Network and Communication Security

The network topology for master data is based on the topology used by the ABAP platform. The security guidelines and recommendations described in the [ABAP Platform Security Guide](#) and the corresponding component-specific sections of this security guide also apply to In-House Repair.

Communication Channel Security

The following communication channels are used:

- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the [Communication Channel Security](#) section above:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to Fiori front-end	HTTP/HTTPS	URLs	Passwords, all sensitive data such as credit card information, customer data, and conditions
Front-end client using a Web browser	HTTP/HTTPS	All application data	Passwords, all sensitive data such as credit card information, customer data, and conditions

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, no special data storage security measures are required. In-House Repair is a dependent application, so the leading application storage security applies to survey read or edit rights.

13.7.7 Interaction Center

Related Security Guides

Application	Guide
ABAP Platform	ABAP Platform Security Guide
Business Communication Broker (BCB)	ABAP Platform Security Guide
Interaction center manager (IC manager)	SAPS/4HANA Security Guide

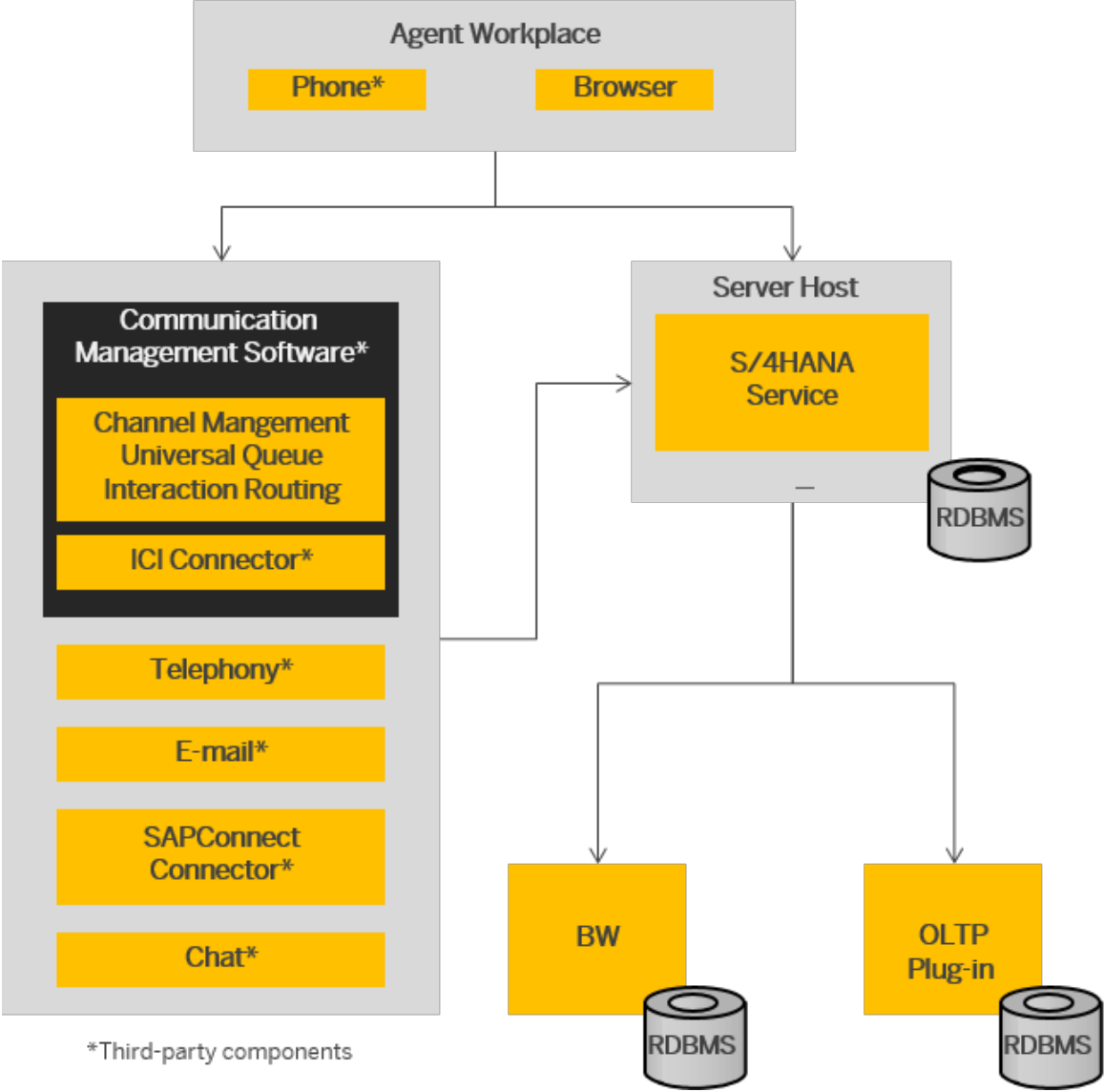
Why Is Security Necessary?

Security is necessary because:

- The Interaction Center WebClient (IC WebClient) synchronizes data from the communication management software. Such data could include personal data or restricted business data such as contract order data and must be protected.
- Interaction center agents (IC agents) can log on to SAP S/4HANA Service and access data such as customer master data. Such customer-sensitive data must be protected.

Technical System Landscape

The following figure illustrates the system landscape:



*Third-party components

Technical System Landscape

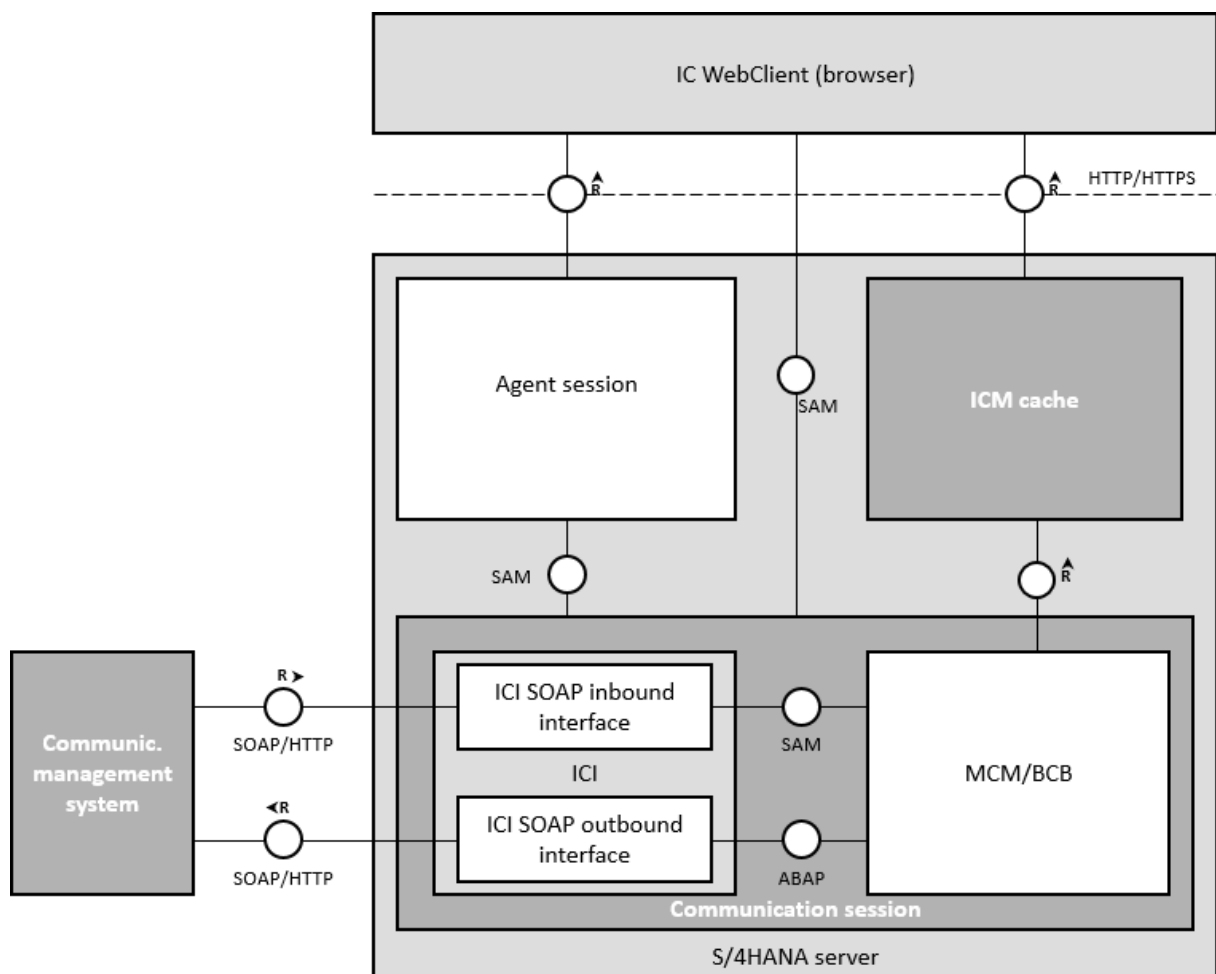
Abbreviation Key for Figure Above

Abbreviation	Description
ICI	Integrated Communication Interface
OLTP	Online Transaction Processing System
RDBMS	Relational Database Management System

Abbreviation	Description
BW	Business Warehouse

Security Aspects of Data Flow and Processes

The figure below shows an overview of the communication channel integration into the IC WebClient:



Overview of Communication Channel Integration

The HTTP security session management ensures the security of the communication paths displayed in the graphic. For an overview of the communication paths and more detailed information, see the section on [Network and Communication Security](#).

Abbreviation Key for Figure Above

Abbreviation	Description
ICI	Integrated Communication Interface
ICM	Internet Communication Manager
BCB	Business Communication Broker
MCM	Multi Channel Management
SAM	Simplified ABAP Messaging
SOAP	Simple Object Access Protocol

User Administration and Authentication

The IC WebClient uses the user management and authentication mechanisms provided by ABAP platform. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *ABAP Platform Security Guide* also apply to the Interaction Center. For more information, go to SAP Help Portal at <https://help.sap.com/s4hana>, choose the relevant release and search for *ABAP Platform Security Guide*.

User Management

Non-SAP Fiori Technology

User management uses the mechanisms provided by the ABAP Platform, such as tools, user types, and password concept.

Tool	Description
<i>User Maintenance</i> (SU01) transaction	For more information, see User Administration and Authentication [page 10] .
Profile generator (PFCG) transaction	You use the profile generator to create roles and assign authorizations to users in ABAP-based systems.

SAP Fiori Technology

- For more information on user management and authorization concepts used in SAP Fiori, go to https://help.sap.com/s4hana_op_2020, enter *SAP Fiori Overview* into the search bar, press , and open the search result with that title.
Also refer to the documentation in Customizing for SAP S/4HANA Service. Choose **Basic Functions** > **UI Navigation** > **Configure UI Navigation**.

Users

No users are delivered in the standard system. You need to configure the following users:

System	User	Delivered?	Type	Default Password	Description
SAP S/4HANA Service	End user	No	Dialog user created in <i>User Maintenance</i> (SU01) transaction	No	Created by a system administrator for accessing the IC WebClient
SAP S/4HANA Service	Customizing user	No	Dialog user created in <i>User Maintenance</i> (SU01) transaction	No	Created by a system administrator for customizing the IC WebClient
SAP Fiori front-end user	End user	No	Dialog user created in <i>User Maintenance</i> (SU01) transaction	No	Created by a system administrator for accessing Fiori launchpad

→ Recommendation

Users created with a default password must change their password before first use.

Authorizations

The IC WebClient uses the SAP S/4HANA Service standard for authorizations.

ABAP Stack Standard Roles Used by SAP S/4HANA Service

Role	Description
SAP_CRM_UIU_UTIL_LEAN_AGENT	PFCG Role for Utilities Interaction Agent
SAP_S4C_UIU_SRV_ICAG	PFCG Role for Service Interaction Center Agent

ABAP Stack Standard Roles Delivered With SAP S/4HANA Service Used by Industry Solutions

Role	Description
SAP_CRM_UIU_UTIL_IC_LEAN_AGENT	PFCG Role for Utilities Interaction Center Agent

Standard Authorization Objects

Authorization objects for the different business objects that are used, such as business partners or business transactions, are used in the IC agent scenario. These authorization objects are listed in the respective PFCG roles. For more information about these authorization objects, see the respective sections of the security guide for SAP S/4HANA.

The following table shows the security-relevant authorization objects used in the IC agent scenario:

Authorization Object	Field	Value	Description
CRM_CATEGO	ACTVT (Activity)	N/A	(Optional) This authorization object is used in the auto suggest function in the IC WebClient. For more information, see SAP Help Portal at https://help.sap.com/s4hana > <Choose release> > <i>Product Assistance</i> > <i>Enterprise Business Applications</i> > <i>Service</i> > <i>Basic Functions</i> > <i>Multilevel Categorization</i> > <i>Authorizations for the Category Modeler</i> > .
	SC_ID (Application ID)		
	LN_TYPE (Object links)		
	SC_PART (Part)		
	ASP_STATE (Schema status)		
	ACTVT	16	(Optional) This authorization is needed for a remote function call (RFC) used by the heartbeat function, which is activated through functional profile ICI_HEART_BEAT.
	RFC_NAME	CRM_ICI_HBT	
	RFC_TYPE	FUGR	

Network and Communication Security

Communication Channel Security

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Communication between a Web browser and AS ABAP	HTTP/HTTPS	User requests are transferred between a Web browser and AS ABAP. Logon information and subsequent requests from the browser are transferred from the browser to AS ABAP.	Used when IC agents log on to SAP S/4HANA Service from a Web browser. User-sensitive data must be protected. To configure secure sockets layer (SSL) over AS ABAP, see the <i>Application Server ABAP Platform Security Guide</i> . For more information, go to SAP Help Portal at https://help.sap.com/s4hana , choose the relevant release and search for <i>Application Server ABAP Security Guide</i> .

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Communication channel between components residing in different ABAP sessions of IC WebClient	HTTP/HTTPS	Each IC WebClient application session consists of multiple ABAP sessions running concurrently.	Used when IC WebClient is initiated. To enable HTTPS, an additional HTTP destination is created (see the Communication Destinations section below). To configure SSL over AS ABAP, see Application Server ABAP Security Guide . For more information, go to SAP Help Portal at https://help.sap.com/s4hana , choose the relevant release and search for Application Server ABAP Security Guide .
Communication between a remote SAP S/4HANA Service system or a remote SAP S/4HANA system	HTTP/HTTPS through SAP Internet transaction server	Business transactions and business objects are exchanged between SAP S/4HANA Service and SAP S/4HANA.	(Optional) Used when an IC agent in SAP S/4HANA Service tries to access data in an SAP S/4HANA system by launching a transaction. Used when creating and prepopulating a service request from a remote SAP S/4HANA system.
Communication within SAP S/4HANA	HTTP through UI	N/A	(Optional) Used when an IC agent tries to launch a UI application by launching a transaction.
Communication between an SAP S/4HANAService and communication management software (CMS), such as telephony or e-mail routers	Business communication broker (BCB) application programming interface (API) communicates with the CMS using the Simple Object Access Protocol (SOAP)	Data (such as incoming call, contact attached data, and e-mail) is transferred from the CMS to the SAP S/4HANA Service system.	(Optional) Used when multichannel is used in the IC WebClient to handle telephone calls, e-mails, chat, and so on.
Communication between an SAP S/4HANA Service system and a third-party telephony switch	SAPphone API communicates with the third-party telephony switch using RFC	Incoming call data is exchanged.	(Optional) Used when IC agents handle telephone calls through SAPphone.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Communication between SAP S/4HANA Service and Solution Manager	RFC and WebService	Incidents (both directions), from Solution Manager to SAP S/4HANA Service	Optional

Network Security

The Business Server Page (BSP) ports for HTTP/HTTPS have to be opened in the firewall if agents access the IC WebClient from another network or from the Internet by launching the IC BSP URL

Communication Destinations

The table below shows an overview of the communication destinations used by the IC WebClient:

Destination	Delivered?	Type	User, Authorizations	Description
Remote SAP S/4HANA Service system	No	RFC	N/A	(Optional) Communication with a remote SAP S/4HANA system or a remote SAP S/4HANA Service system through the transaction launcher
SAP S/4HANA	No	HTTP/HTTPS	N/A	(Optional) Communication with a remote SAP S/4HANA system through the SAP Fiori launchpad.
SAP Solution Manager	No	RFC WebService	N/A	(Optional) Communication with a remote SAP Solution Manager system
Third-party telephony server	No	RFC	N/A	(Optional) Only if IC agents handle calls using SAPphone.

You must add the following additional communication destination for HTTPS:

Destination	Delivered?	Type	User, Authorizations	Description
Connection between two different IC sessions	No	RFC	SSL is activated	Created by a system administrator using the <code>CRMM_IC_GFS</code> transaction to set up the communication between different IC WebClient sessions (agent session, worker session, or SAPphone session).

Internet Communication Framework Security

You should only activate the services that are needed for the applications running in your system.

If your firewall(s) use URL filtering, also take note of the URLs used for the services and adjust your firewall settings accordingly.

For more information about ICF Services, search for *Activating and Deactivating ICF Services* in the relevant version of [SAP S/4HANA](#) on SAP Help Portal.

For more information about ICF security, search for *RFC/ICF Security Guide* in the relevant version of [SAP S/4HANA](#) on SAP Help Portal.

Data Storage Security

Stored Data

Data	Stored Where	Stored When	Type of Access
Customizing	AS ABAP database	After installation	Read/write/change/delete Only by user with customizing authorization
Application data	AS ABAP database	IC user logon/request	Read/write/change/delete
Generated class	SAP system	During Customizing of transaction launcher	Read/write/change/delete
Configuration	SAP system	After installation	Read/write/change

The IC WebClient requires a web browser as the user interface. The data is stored on the SAP S/4HANA server.

All data stored in SAP S/4HANA Service is protected by the SAP S/4HANA backend. Customizing data can be accessed only by persons with Customizing authorization. This data is accessed by the system administrator during system configuration. Application data is protected by the authorization object. Roles define the authorization. Users assigned to a role inherit the authorization from the role.

The simplified ABAP messaging (SAM) component stores the HTTP(S) URLs of the different ABAP sessions of the IC WebClient as server-side cookies. (Each IC WebClient application session consists of multiple ABAP sessions running concurrently.) This URL contains the session ID of the ABAP session. This data is not sensitive and is not accessible from outside the current application server (AS), so there is no severe security risk. This information is deleted from the server-side cookie once the application session is shut down.

Security for Text Message Integration in Interaction Center

- If you are configuring SAPconnect for sending text messages, check the security-related settings. For more information, search for *SAPconnect (BC-SRV-COM)* in the relevant version of [SAP S/4HANA](#) on SAP Help Portal.
- For general security information regarding RFC scenarios, search for *RFC/ICF Security Guide* in the relevant version of [SAP S/4HANA](#) on SAP Help Portal.
- If the default connector, which uses SAPconnect, does not meet your requirements in terms of the dedicated service provider, you can use a customer-defined connector. In this case ensure that the network communication is secure. For more information see [Network and Communication Security \[page 19\]](#).

- Authorization concept for text message integration in Interaction Center:
 - Triggering text messages: The text message is triggered by service order actions. If a business user has the authorization to change the service order, there will be no additional authorization checks for the text message.
 - Displaying text messages: The entry of the outbound plug mapping `CRM_SMS` is enhanced for text messages in the navigation bar profile `S4C_SRV_ICAGT`. The entry is assigned to the `PFCG` role `SAP_S4C_UIU_SRV_ICAG` to control the authorization for displaying text messages.

Security for Additional Applications

The following additional applications are associated with the IC WebClient or delivered with it:

- Third-party communication management software (CMS)
It has its own authentication and authorization mechanism to provide security. Currently, it does not support HTTPS communication.
- Business communication broker (BCB)
- SAPphone
Provides a telephony function for the interaction center (IC).

There are no particular frontend clients that deviate from the standard SAP system.

The following table lists details for the additional applications

Additional Application	Vendor	Security Guide	Special Security Settings
SAP ITS	SAP internal	ABAP Platform Security Guide	No
UI	SAP internal	Security Guide for SAP S/4HANA Service	To use the UI-based application within the IC WebClient, users must have authorization to start the UI-based application
BCB	SAP internal	ABAP Platform Security Guide	No
SAPphone	SAP internal	N/A	No

Other Security-Relevant Information

Active Code	Location	Functions Disabled Without This Active Code
JavaScript	Widely used in frontend	IC WebClient

Trace and Log Files

The following information is traced in the AS cache:

- Messages exchanged between CMS and SAP S/HANA Service
- Messages exchanged between ABAP sessions

Trace is turned off by default. For more information on turning the trace on and changing trace levels, search for *Administration of the Internet Communication Manager* in the relevant version of [SAP S/4HANA](#) on SAP Help Portal.

13.7.8 Subscription Order Management

Subscription Order Management is a part of Service. You use it to manage subscription products and subscriptions to usage-based services (involving recurring fees, usage-based charges, and one-off charges).

You can further use Subscription Order Management to manage product bundles (multiple combinations of products and services), subscription orders, and subscription contracts (through contract change processes).

Additionally, you can work in a revenue sharing model using partner agreements and partner agreement orders.

User Management

Subscription Order Management uses the normal user management of SAP NetWeaver AS and require dialog users.

Users

System	User	Delivered?	Type	Default Password	Description
Service	End user	No	Dialog user created in User Maintenance (SU01) transaction	No	Used for Web-Client applications, such as Subscription Order Maintenance.
SAP Fiori frontend	End user	No	Dialog user created in User Maintenance (SU01) transactions	No	Used for Fiori applications, such as Subscription Product Maintenance

Business Roles and Authorizations

WebClient UI Business and PFCG Roles

The following business roles are used for the WebClient UI related features and functionality. You must assign these roles, in the backend system, to the users.

Business Role	PFCG Role	Purpose
S4C_SOM_REP	SAP_S4C_UIU_SOM_REP	For the sales representative working with subscription orders and contracts.
S4C_SOM_PROD	SAP_S4C_UIU_SOM_PROD	For the product modeler who models subscription products.

Mass Run-specifics

If you are using the Mass Run functionality ensure that you maintain the following authorization objects consistently:

- CRM_ORD_PR controls the business transaction types permissions, e. g. which types the user can view or create. An example for a business transaction type is PRVO, which is the delivered transaction type for “Subscription Order”
- CRMS4_SOM_MR controls the Mass Run permissions, e. g. which Mass Run types the user is allowed to view or create. Examples for Mass Run type are BULK_CALL_OFF_MA (Call-Off Master Agreement) or BULK_CREATE (Creation Subscription Orders)

Now ensure that you when you maintain restrictions on a transaction type, then keep it consistent with the Mass Run types.

❖ Example

If you restrict a user in your system so that she must not access any Master Agreements, also ensure that she cannot access the Mass Run types that are dealing with Master Agreement data. The reason is that certain Master Agreement data is replicated into the Mass Run data and hence, the user may be able to see this data (e. g. business partner ID, Master Agreement transaction ID, etc.) when accessing the Mass Run.

SAP Fiori PFCG Roles

The following PFCG roles are used for the subscription product Fiori apps that are used to maintain the subscription-specific product data:

PFCG Role	System	Purpose
SAP_SOMPRODMANS1_APP	Backend	For Manage Subscription Product-Specific app
SAP_ALLWNCDEF_MANS1_APP	Backend	For Manage Allowance Definition Group app
SAP_SHRNGGRP_MANS1_APP	Backend	For Manage Sharing Group app
SAP_BR_PROD_CONF_MODELER_SOM	Fiori Frontend	Controls launchpad for Manage Subscription Product-Specific and Manage Allowance Definition Group app
SAP_BR_INTERNAL_SALES_REP_SOM	Fiori Frontend	Controls launchpad for order and contract apps including the Manage Sharing Group app

SOAP Web Services

If you are planning to use the SOAP web services for creating a subscription order (SubscriptionOrderRequest_In) or changing a subscription contract (SubscriptionContractChangeProcessRequest_In), you also require service-specific permissions for the following authorization objects, to be able to execute the web services:

- S_SERVICE
- /AIF/PROC

Note

These permissions are required in addition to the functional PFCG roles (your custom role based on SAP_S4C_UIU_SOM_REP).

For more information about these web services, refer to [SAP S/4HANA](#) and navigate to [Product Assistance > Enterprise Business Applications > Service > Subscription Order Management > Subscription Orders and Subscription Contracts > Application Programming Interface \(API\) for Subscription Orders and Contracts](#).

Network and Communication Security

The network topology for master data is based on the topology used by the ABAP platform. The security guidelines and recommendations described in the [ABAP Platform Security Guide](#) and the corresponding component-specific sections of this security guide also apply to Subscription Order Management.

Communication Channel Security

The following communication channels are used:

- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the [Communication Channel Security](#) section above:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to Fiori front-end	HTTP/HTTPS	URLs	Passwords, all sensitive data such as credit card information, customer data, and conditions
Front-end client using a Web browser	HTTP/HTTPS	All application data	Passwords, all sensitive data such as credit card information, customer data, and conditions
Client using SOAP web services from Subscription Order Management	HTTP/HTTPS (strongly recommended)	Authentication, Application data	Authentication data, all sensitive data, such as credit card information, customer data, and conditions.

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, no special data storage security measures are required. Subscription Order Management is a dependent application, so the leading application storage security applies to survey read or edit rights.

13.7.9 E-Mail Response Management System

The E-Mail Response Management System (ERMS) is based on the AS ABAP and SAP S/4HANA Service. ERMS runtime runs on top of the workflow system. The design time uses the UI framework.

Related Security Guides

Application	Guide
AS ABAP	AS ABAP Security Guide
Workflow	ABAP Platform Security Guide

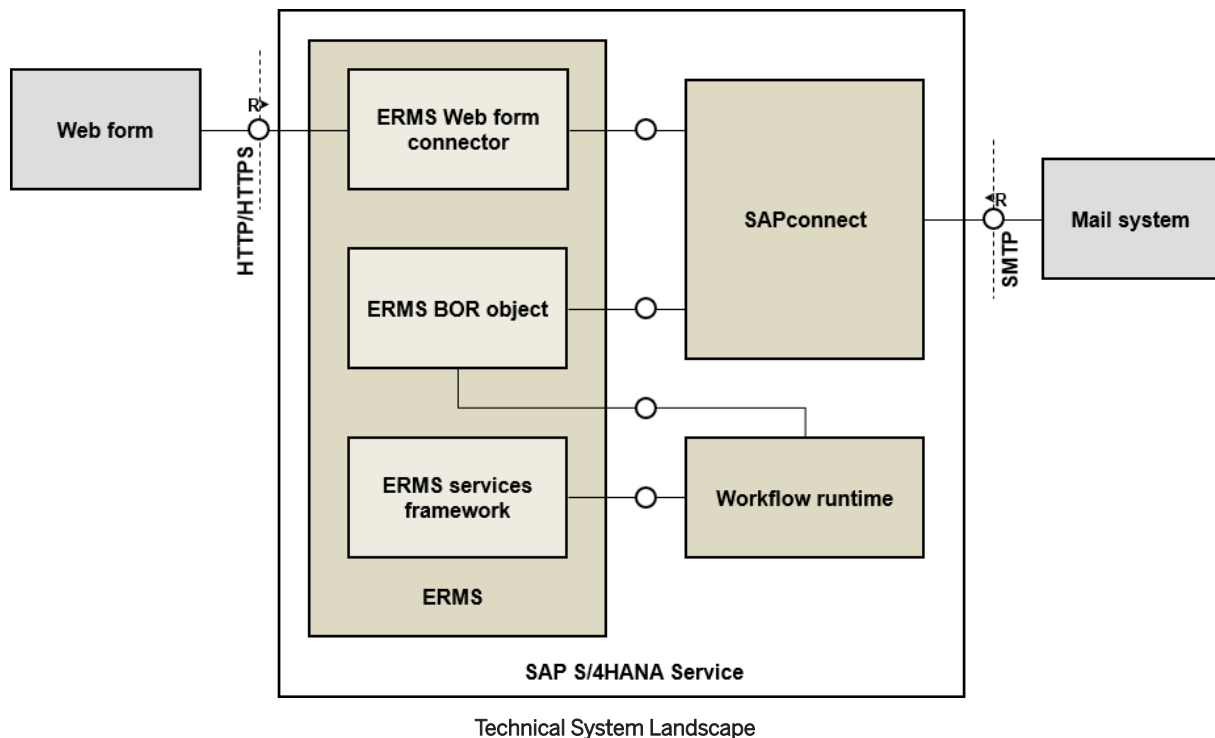
Why Is Security Necessary?

The ERMS deals primarily with e-mail. The openness of this communication channel allows anyone to send an e-mail to this system. The following measures ensure:

- High system availability (that is, make sure the system is not brought down by massive numbers of requests)
- Protection from e-mails containing malicious content
- Protection of personal data stored in the system

Technical System Landscape

The following figure illustrates the technical system landscape:



The entry point to ERMS runtime is SAPconnect. Once an e-mail is received by SAPconnect, it hands over the e-mail item to ERMS BOR object `ERMSSUPRT2`. This starts the execution of workflow `ERMS1`. You can associate an e-mail address in the system with this ERMS BOR object in the *Inbound Distribution: Settings for Recipient Determination* (SO28) transaction. Once the workflow is triggered by the incoming e-mail, it starts the ERMS service manager.

User Administration and Authentication

User Management

For general information about user management in SAP S/4HANA Service, see the [User Administration and Authentication \[page 10\]](#) section.

User Management Tools

Tool	Description
<i>User Maintenance</i> (SU01) transaction	N/A
Profile generator (PF00) transaction	You use the profile generator to create roles and assign authorizations to users in ABAP-based systems.

No users are delivered. You need to create the following users:

- Background user
User for executing workflow tasks in the background
- Individual users
In addition to creating the above workflow user above, it is necessary to do the following:
 - Give the system administrator access to modeling tools available for the ERMS
 - Create users for interaction center agents (IC agents) so that they can access the system and process incoming e-mails

Users

System	User	Delivered?	Type	Default Password	Description
SAP S/4HANA Service	End user	No	Dialog	No	Created by an SAP system administrator for access to the IC WebClient
SAP S/4HANA Service	Background user	No	System	No	For executing workflow tasks in the background

→ Recommendation

Users created with a default password must change the password before the first use.

User Data Synchronization

Authorizations

The ERMS uses the SAP S/4HANA standard for authorizations.

To enable ERMS administrators to use the ERMS design-time tools (such as the profile generator), you must assign ERMS administrators to the Service Professional role `SAP_S4C_SRV_PRO`. This role includes the necessary authorization to access the following tools:

- Rule modeler
- Category modeler
- ERMS reporting
- E-mail workbench

In addition, authorization groups make it possible to restrict different permissions (read, write, deploy, and so on) in the rule modeler. You can maintain authorization groups in Customizing for [Service](#) under **► E-Mail Response Management System** **► Define Repository** **►**. Select the appropriate context (such as *ERMS*) and select *Authorization Groups*.

Finally, add authorization `CRM_ERMS_P` to role `SAP_S4C_SRV_PRO`, and set the following parameters accordingly:

- Activity
- ERMS authorization group
- Context

Network and Communication Security

Communication Channel Security: E-Mail

We recommend that you use a general purpose e-mail server, such as Microsoft Exchange. You must implement a virus scanner on the e-mail server to scan e-mails or e-mail attachments. After scanning, the e-mail is handed over to the ERMS for processing. If you allow HTML e-mails, you must install a filter for script on your e-mail server.

SAPconnect uses the Simple Mail Transfer Protocol (SMTP) to receive e-mails. Another option for configuring your system is to send an e-mail directly to SAP S/4HANA for customer management and have it processed by ERMS. Note that this latter option is not recommended. For more information about SAPconnect, see SAP Note [738326](#).

To display or process HTML content of e-mails within the Interaction Center, your e-mail infrastructure must be able to secure or sanitize HTML mails with active content (such as, but not limited to, JavaScript) before they are sent to the Interaction Center. You must also guarantee that measures for securing or sanitizing these mails (for example filtering on the e-mail server) are switched on.

If you cannot guarantee that such measures are in place, you can disable or filter the display of HTML e-mails in the interaction center as follows:

1. Configure the display of HTML e-mails


You do this in Customizing for [Service](#) under **► Interaction Center WebClient** **► Basic Functions** **► Communication Channels** **► Define E-Mail Profiles** **►**, by setting the field *Disp. HTML Mail* (Display of HTML Mails) to *Disabled* or *Filtered*.

If you filter the display of HTML e-mails, the system triggers a warning message if a user opens an HTML e-mail that contains non-secure content. The user can decide whether the e-mail sender is trustworthy before displaying the entire content of the e-mail.

2. Assign the corresponding e-mail profile to each business role that uses the e-mail editor in the agent inbox or the ERMS e-mail workbench.

In Customizing for *Service*, choose **► UI Framework ► Business Roles ► Define Business Role** , and choose the step *Assign Function Profiles*. The relevant function profile ID for e-mail profiles is `EMAIL`.

The value assigned to the function profile `EMAIL` should be the e-mail profile ID that you have changed in the first step. If there is no entry for the function profile `EMAIL`, you have to add one.

You can also define an ERMS rule to handle, that is delete, incoming HTML mails and inform the sender automatically that you are not able to view HTML mails. HTML mails can be recognized by the e-mail document type `HTM` in the ERMS rule modeler after adding the following Customizing: In Customizing for *Service*, choose **► E-Mail Response Management System ► Define Repository** . Choose the context *ERMS* and go to the step *Attributes*. Add the following entry:

Attribute: <Attribute ID> (for example, `ZMAIL_DOCTYPE`)

Description: E-Mail Document Type

Show Attribute: X

XPath: `/paths/EMAIL/OBJ_TYPE/text ()`

Fact Gathering Service: `FG_EMAIL`

Attribute Extension Class: `CL_CRM_ERMS_ATTR_EXT_EQUALS`

Communication Channel Security: Web Form Connector

If you are using the web form connector, you must do the following to handle undefined web form IDs:

- Create a default implementation of `BAdI_CRM_ERMS_WF_CON`. In the `BAdI` implementation, form data from undefined web form IDs must be rejected.
- Submit the form data to the `confirmation.htm` BSP page.
- Ensure that the form data has successfully passed a `CAPTCHA` before it is submitted to the web form connector.

Data Storage Security

ERMS data is stored in the SAP HANA database. You do not need to implement additional security measures. The stored data can be classified as shown in the following table:

Stored Data

Data	Stored Where	Stored When	Type of Access	Who Can Access It
E-mail document	SAP S/4HANA business workplace persistence Database table CRMD_ERMS_CONTNT	When an e-mail arrives	Read/delete	ERMS routes the e-mail to an organizational unit. Users in that organization can access the e-mail document.
ERMS fact base	SAP S/4HANA under workflow container	When ERMS processes an e-mail	Read/write/delete/change	Service Professional in the ERMS log, or the Selection Report for Work Items (SWI1) transaction (only in read-only mode)
ERMS rules	Customizing for Service under E-Mail Response Management System Define Repository	When rules are maintained	Read/write/delete/change	Service Professional
ERMS configuration	SAP S/4HANA system under ERMS repository (customizing data)	During configuration	Read/write/delete/change	ERMS administrator Person who makes the Customizing settings for customer management

Trace and Log Files

Log information is available in [Check Automatic Processing Details](#) (transaction CRM_ERMS_LOGGING). The log provides information about the following:

- Services by ERMS service manager
- Data gathered by ERMS services
- Rules evaluation
- Category assignment
- Execution times for different services

Checklist

Feature	Check	How to Check
Restrict access to e-mail processing	Workflow e-mail task can be processed only by authorized organizational units or authorized users	<p>In the SAP Easy Access screen, choose</p> <p>▮ Service ▸ Interaction Center ▸ E-Mail Response Management System ▸ Settings ▸ Assign Agent for E-Mail Handling ▮.</p> <p>Choose Assign Agents.</p> <p>Expand workflow template ERMS1 and select task TS 00207914.</p> <p>Choose Attributes and select the item as required.</p> <p>In the toolbar, choose Create agent assignment. (Not necessary for a general task because everybody can process this task.)</p>
Restrict access to e-mail processing	Authorized agents are properly assigned to the organizational unit	<p>For the e-mail workflow task above, in the application in the Service Professional role, choose ▮ Service Operations ▮</p> <p>▮ Search: Organizational Model ▮.</p>
Restrict or allow access to certain policies in ERMS rule modeler	ERMS authorization group concept is used	<p>To define your authorization groups, use transaction CRMC_ERMS_REPOSITORY.</p> <p>To define which policies users can read, change, create, and deploy, and under which ERMS authorization groups such operations can be performed, use authorization object CRM_ERMS_P as a template.</p>
Web form connector (if used)	Default implementation for the ERMS Web Form Connector BAdI (CRM_ERMS_WF_CON) exists	<ol style="list-style-type: none"> 1. In the BAdI Builder transaction (SE18), display the BAdI CRM_ERMS_WF_CON. 2. Ensure that the Enhancement Implementations tab page contains a BAdI implementation in which the Default Implementation checkbox is selected.

13.7.10 UI Framework

User Administration and Authentication

User Management

Tool	Description
User Maintenance (SU01) transaction	To use Web applications, all users must first have an account created using the User Maintenance (SU01) transaction.

User authentication is performed by using standard tools of provided by the ABAP platform along with the connected application system.

Logon Procedure

The logon procedures are provided by the Internet communication framework of the ABAP platform: [Maintain Services](#) (transaction SICF).

The logon procedure is configured in:

- `/default_host/sap/bc/bsp/sap/crm_ui_start`
 - Default form-based logon procedure (user/password)
 - Function for changing passwords

If you want to change the default logon procedure, create your own alias of service `/default_host/sap/bc/bsp/sap/crm_ui_start` and make the changes there. Do not change the SAP service/alias.

For more information about ICF Services, search for *Activating and Deactivating ICF Services* in the relevant version of [SAP S/4HANA](#) on SAP Help Portal.

For more information about ICF security, search for *RFC/ICF Security Guide* in the relevant version of [SAP S/4HANA](#) on SAP Help Portal.

Authentication When Using Search Modeling Workbench

The enterprise search modeling workbench (transaction `CRM_ES_WB`) is an SAP GUI application. Users are authenticated when they log on to the system.

Authentication When Using Atom Feed

When `Atom Feed` service is accessed, the standard user authentication is performed. This implies that the Atom reader used must support feeds requiring authentication.

Once the user is authenticated, the system sends the corresponding data back to the Atom reader under the following conditions:

- The user has the right to use the feed, as checked with the authorization object `S_WCF_FEED`.
 - The user is assigned to the business role for which the feed is requested.
 - The authority checks allow the user to access the corresponding data.
- For more information, see the [Authorizations](#) section below.

An individual entry returned by the feed can contain a direct link to a business object on the WebClient UI. The user can click that link to open the standard application in the Web browser. The security standards are the same as when the user accesses the WebClient UI in Web browser and navigates to the business object.

Authorizations

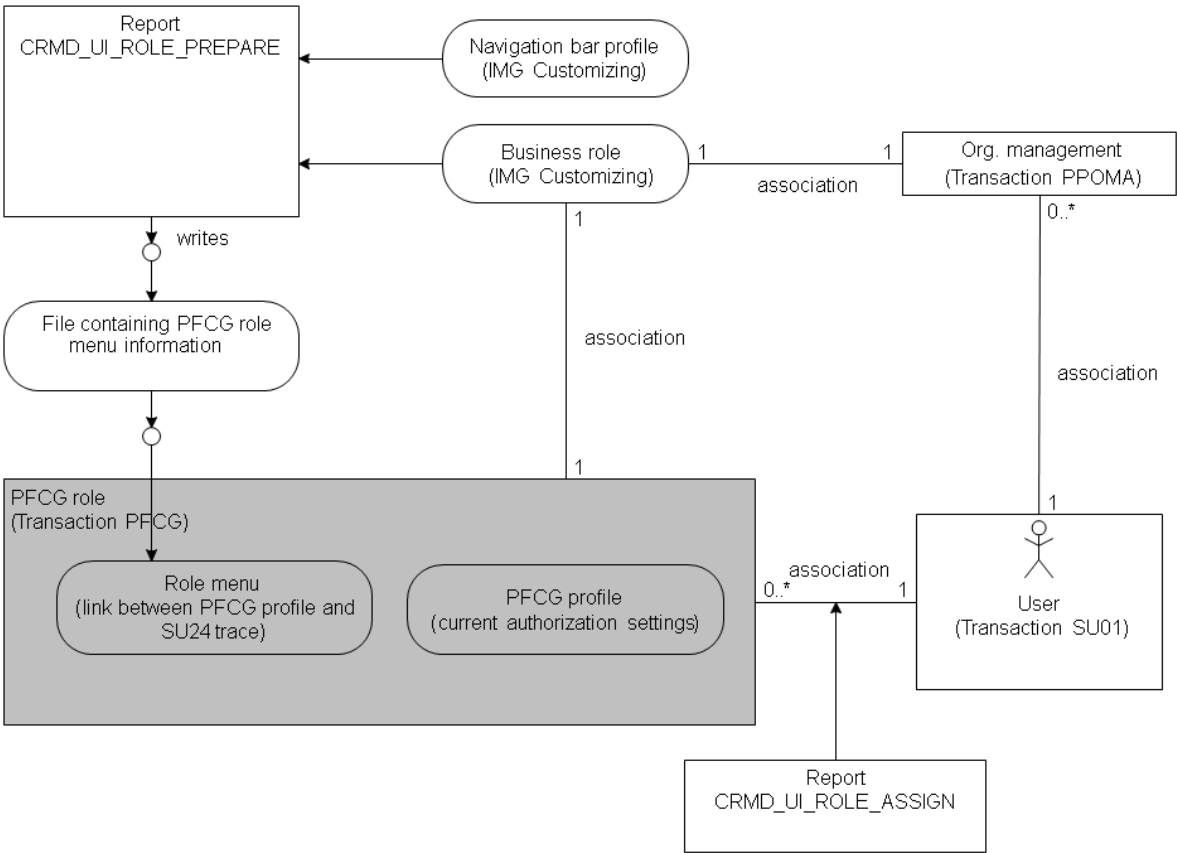
Authorization Concept Overview

In the application role concept, there is a dependency between business roles and PFCG roles. Each business role has a corresponding PFCG role containing only those authorization objects needed to fulfill the task defined in the business role. This section describes the parts involved in creating custom PFCG roles for business roles.

For more information about setting up authorizations for business roles, see Customizing for [Service](#) under [UI Framework > Business Roles > Overview](#).

The figure below, along with the table that follows, illustrates dependencies between the following:

- PFCG role menu and the business role
- User and the PFCG role

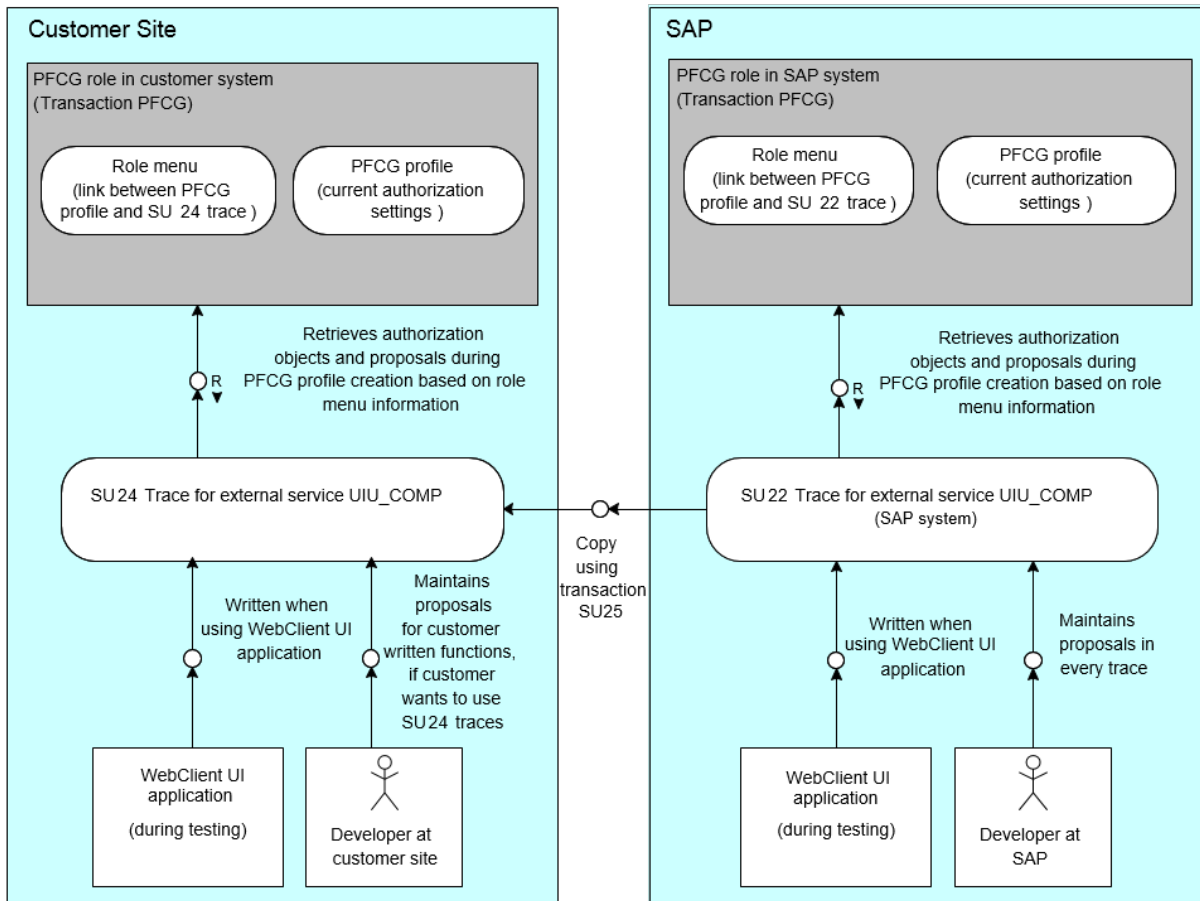


Role Dependencies

Component	Description
User	Users are maintained with <code>SU01</code> . Authorizations are provided using PFCG profiles and roles assigned to the users.
Organizational management	<p>Users are indirectly assigned to business roles using organizational management. If a position in organizational management is assigned to a business role using info type <i>Business Role</i>, then in turn, all users are assigned to this business role as well.</p> <p>For more information about other ways to assign business roles, see the <i>Determination of Business Roles</i> section below.</p>
Navigation bar profile	Used to define work centers, logical links, and so on. Provides common settings used in business roles.
Business role	Uses and adopts the navigation bar profile to the needs of particular business functions. For example, work centers can be turned off. There is usually an assignment to one PFCG role.
Report <code>CRMD_UI_ROLE_ASSIGN</code>	Assigns PFCG roles to users based on user assignments in organizational management (positions in organizational management are assigned in turn to business roles).
PFCG role	<p>Contains authorizations tailored to the business role. The authorizations are retrieved from <code>SU22/SU24</code> traces (at SAP customers), based on the PFCG role menu.</p> <div style="border: 1px solid orange; padding: 5px; margin: 10px 0;"> <p>⚠ Caution</p> <p>Every user must be assigned to the PFCG role <code>SAP_CRM_UIU_FRAMEWORK</code>, in addition to the business role-specific PFCG role.</p> </div> <p>Usually there is a 1:1 relation between business roles and PFCG roles. There are, however, cases where this is not suitable. You can then use Customizing for business roles to assign the same PFCG role to several business roles or to omit a PFCG role.</p>
PFCG role menu	This menu is imported from a file created by report <code>CRMD_UI_ROLE_PREPARE</code> in the PFCG transaction. Each role menu option is linked to an <code>SU22/SU24</code> trace. The menu contains all traces and in turn all the authorizations needed to run a specific business role.
Report <code>CRMD_UI_ROLE_PREPARE</code>	The report creates the role menu file based on the settings in Customizing. This information represents the link between the business role settings and the <code>SU24</code> traces.

The figure below, along with the table that follows, illustrates dependencies between the following:

- PFCG role and the SU22/SU24 traces
- PFCG role and the WebClient-based application



Dependencies

Component	Description
PFCG profile	Contains authorization objects needed for a particular business role. The profile retrieves authorization objects from the SU22/SU24 trace during profile creation. Only the traces connected to the PFCG role by the role menu are read.
SU22 trace	Authorization traces delivered by SAP. The WebClient UI uses the external trace type UIU_COMP.
SU24 trace	Authorization traces maintained by the customer. These traces are copied from the SAP namespace (SU22) using transaction SU25.

Component	Description
Applications	<p>Available UI functions are controlled using business role Customizing. Authorizations are controlled by PFCG roles.</p> <p>SU22 (at SAP) and SU24 (at the customer) traces are written if they are activated when the application performs an authorization check.</p> <p>To activate or deactivate a trace, use transaction RZ11:</p> <p>auth/authorization_trace = Y: active</p> <p>auth/authorization_trace = N: inactive</p> <p>To optimize the coverage of the authorization check in the SU22 and SU24 traces, execute a larger number of functions in the application.</p>

Determination of Business Roles

To use the WebClient UI, the user needs to have a business role assigned to his or her user. Business roles are determined in the following order:

1. Check whether a single business role is assigned using the user parameter `CRM_UI_PROFILE`. This setting overrules any other role assignments.
2. Check whether there are business roles assigned using *Organizational Management*.
3. If neither of the above cases are true, the system determines the PFCG roles assigned to the user and checks whether they are linked to a business role. If this is the case, this business role is used.

Web-Based Business Role Customizing

It is possible to customize business roles using the WebClient UI. For more information, see the product assistance on SAP Help Portal at <https://help.sap.com/s4hana> ► *Enterprise Business Applications* ► *Service* ► *WebClient UI Framework* ► *Business Roles* ►.

Application Enhancement Tool

The application enhancement tool is defined in the *Administration* work center (work center link groups: CT-ADM-SR). Activating the *Administration* work center in any business role requires an update of the PFCG role.

The application enhancement tool provides a standard PFCG role with the name `SAP_AXT_EXTENSIBILITY_ADMIN`, which contains the entire needed authorization object from the SU22 trace.

To use the *Application Reference* field type, ensure that users accessing fields of that type have application-specific authorization objects. For more information about application-specific authorization objects, see the relevant application-specific section.

To use tags from the central data storage in calculated fields or the embedding mechanism, you need the authorization object `TAG_ATB`.

To define calculated fields from the Application Enhancement Tool, no additional authorization is needed. For support or administration of Business Rule Framework plus (BRFplus) formula, you need the `SAP_BC_FDT_ADMINISTRATOR` role.

Central Sharing Tool: Prevention of Unauthorized Access to Items by Recipients

The central sharing tool is a feature that allows users with special privileges to share their tags, favorite objects, saved searches, and reports with other users, business roles, an organizational unit, or a position in a business role.

Technical and authorization checks are run to prevent recipients from accessing items, such as saved searches, that they would not be otherwise allowed to access. A two-level approach is used.

First, when the object is shared, all technically possible checks are run to verify that the recipients have the authorization/option to view the shared items. If a problem is detected, sharing is not possible.

Secondly, before the items are displayed in the recipient's share box, all the remaining checks are run. If any authorization problems are detected, the corresponding item is not displayed.

The following table is a description of the checks that are run:

Object	Description	Sharing Time	Recipient Display Time
Saved Search	The user needs to navigate to the relevant search page or result page. Criteria are shared, not the result. It is not necessary to check each result entity. When the actual search is executed, the results of the authorization checks dictate whether or not the BOL returns the entity.	Is the required Customizing for navigation available?	Is the required Customizing for navigation available?
Favorites	The user needs to be able to dynamically navigate to the object overview page and to display the corresponding entity.	Is the required Customizing for navigation available? (Navigation to mixed list and to the object overview page)	Is the required Customizing for navigation available? (Navigation to mixed list and to the object overview page) Can the current user access the corresponding BOL entity?
Tags	The tag itself is shared, not the tagged object. It is not necessary to check each tagged entity. When the mixed list is called, the objects are filtered to display only those that the user is allowed to see.	Is the required Customizing for navigation available? (Navigation to mixed list)	Is the required Customizing for navigation available? (Navigation to mixed list)

Object	Description	Sharing Time	Recipient Display Time
Reports	If the <i>Logical Link</i> report is customized for a business role, the report can be displayed by all users of that business role. There is only an authorization check on the content of the report. Different users might see different data in the report based on their authorizations.	Is the required Customizing for navigation available? (Navigation to the logical link)	Is the required Customizing for navigation available? Navigation to the logical link)

The BOL implementation authorization check is used to check if the recipient has access to a BOL entity.

Central Sharing Tool: Prevention of Unauthorized Access to Items by Sharers

The sharer can select the following as recipients:

- Organizational units
- Positions within an organizational unit
- Business roles
- Individual users

The following authorization objects are used to control access by the sharers to only those recipients to whom they were granted access.

Audience Type	Authorization Object	Field/Suggested Values
Users	S_USER_GRP	ACTVT/03 (Display)
Business role	S_TABU_DIS	S_USER_GRP (Display) DICBERCLS/CRMC
Organizational units and positions	PLOG	PPFCODE/DISP PLVAR/01 OTYPE/O, S, US

Standard Roles

Role	Role Description
SAP_CRM_UIU_FRAMEWORK	This role is a special role that is assigned to every user. It contains the authorizations that are necessary to use the WebClient UI framework.

Authorization Objects

The WebClient UI framework includes the following authorization objects:

Used By	Authorization Object	Description
UI framework	UIU_COMP	Restricts access to applications at the component level. Only authorized users can launch the WebClient UI.
UI Customizing	CRM_CONFIG	The authorization object CRM_CONFIG is used to restrict authorization for UI configuration based on component name, BSP view name, UI object type, and role configuration key.
Transaction launcher	C_LL_TGT	Controls authorizations of logical links of type C (launch transaction) and D (BI report).
Web service tool	CRM_WST	Controls access to the Web service tool.
Rapid Application Tool	S_CTS_ADMI	Needed to transport rapid applications
	S_CTS_SADM	Needed to transport rapid applications
	S_DEVELOP	This authorization object is used in the embedding tool to generate rapid applications.
	S_ICF_ADM	This authorization object is needed to generate UIs for rapid applications.
	S_TABU_DIS	This authorization object is used in the embedding tool to restrict authorization for generation of table entries.
	S_TCODE	This authorization object is within the generation framework to regenerate invalid load.
	TAG_ATB	This authorization object is needed to make use of the tag attribute.
	S_TRANSPRT	This authorization object is used in the embedding tool to create new transport requests or new tasks.
Web Service Consumption Tool	CRM_WSC	Controls access to the Web Service Consumption Tool. For more information, see SAP Library on SAP Help Portal at http://help.sap.com/crm >> <Choose a release> > Application Help > Basic Functions > Web Services > Web Service Consumption >.
	S_CTS_ADMI	This authorization object is needed to transport the generated objects.
	S_CTS_SADM	This authorization object is needed to transport the generated objects.

Used By	Authorization Object	Description
	S_DATASET	This authorization object is needed to access the locally saved WSDL file.
	S_DEVELOP	This authorization object is used to generate the objects.
	S_TRANSPRT	This authorization object is used to create new transport requests or new tasks.
Enterprise search integration	S_DEVELOP	Restricts access to the enterprise search modeling workbench
	S_ESH_ADM	Restricts transfer of application models to enterprise search to authorized users
	S_TABU_DIS	Restricts client copy of application models to authorized users
	S_TRANSPRT	Restricts maintenance of Customizing transports containing the application models to authorized users
Atom feed	S_WCF_FEED	This authorization object is used to restrict access to the feed function in the applications.

For more information, see the object documentation using *Maintain the Authorization Objects* (transaction SU21) and the UI configuration guide.

The main business-related authority checks are done by business objects within the business object layer (BOL) and by applications.

For more information about authority checks and working with authorization objects, see the *ABAP Platform Security Guide* on SAP Help Portal at <http://help.sap.com/s4hana>.

Authorizations of Atom Feeds

The authorization object WCF_FEED is used to authorize or forbid the usage of the Atom feed feature in applications. The following authorization check is performed to verify the rights of the user to access the feed:

```
AUTHORITY-CHECK OBJECT 'WCF_FEED'
  ID 'FEED_ID' FIELD iv_feed_id
  ID 'ACTVT' FIELD '03'.
```

In other words, the user needs display rights to access the feed with ID iv_feed_id. So far only the feed with ID DEFAULT is delivered, so the only value used for iv_feed_id variable is DEFAULT.

In addition to this authorization check, when a given type of data is being retrieved, such as an alert, the authority checks performed are the same ones that are used when data is accessed in the standard WebClient UI (for example, in worklist alerts).

Protection of User Parameters

We recommend that you prevent users from adding new parameters or changing user parameters in the profile.

i Note

If users have access to the WebClient UI, but not the SAP GUI, users should not be able to use the [Maintain User Profile \(SU3\)](#) transaction to change user parameters.

Network and Communication Security

Communication Channel Security

The following table shows the general communication paths used, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Browser to application	HTTP/HTTPS (secure)	All application data	Passwords and other sensitive data
Server to server	Remote function call (RFC)/ Secure network communication (SNC) (secure)	System ID, client name, and host name; all application data	System information and application data
Atom feeds	HTTPS	Business data	The SICF service <code>/sap/crm/crm_feed</code> requires SSL. This means that the Atom reader that is used must support HTTPS access.
Communication between WebClient UI and SAP Net-Weaver enterprise search	TCP/IP	Used for all enterprise search-related activities in such as transfer of models, extraction of templates, and search.	N/A

Communication Channel Security: Virus Scan Profiles

For information about virus scan profiles, see [Network and Communication Security \[page 19\]](#).

Secure Sockets Layer (SSL)

The interaction between the the WebClient UI framework and SSL is limited. You use SSL to extend the capabilities of HTTP.

The AS ABAP and SSL do not interact with the Web applications running in the browser, nor do they affect the WebClient UI framework, which is used by these applications.

Level of Protection

The URL connection to the back-end system is base64 encoded. The BSP technology ensures base64 encoding for all form parameters in the URL. However, this mechanism is not used within the WebClient UI

framework. The WebClient UI framework does not prevent you from using any sort of security technique. You can also safeguard the data in the URL using either:

- SSL for HTTP
- Direct server communication using HTTP POST

Data Storage Security

Stored Data

Data	Storage Location	Stored When	Access Type
Customizing	AS ABAP database	Post installation	Read/write/change/delete Only by users with Customizing authorizations
Application data	AS ABAP database	User logon/request	Read/write/change/delete
Atom feed	No data is stored by application feeds.		

i Note

The feed reader can store user credentials. SAP does not have any control over third-party readers.

The WebClient UI framework supports or requires a Web browser as its user interface. The data is stored on the application server.

All data stored in the system is protected by the back end. Customizing data can be accessed only by users with Customizing authorizations. This data is accessed by the system administrator during system configuration. Application data is protected by authorization objects. Roles define the authorizations. Users assigned to a role inherit authorizations from that role.

Tracing and Log Files

The following information is traced in the AS ABAP cache:

- Messages exchanged between a communication management software (CMS) and the application server
- Messages exchanged between ABAP sessions

By default, tracing is switched off. For more information on turning on the trace and changing the trace level, search for *Administration of the Internet Communication Manager* in the relevant release of [SAP S/4HANA](#) on SAP Help Portal.

Other Security-Related Information

JavaScript

The WebClient UI framework uses JavaScript and AJAX to render the UI in the browser, and to handle user interactivity as well. Precautions have been taken against cross-site scripting (CSS) and other related types of attacks.

ActiveX

Name	Used In
Microsoft.XMLHTTP	AJAX, e-mail integration (Microsoft Excel, Notes)
Mxml2.XMLHTTP	New version of Microsoft.XMLHTTP
Word.Application	Displaying of data in a Microsoft Word document
Excel.Application	Displaying of data in a Microsoft Excel spreadsheet
Outlook.Application	Microsoft Outlook integration: <ul style="list-style-type: none">• Exchange of e-mails from Microsoft Outlook to applications and the other way around• Address lookup in Microsoft Outlook
Lotus.NotesSession	Lotus Notes integration: <ul style="list-style-type: none">• Exchange of e-mails from Lotus Notes to applications and the other way around• Address lookup in Lotus Notes

Required Settings in Microsoft Internet Explorer:

- Active scripting
- Run ActiveX controls and plug-ins
- Initialize and script ActiveX controls not marked as safe (XMLHTTP libraries just need: *Script ActiveX controls marked safe for scripting*)

Cookies

WebClient UI Framework does not use its own session or persistent cookies.

Additional Information

For more information, see:

- *ABAP Platform Security Guide* on SAP Help Portal at <http://help.sap.com/s4hana>.
- *Application Server ABAP Security Guide* on SAP Help Portal at <http://help.sap.com/s4hana>.

13.7.11 Knowledge Management

The Knowledge Management (KM) component delivers functions and services for managing unstructured or partially structured content. It enables the user to save and find documents in different types of repositories, and allows the user to find and access information using advanced information finding and document classification methods. It supports Web authoring and publishing and includes form-based publishing of standard content. The KM component offers generic services, for example, for informing users about changed content and for introducing approval processes into the publishing process.

Why Is Security Necessary?

Security is necessary to protect internal documents from misuse due to external access or access from other departments. If documents are not protected, sensitive data may become public knowledge and harm your enterprise.

Documents may also contain viruses that can damage your entire network if they are not discovered and eliminated in time.

User Administration and Authentication

Integration with the Single Sign-On Environment

KM works in a single sign-on (SSO) environment.

Authorizations

In SAP S/4HANA Service, user authorizations for a business object to which documents are assigned are copied to the documents: For example, if a user only has read authorization for an application, then he or she only has read authorization for the associated documents.

Authorization Check on Document Level

You can also implement an authorization check at document level. In Customizing for *Service*, choose ► [Basic Functions](#) ► [Content Management](#) ► [Business Add-Ins \(BAIs\)](#) ► [BAI: Authorization Check on Document Level](#) ►

13.7.12 Deletion of Personal Data in Service

Use

Business objects in *Service* might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under [Product Assistance](#) [Enterprise Business Applications](#) [Service](#) [Basic Functions](#) [Information Lifecycle Management](#).

Relevant Business Objects and Available Deletion Functionality

Business Objects	Provided Deletion Functionality
Business Solution Portfolio	Archiving object CRMS4_BSP
Service Contract	Archiving object CRM_SRCONT
Service Confirmation	Archiving object CRM_SRVCON
Service Order	Archiving object CRM_SERORD
Knowledge Article	Archiving object CRM_KA
Service Request	Archiving object CRM_INCDNT
In-House Repair	Archiving object CRMS4_REPA

Relevant Business Objects and Available EoP Functionality

Business Objects	Implemented Solution (EoP or WUC)	Further Information
Service (CRM-S4-SRV)	EoP check	This EoP check includes business in the areas of the following: <ul style="list-style-type: none">• Sales• Service• Billing• Pricing• Procurement• Delivery

More Information

- For more information about data protection, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under **Product Assistance** > **Enterprise Business Applications** > **Service** > **Basic Functions** > **Data Protection**.
- For more information about archiving business objects that belong to completed business processes, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under **Product Assistance** > **Enterprise Business Applications** > **Service** > **Basic Functions** > **Data Archiving**.

13.7.13 Warranty Management

13.7.13.1 Authorizations

Warranty (LO-WTY) uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
C_WTY_ACT	Warranty: Actions Authorization Object
C_WTY_OBJ	Warranty: Process Object Authorization Object
C_WTY_STAT	Warranty: Status Authorization Object

13.7.13.2 Deletion of Personal Data

Use

Warranty (LO-WTY) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Warranty (LO-WTY)	Archiving Object WTY_CLAIM ILM Object WTY_CLAIM

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Warranty (LO-WTY)	EoP check	Checks tables: PNWTYH, PNWTYV

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components*→*Data Protection*.

13.8 Sourcing and Procurement

13.8.1 Authorizations

Front-End Roles

To use the Fiori Launchpad in SAP S/4HANA, you have to apply the SAP S/4HANA role concept based on business catalogs that are assigned to business roles. For the front-end, the following standard business roles are available for Sourcing and Procurement. You can use these roles as templates for your own roles. For more information, see *SAP Fiori Overview*.

Business Roles

Role	Description
SAP_BR_AP_ACCOUNTANT_PROCUREMT	Accounts Payable Accountant - Procurement
SAP_BR_BUYER	Strategic Buyer
SAP_BR_EMPLOYEE PROCUREMENT	Employee - Procurement
SSAP_BR_PURCHASER	Purchaser
SAP_BR_PURCHASING_MANAGER	Purchasing Manager

Back-End Roles

In the back-end, you have to create roles in transaction PFCG and assign business catalogs to the roles. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

If you have converted your system from SAP ERP to SAP S/4HANA, you may still be accessing transactions via the SAP Easy Access menu. To support this case, the standard role templates for back-end roles are still available and are listed below:

Back-End Roles (Relevant for System Converted from SAP ERP)

Role	Description
SAP_MM_PUR_ADDITIONAL_FUNC	Non-Assigned Purchasing Functions
SAP_MM_PUR_ARCHIVE	Archive Purchasing Documents

Role	Description
SAP_MM_PUR_ARCHIVE_LISTS	Analyses Using the Purchasing Archive
SAP_MM_PUR_CONDITIONS	Conditions in Purchasing - Overview
SAP_MM_PUR_CONDITIONS_DISCOUNT	Discounts in Purchasing
SAP_MM_PUR_CONDITIONS_PRICES	Prices in Purchasing
SAP_MM_PUR_CONFIRMATION	Confirmations
SAP_MM_PUR_CONTRACT_LISTS	Lists for Outline Agreements
SAP_MM_PUR_CONTRACT_MESSAGE	Output Outline Agreements
SAP_MM_PUR_CONTRACT_MESSAGE_MT	General Message Maintenance for Outline Agreements
SAP_MM_PUR_CONTRACT_RELEASE	Release Outline Agreements
SAP_MM_PUR_CONTRACTING	Process Contracts
SAP_MM_PUR_DISPLAY_OBJECTS	General Display Functions in Purchasing
SAP_MM_PUR_GENERAL	General Functions in Purchasing
SAP_MM_PUR_INFORECORD	Maintain Purchasing Info Record
SAP_MM_PUR_INFORECORD_LISTS	Lists of Purchasing Info Records
SAP_MM_PUR_LIS_GENERAL	General Analyses for LIS
SAP_MM_PUR_LIS_SERVICE	LIS Analyses for Services
SAP_MM_PUR_LIS_STOCK_MATERIAL	LIS Analyses for Stock Material
SAP_MM_PUR_LIS_VE	LIS Analyses for Vendor Evaluation
SAP_MM_PUR_LISTS_GENERAL	General Analyses in Purchasing
SAP_MM_PUR_MASS_CHANGE	Mass Maintenance in Purchasing
SAP_MM_PUR_MESSAGE	Output Purchasing Documents
SAP_MM_PUR_MESSAGE_MAINTENANCE	General Message Maintenance in Purchasing
SAP_MM_PUR_MPN_AMPL	Approved Manufacturer Parts
SAP_MM_PUR_MPN_AMPL_ARCHIVE	Archive Approved Manufacturer Parts List
SAP_MM_PUR_NEGOTIATION_LISTS	Lists for Purchasing Negotiations
SAP_MM_PUR_PO_RELEASE	Release Purchase Orders

Role	Description
SAP_MM_PUR_PR_LISTS	Lists of Purchase Requisitions
SAP_MM_PUR_PR_RELEASE	Release Purchase Requisitions
SAP_MM_PUR_PURCHASEORDER	Process Purchase Orders
SAP_MM_PUR_PURCHASEORDER_LISTS	Lists of Purchase Orders
SAP_MM_PUR_PURCHASEREQUISITION	Process Purchase Requisitions
SAP_MM_PUR_QUOTA_ARRANGEMENT	Maintain Quota Arrangement
SAP_MM_PUR_QUOTA_MAINTENANCE	Revise Quota Arrangement
SAP_MM_PUR_QUOTATION	Maintain Quotation
SAP_MM_PUR_RFQ	Process Request for Quotation
SAP_MM_PUR_RFQ_LISTS	Lists of Requests for Quotations
SAP_MM_PUR_SCHEDULE	Maintain Scheduling Agreement Delivery Schedules and Releases
SAP_MM_PUR_SCHEDULE_MAINTENANC	Administer Scheduling Agreements
SAP_MM_PUR_SCHEDULEAGREEMENT	Process Scheduling Agreements
SAP_MM_PUR_SERVICE	Service Entry Sheet
SAP_MM_PUR_SERVICE_CONDITIONS	Service Conditions for Service
SAP_MM_PUR_SERVICE_LISTS	Lists of Service Entry Sheets
SAP_MM_PUR_SERVICE_TRANSFER	Data Transfer for Services
SAP_MM_PUR_SOURCE_LIST	Maintain Source List
SAP_MM_PUR_SRV_CONDITIONS_GEN	Service Conditions for Services (General)
SAP_MM_PUR_SRV_MODEL_SPEC	Maintain Model Service Specifications
SAP_MM_PUR_SRV_STANDARD_SPEC	Maintain Standard Service Specifications
SAP_MM_PUR_SRV_VENDOR_COND	Service Conditions for Vendor
SAP_MM_PUR_SRV_VENDOR_PLANT_CO	Service Conditions for Vendor and Plant
SAP_MM_PUR_SUPPLIER_LOGISTICS	Logistics information for the vendor on the Internet
SAP_MM_PUR_TAXES	Taxes in Purchasing

Role	Description
SAP_MM_PUR_VE	Maintain Vendor Evaluation
SAP_MM_PUR_VE_LISTS	Lists of Vendor Evaluations
SAP_MM_PUR_VE_MAINTENANCE	Vendor Evaluation in the Background
SAP_MM_PUR_VENDOR_PRICE	Change Prices for Vendor
SAP_MM_PUR_SOURCE_LIST	Maintain Source List
SAP_AUDITOR_BA_MM_PUR	This transaction role allows evaluations to be collected, structured, and configured for the audit area: <ul style="list-style-type: none"> • Business Audit - Process View • Purchasing: From Purchase Order to Outgoing Payment • Purchasing
SAP_AUDITOR_BA_MM_PUR_A	This role provides read access for the audit area: <ul style="list-style-type: none"> • Business Audit - Process View • Purchasing: From Purchase Order to Outgoing Payment • Purchasing
SAP_MM_IV_CLERK_BATCH1	Enter Invoices for Verification in the Background
SAP_MM_IV_CLERK_BATCH2	Manual Processing of Invoices Verified in the Background
SAP_MM_IV_CLERK_GRIR_MAINTAIN	GR/IR Clearing Account Maintenance
SAP_MM_IV_CLERK_GRIR_MAINTAIN	GR/IR Clearing Account Maintenance
SAP_MM_IV_CLERK_ONLINE	Online Invoice Verification
SAP_MM_IV_CLERK_PARK	Park Invoices
SAP_MM_IV_CLERK_RELEASE	Invoice Release
SAP_MM_IV_SUPPLIER_FINANCE	Settlement Information for Vendor (External Supplier) on the Internet
SAP_MM_IV_CLERK_AUTO	Automatic Settlements
SAP_AUDITOR_BA_MM_IV	This transaction role allows evaluations to be collected, structured, and configured for the audit area: <ul style="list-style-type: none"> • Business Audit - Individual Account Closing • Profit and Loss Statement • Material Expense

Role	Description
SAP_AUDITOR_BA_MM_IV_A	<p>This authorization role provides read access for the audit area:</p> <ul style="list-style-type: none"> • Business Audit - Individual Account Closing • Profit and Loss Statement • Material Expense

Standard Authorization Objects

The table below shows the security-relevant authorization objects that you can use in SAP S/4HANA when you create back-end roles. These objects were also used in the above listed standard back-end roles.

Authorization Object	Description
M_AMPL_ALL	Approved Manufacturer Parts List
M_AMPL_WRK	Approved Manufacturer Parts List - Plant
M_ANFR_BSA	Document Type in RFQ
M_ANFR_EKG	Purchasing Group in RFQ
M_ANFR_EKO	Purchasing Organization in RFQ
M_ANFR_WRK	Plant in RFQ
M_ANFR_LGO	Storage Locations in RFQ
M_ANGB_BSA	Document Type in Quotation
M_ANGB_EKG	Purchasing Group in Quotation
M_ANGB_EKO	Purchasing Organization in Quotation
M_ANGB_WRK	Plant in Quotation
M_ANGB_LGO	Storage Locations in Quotation
M_BANF_BSA	Document Type in Purchase Requisition
M_BANF_EKG	Purchasing Group in Purchase Requisition
M_BANF_EKO	Purchasing Organization in Purchase Requisition
M_BANF_FRG	Release Code in Purchase Requisition

Authorization Object	Description
M_BANF_WRK	Plant in Purchase Requisition
M_BANF_LGO	Storage Location in Purchase Requisition
M_BEST_BSA	Document Type in Order
M_BEST_EKG	Purchasing Group in Purchase Order
M_BEST_EKO	Purchasing Organization in Purchase Order
M_BEST_WRK	Plant in Purchase Order
M_BEST_LGO	Storage Location in Purchase Order
M_EINF_EKG	Purchasing Group in Purchasing Info Record
M_EINF_EKO	Purchasing Organization in Purchasing Info Record
M_EINF_WRK	Plant in Purchasing Info Record
M_EINK_FRG	Release Code and Group (Purchasing)
M_LFM1_EKO	Purchasing Organization in Vendor Master Record
M_LIBE_EKO	Vendor Evaluation
M_LPET_BSA	Document Type in Scheduling Agreement Delivery Schedule
M_LPET_EKG	Purchasing Group in Scheduling Agreement Delivery Schedule
M_LPET_EKO	Purchasing Org. in Scheduling Agreement Delivery Schedule
M_LPET_WRK	Plant in Scheduling Agreement Delivery Schedule
M_LPET_LGO	Storage Location in Scheduling Agreement Delivery Schedule
M_ORDR_EKO	Purchasing Organization in Source List
M_ORDR_WRK	Plant in Source List
M_QUOT_EKO	Purchasing Organization (Quotas)
M_QUOT_WRK	Plant (Quotas)
M_RAHM_BSA	Document Type in Outline Agreement
M_RAHM_EKG	Purchasing Group in Outline Agreement
M_RAHM_EKO	Purchasing Organization in Outline Agreement

Authorization Object	Description
M_RAHM_WRK	Plant in Outline Agreement
M_RAHM_LGO	Storage Location in Outline Agreement
M_RAHM_STA	Status in Contract
M_SRV_LS	Authorization for Maintenance of Service Master
M_SRV_LV	Authorization for Maintenance of Model Serv. Specifications
M_SRV_ST	Authorization for Maintenance of Standard Service Catalog
M_SES_EKG	Purchasing Group in Service Entry Sheet
M_SES_EKO	Purchasing Organization in Service Entry Sheet
M_SES_WRK	Plant in Service Entry Sheet
S_ME_SYNC	Mobile Engine: Synchronization of Offline Applications
V_KONH_EKO	Purchasing Organization in Master Condition
M_TEMPLATE	Create/Change/Delete Public Templates
M_POIVVEND	Read Invoices of a Vendor
CMM_MEV_WL	CMM: Worklist
CMM_MEV_AD	CMM: Accrual Document
M_RECH_BUK	Invoices: Company Code
M_RECH_CPY	Copy Invoice: Company Code
M_RECH_WRK	Invoices: Plant
M_RECH_AKZ	Invoices: Accept Invoice Verification Differences Manually
M_RECH_EKG	Invoice Release: Purchasing Group
M_RECH_SPG	Invoices: Blocking Reasons
M_RECH_UPL	Invoice: Upload
M_RECH_WF	Invoice: Workflow
F_BKPF_BUK	Accounting Document
M_CCTR_BSA	Purchasing Document Type in Central Purchase Contract
M_CCTR_EKG	Purchasing Group in Central Purchase Contract

Authorization Object	Description
M_CCTR_EKO	Purchasing Organization in Central Purchase Contract
M_CR_WERKS	Plant and Company Code in Central Purchase Requisition of Connected System
M_HUB_WGR	Material Groups for Central Purchasing
M_HUB_MAT	Materials for Central Purchasing
M_HUB_MAR	Material Types for Central Purchasing
M_LFA1_GEN	Vendor: Central Data for Central Purchasing
M_LFA1_GRP	Vendor: Account Group Authorization for Central Purchasing
M_LFA1_BEK	Vendor: Account Authorization for Central Purchasing
M_CPR_BSA	Document Type in Central Purchase Requisition
M_CPR_WRK	Plant in Central Purchase Requisition
M_CPR_EKG	Purchasing Group in Central Purchase Requisition
M_CPR_EKO	Purchasing Organization in Central Purchase Requisition
M_CPO_BSA	Document Type in Central Purchase Order
M_CPO_EKO	Purchasing Organization in Central Purchase Order
M_CPO_EKG	Purchasing Group in Central Purchase Order
M_CPO_WRK	Plant in Central Purchase Order
V_KOND_VEA	Activity in Master Conditions

13.8.2 Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

Materials Management saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by Materials Management and for which programs these file names and paths apply:

Logical File Names Used

The following logical file names have been created in order to enable the validation of physical file names:

- MM_PURCHASING_INFORECORDS_NEW
 - Programs using this logical file name and parameters used in this context:
 - RM06IBIS
 - RM06IBIE
- MM_PURCHASING_REQUISITIONS_NEW
 - Programs using this logical file name:
 - RM06BBIS
 - RM06BBIE
- SAP_SOURCING_CUSTOMIZING_DOWNLOAD_FILE
 - Programs using this logical file name:
 - BBP_ES_CUST_DOWNLOAD

Logical Path Names Used

The logical file names MM_PURCHASING_INFORECORDS_NEW and MM_PURCHASING_REQUISITIONS_NEW use the logical file path MM_PUR_ROOT. The logical file name SAP_SOURCING_CUSTOMIZING_DOWNLOAD_FILE uses the logical file path SAP_SOURCING_CUSTOMIZING_DOWNLOAD.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To add the aliases for the view V_FILEALIA, use transaction SM31.

For more information, see about data storage security, see the respective chapter in the ABAP Platform Security Guide.

Using Data Storage Security

Check whether the conditions are classified as sensitive data. You can protect conditions with the following authorization objects:

Authorization Object	Description
V_KONH_EKO	Purchasing Organization in Master Condition
V_KONH_VKS	Condition: Authorization for Condition Types

Prices are also potential sensitive data. You can protect the display authority for prices with the value 09 of the authorization field `ACTVT` (Activity) of the purchasing document-specific authorization objects listed below:

Authorization Object	Description
M_ANFR_BSA	Document Type in RFQ
M_ANFR_EKG	Purchasing Group in RFQ
M_ANFR_EKO	Purchasing Organization in RFQ
M_ANGB_BSA	Document Type in Quotation
M_ANGB_EKG	Purchasing Group in Quotation
M_ANGB_EKO	Purchasing Organization in Quotation
M_BEST_BSA	Document Type in Order
M_BEST_EKG	Purchasing Group in Purchase Order
M_BEST_EKO	Purchasing Organization in Purchase Order
M_BEST_WRK	Plant in Purchase Order
M_BEST_LGO	Storage Location in Purchase Order
M_LPET_BSA	Document Type in Scheduling Agreement Delivery Schedule
M_LPET_EKG	Purchasing Group in Scheduling Agreement Delivery Schedule
M_LPET_EKO	Purchasing Org. in Scheduling Agreement Delivery Schedule
M_RAHM_BSA	Document Type in Outline Agreement
M_RAHM_EKG	Purchasing Group in Outline Agreement
M_RAHM_EKO	Purchasing Organization in Outline Agreement

Authorization Object	Description
M_RAHM_WRK	Plant in Outline Agreement
M_RAHM_LGO	Storage Location in Outline Agreement

13.8.3 Other Security-Relevant Information

Open Catalog Interface

Use

The Open Catalog Interface (OCI) incorporates external product catalogs into SAP S/4HANA applications using Hyper Text Transfer Protocol (HTTP). This way, the data required to create purchasing document items in SAP S/4HANA can be transferred directly from the external catalog to the SAP S/4HANA application.

Reason and Prerequisites

SAP S/4HANA and the catalog communicate via HTTP/HTTPS URL parameters. It is possible for an end user to identify these parameters and also change them using specialized tools. Security depends heavily on the fact whether the catalogue system resides before or behind the firewall.

Solution

SAP recommends the following to the customers who wish to integrate SAP S/4HANA and catalogs using Open catalog Interface (OCI):

- Double check the values transferred from the catalogue into the SAP S/4HANA application manually. Check whether the values are the same one as the one in the catalogue.
- In addition to that, authority checks are happening on SAP S/4HANA side: the application checks whether the user is allowed to change the data on SAP S/4HANA side which is transferred from the catalogue. Example: if a price is transferred from the catalogue into the purchasing document, the system checks whether the user has the authority to change the price in the purchasing document in general.
- To prevent end users from sniffing the catalog login data (User names, password), avoid specifying the login information in the OCI Catalog configuration in Customizing. Instead, configure the catalog to accept individual user authentication information from the end user. This can be done in the form of SSO (Single Sign-On) tools, Digital Certificates or Individual Login Information (User name/password). These features are dependent upon whether the Catalog provider supports the above mentioned features to logon.

You define the setting for the OCI in Customizing for [Materials Management](#) under [Purchasing](#) [Environment Data](#) [Web Services: ID and Description](#).

Security-Relevant Logging and Tracing

Use

Purchasing uses change documents to track changes made to purchasing documents. This includes changes to security-sensitive data such as prices. The following authorization objects specific to purchasing documents

allow the restriction of the visibility of those change documents using the value 08 of the authorization field ACTVT (Activity):

Authorization Object	Description
M_ANFR_BSA	Document Type in RFQ
M_ANFR_EKG	Purchasing Group in RFQ
M_ANFR_EKO	Purchasing Organization in RFQ
M_ANFR_WRK	Plant in RFQ
M_ANFR_LGO	Storage Locations in RFQ
M_ANGB_BSA	Document Type in Quotation
M_ANGB_EKG	Purchasing Group in Quotation
M_ANGB_EKO	Purchasing Organization in Quotation
M_BANF_BSA	Document Type in Purchase Requisition
M_BANF_EKG	Purchasing Group in Purchase Requisition
M_BANF_EKO	Purchasing Organization in Purchase Requisition
M_BANF_FRG	Release Code in Purchase Requisition
M_BANF_WRK	Plant in Purchase Requisition
M_BANF_LGO	Storage Location in Purchase Requisition
M_BEST_BSA	Document Type in Order
M_BEST_EKG	Purchasing Group in Purchase Order
M_BEST_EKO	Purchasing Organization in Purchase Order
M_BEST_WRK	Plant in Purchase Order
M_BEST_LGO	Storage Location in Purchase Order
M_EINF_EKG	Purchasing Group in Purchasing Info Record
M_EINF_EKO	Purchasing Organization in Purchasing Info Record
M_EINF_WRK	Plant in Purchasing Info Record
M_LFM1_EKO	Purchasing Organization in Vendor Master Record
M_LPET_BSA	Document Type in Scheduling Agreement Delivery Schedule

Authorization Object	Description
M_LPET_EKG	Purchasing Group in Scheduling Agreement Delivery Schedule
M_LPET_EKO	Purchasing Org. in Scheduling Agreement Delivery Schedule
M_ORDR_EKO	Purchasing Organization in Source List
M_ORDR_WRK	Plant in Source List
M_QUOT_EKO	Purchasing Organization (Quotas)
M_QUOT_WRK	Plant (Quotas)
M_RAHM_BSA	Document Type in Outline Agreement
M_RAHM_EKG	Purchasing Group in Outline Agreement
M_RAHM_EKO	Purchasing Organization in Outline Agreement
M_RAHM_WRK	Plant in Outline Agreement
M_RAHM_LGO	Storage Location in Outline Agreement
M_RAHM_STA	Status in Contract

13.8.4 Deletion of Personal Data

Use

Purchasing (MM-PUR), *Invoice Verificaton* (MM-IV), and *Supplier and Category Management* might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data.

Business partner master data can be blocked as soon as business activities that use this data are completed and the residence period for the data has elapsed; after this time, only users with additional authorizations can access this data.

Depending on the type of business documents, authorized users have to use either a Fiori app or an *Advanced* or *Professional* Fiori app to access the document. The following table gives you an overview of what to use for the business documents of Sourcing and Procurement.

Type of Business Document	Display Option for Blocked Documents
<ul style="list-style-type: none"> • Service entry sheet • Request for quotation • Supplier quotation • Quota arrangement • Supplier invoice 	<ul style="list-style-type: none"> • Using the Fiori apps
<ul style="list-style-type: none"> • Purchase requisition • Purchase order • Scheduling agreement • Purchase contract • Shopping cart • Purchasing info record 	<ul style="list-style-type: none"> • Using the "Advanced" or "Professional" Fiori apps

In apps of **Supplier and Category Management**, all entries related to blocked suppliers are displayed as *Blocked Supplier*, and all supplier-related links are disabled. Evaluation scorecards for the blocked suppliers are not displayed in the scorecards list in the *Display Scorecards* app. The standard Web Dynpro apps can be used to display the blocked data. For more information, see the section [► Supplier and Category Management ► Deletion of Personal Data ►](#).

When the retention period for data expires, personal data of the business partner can be destroyed completely so that it can no longer be retrieved. Retention periods must be defined in the customer system.

For more information about blocking of data, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 [► Product Assistance ► Cross Components ► Data Protection ►](#).

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
Purchase Requisitions	Archiving Purchase Requisitions (MM-PUR)	Archiving object MM_EBAN
Purchasing Documents	Archiving Purchasing Documents (MM-PUR)	Archiving object MM_EKKO
Purchasing Info Records	Archiving Purchasing Info Records (MM-PUR)	Archiving object MM_EINA
Invoice Documents	Archiving Invoice Documents (MM-IV)	Archiving object MM_REBEL

Application Object	Detailed Description	Provided Deletion Functionality
Non-Ferrous Metals and Returnable Packaging Settlement	Business partner data is stored for non-ferrous rate determination, goods movement, and returnable packaging settlement	<p>You can delete by using the report /NFM/ILM_DEL_01. A where used check is done for the following tables:</p> <ul style="list-style-type: none"> • /NFM/TPROVMOV • /NFM/TVGW_TMP • /SAPMP/SD_LEIHG

For documentation about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under [▶ Product Assistance](#) [▶ Enterprise Business Applications](#) [▶ Sourcing and Procurement](#) [▶ Materials Management \(MM\)](#) [▶ Data Management in Sourcing and Procurement](#) [▶ Data Archiving in Materials Management \(MM\)](#) [▶](#).

Prerequisite: End of Purpose Check

Before objects can be archived, and end of purpose check must be performed.

Relevant Application and Available EoP Functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Materials Management (MM)	End of purpose check (EoP)	<p>For more information about the end of purpose check, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ▶ Product Assistance ▶ Enterprise Business Applications ▶ Sourcing and Procurement ▶ Materials Management (MM) ▶ Data Management in Sourcing and Procurement ▶ Blocking of Personal Data in Sourcing and Procurement ▶ Business Partner End of Purpose (EoP) Check in MM-PUR, MM-IM, and MM-IV ▶.</p>

Configuration of Simplified Blocking and Deletion

To use *SAP Information Lifecycle Management (ILM)* to simplify the deletion of application-specific personal data, you have to do the following:

- Activate the following business functions:
 - ILM-Based Deletion of Business Partner Data (BUPA_ILM_BF)

- ILM-Based Deletion of Customer and Supplier Master Data (ERP_CVP_ILM_1)
- Information Lifecycle Management (ILM)
- Perform the necessary customizing settings related to SAP Information Lifecycle Management (ILM) in Customizing for [▶ SAP NetWeaver ▶ Application Server ▶ Basis Services ▶ Information Lifecycle Management ▶](#).
- Perform the necessary customizing settings related to the blocking and deletion of business partner master data in Customizing for [▶ Cross-Application Components ▶ Data Protection ▶](#).
- Run transaction ILMARA and maintain and activate the required audit areas for the ILM objects of the application.
- Run transaction IRMPOL and maintain the required retention policies for the ILM objects of the application.
- Configure the settings related to the blocking and deletion of customer and supplier master data in Customizing under [▶ Logistics - General ▶ Business Partner ▶ Deletion of Customer and Supplier Master Data ▶](#).

See Also

For general information about the deletion of personal data, see the following chapters in the product assistance for SAP S/4HANA that is available on the SAP Help Portal at <http://help.sap.com/s4hana> <choose a release> [▶ Product Assistance ▶ Cross Components ▶](#):

- [SAP Information Lifecycle Management](#)
- [▶ Data Protection ▶ Deletion of Business Partner ▶ Customer and Supplier Master Data ▶](#)
- [▶ Data Protection ▶ Configuring Data Protection Features ▶ Activating Business Functions ▶](#)

13.8.5 Specific Read Access Log Configurations

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions.

SAP delivers sample configurations for applications.

Invoice Verification (MM-IV) logs data in order to track who has accessed the bank details in supplier invoices. You can find the configurations as described in the [Read Access Logging \[page 33\]](#) chapter.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Channel	Configuration	Fields Logged
Dynpro	Recording:	IBAN
	MM_IV/DPP_BANK	SWIFT
		BANKN
		BANKA

Channel	Configuration	Fields Logged
SAP Gateway	Service ID:	IBAN
	MM_SUPPLIER_INVOICE_MANAGE	SWIFT
		BANKN
		BANKA
RFC	Function modules:	ADDRESSDATA-BANK_ACCT
	BAPI_INCOMINGINVOICE_CHANGE	ADDRESSDATA-BANK_CTRY
	BAPI_INCOMINGINVOICE_CREATE	ADDRESSDATA-BANK_NO
	BAPI_INCOMINGINVOICE_CREATE1	
	BAPI_INCOMINGINVOICE_PARK	
	BAPI_INCOMINGINVOICE_SAVE	
	MRM_XMLBAPI_INCINV_CREATE	
RFC	Function modules:	ADDRESSDATA-BANK_ACCT
	BAPI_INCOMINGINVOICE_GETDETAIL	ADDRESSDATA-BANK_CTRY
	MRM_XMLBAPI_INCINV_GETDETAIL	ADDRESSDATA-BANK_NO
RFC	Function module:	DOC_HEADER_LIST[]-BANKL
	MRM_INVOICE_GETLIST	DOC_HEADER_LIST[]-BANKN
		DOC_HEADER_LIST[]-BANKS
Web Service	Interface name:	SupplierInvoice/BillFromParty/Bank-AccountID
	SupplierInvoiceERPByIDQueryResponse_In	SupplierInvoice/BillFromParty/Bank-AccountStandardID
		SupplierInvoice/BillFromParty/BankInternalID
		SupplierInvoice/BillFromParty/Bank-Name

The following apps of MM-IV are affected:

- [Enter Invoice](#) (MIRO)
- [Park Invoice](#) (MIR7)
- [Display Invoice Document](#) (MIR4)
- [Enter Invoice for Invoice Verification in Background](#) (MIRA)

The following Fiori apps are affected:

- [Manage Supplier Invoices](#)
- [Create Supplier Invoice \(Advanced\)](#)

13.8.6 Ariba Network Integration

If you want to use integration scenarios with the Ariba Network, see chapter “Business Network Integration” at the end of this guide.

13.8.7 Supplier Management

13.8.7.1 Authorizations

Supplier Management uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

i Note

For more information about how to create roles, see the *ABAP Platform Security Guide* under *User Administration and Authentication*.

Front-End Roles

To use the Fiori Launchpad in SAP S/4HANA, you have to apply the SAP S/4HANA role concept based on business catalogs that are assigned to business roles. For the front-end, the following standard business roles are available for Sourcing and Procurement. You can use these roles as templates for your own roles. For more information, see *SAP Fiori Overview*.

Back-End Roles

In the back-end, you have to create roles in transaction PFCG and assign business catalogs to the roles. For more information, go to https://help.sap.com/s4hana_op_2020, enter *Creating Authorization Roles for Catalogs* into the search bar, press , and open the search result with that title. In addition, manual actions are required.

i Note

- Each user has to be assigned to a business partner to have access to the Supplier Management apps. You create a business partner role in the transaction *Maintain HR Master Data* and assign it to a user in the transaction *User Maintenance*.
- If you delete a user, the business partner for this user can no longer be used either.

Authorization Objects Specific to Supplier Management

The table below shows the security-relevant authorization objects that are specific to Supplier Management:

Authorization Object	Field	Value	Description
/SRMSMC/DB	ACTVT	Reload	<p>Enables users to initiate a download of up-to-date data from D&B. Since downloading data from D&B is subject to charges, you should assign this role only to employees who are aware of this implication.</p> <p>Enables users to interact with an instance of a business object of Supplier Management in a specific way. The authorization object is used in the /SRMSMC/DNB_REQUESTOR role.</p>
/SRMSMC/BO	/BOFU/BO	/SRMSMC/BO_QNR (Questionnaire) /SRMSMC/BO_SEP (Supplier Evaluation Profile) /SRMSMC/BO_SES (Supplier Evaluation Scorecard) /SRMSMC/BO_SEV (Supplier Evaluation) /SRMSMC/BO_SRS (Supplier Evaluation Response) /SRMSMC/MO_PUC (Purchasing Category) /SRMSMC/MO_QLIB (Question Library) /SRMSMC/BO_ACT (Activity) /SRMSMC/BO_TSK (Task) /SRMSMC/MO_BUPA	<p>As the type of business object that the user can access, you can specify the values listed.</p>

Authorization Object	Field	Value	Description
/SRMSMC/AM	ACT_TYP	Customizing, activity type	This authorization object is used to define authorization settings for accessing activities in SAP Supplier and Category Management.

13.8.7.2 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For Supplier Information and Master Data, the following services are needed:

- /sap/bc/ui5_ui5/sap/slc_qnr_resps1
- /sap/bc/ui5_ui5/sap/slc_eval_resps1
- /sap/bc/ui5_ui5/sap/slc_sup_evals1
- /sap/bc/webdynpro/srmsmc/WDA_I_BP_SUPPLIER
- /sap/bc/webdynpro/srmsmc/WDA_I_QNR_OVP
- /sap/bc/webdynpro/srmsmc/WDA_I_SEP_OVP
- /sap/bc/webdynpro/srmsmc/WDA_I_SES
- /sap/bc/webdynpro/srmsmc/WDA_I_SEV_OVP
- /sap/opu/odata/sap/slc_questionnaire_response_srv
- /sap/opu/odata/sap/C_SUPLREVALRSPEVALUATEST_CDS
- /sap/opu/odata/sap/C_SUPLREVALRESPST_CDS
- /sap/bc/webdynpro/srmsmc/wda_puc
- /sap/bc/webdynpro/srmsmc/wda_puc_t
- /sap/bc/webdynpro/srmsmc/WDA_QLB_OVP_MAIN
- /sap/bc/webdynpro/srmsmc/WDA_QLB_OVP_TRNS
- /sap/bc/webdynpro/srmsmc/WDA_QNR_OVP_TRNS
- /sap/bc/webdynpro/srmsmc/wda_sep_ovp_trns
- /sap/bc/webdynpro/srmsmc/wda_act
- /sap/bc/webdynpro/srmsmc/wda_tsk

Use the transaction SICF to activate these services.

For more information about ICF security, see the respective chapter in the ABAP Platform Security Guide.

13.8.7.3 Data Storage Security

Cookies

Supplier Information and Master Data uses a Web Dynpro user interfaces. The SAP Web AS must issue cookies and accept them.

Attachments

You restrict the allowed MIME types and the file size of attachments. You do this in Customizing for Materials Management under [Purchasing > Supplier and Category Management](#) for all business processes you want to use. You can do this in the following Customizing activities:

- [Define MIME Types for Attachments](#)
- [Define Maximum Size for Attachments](#)

The above listed activities are available under each of the business processes nodes in Customizing.

For information about virus scanning for attachments, see [Virus Scanning \[page 24\]](#) and [Application-Specific Virus Scan Profile \(ABAP\) \[page 668\]](#).

Security-Relevant Logging and Tracing

Supplier Management uses change documents to track changes made to supplier evaluation responses, supplier evaluation scorecards, supplier's control data and supplier's sustainability data. You can display change documents as follows:

- Open transaction RSSCD100.
- In the *Object Class* field enter the value from the table that is relevant for the business object you are looking for:

Object Classes per Business Object

Object Class	Business Object
/SRMSMC/S_SUST	Supplier's Sustainability Data
/SRMSMC/S_CTRL	Supplier's Control Data
/SRMSMC/SES	Supplier Evaluation Scorecard
/SRMSMC/SRS	Supplier Evaluation Response

Registering the Change Document Object for Application Business Object

1. In the SAP development system, enter the transaction SPRO.
2. Choose *SAP Reference IMG*.
3. Navigate to **► SAP Customizing Implementation Guide ► Cross-Application Components ► Processes and Tools for Enterprise Applications ► Reusable Objects and Functions for BOPF Environment ► Maintain BO-Specific Change Document Objects ►**.
4. Choose *IMG Activity* button.
5. Choose *Continue* in the dialog box.
6. Choose *New Entries* in the *Change Documents Adaptor: BO Specific Settings* overview window.
7. Enter the business object.
8. Enter the change document.
9. Enter the change document call back class.
10. Save your entries.

Related Information

- Go to https://help.sap.com/s4hana_op_2020, enter *Services for Application Developers* into the search bar, press , open the search result with that title, and navigate to *Change Documents*.
- Go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press , open the search result with that title, and navigate to *Auditing and Logging*.

13.8.7.4 Application-Specific Virus Scan Profile (ABAP)

SAP provides an interface for virus scanners to prevent manipulated or malicious files from damaging the system. To manage the interface and what file types are checked or blocked, there are virus scan profiles. Different applications rely on default profiles or application-specific profiles.

The Web Dynpro user interfaces of Supplier Information and Master Data require that you activate the virus scan profile `/SIHTTP/HTTP_UPLOAD`.

You must make the settings for the virus scan profile in Customizing for Materials Management under **► Purchasing ► Supplier and Category Management ► Virus Scan Interface ►**

For more information about virus scanning, see [Virus Scanning \[page 24\]](#).

13.8.7.5 Deletion of Personal Data

Use

Supplier and Category Management might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at <http://help.sap.com/s4hana> > > <choose your current on-premise release> > *Product Assistance* > *Cross Components* > *Data Protection* > .

Relevant Application Objects and Available EoP/WUC functionality

Supplier and Category Management uses the standard archiving and deletion functions that are available for the business partner functionality. Therefore, there is no dedicated end of purpose check (EoP) nor a where-used check (WUC) for Supplier and Category Management.

Supplier and Category Management in SAP S/4HANA doesn't maintain an own data model in the IRF. An exit was implemented and registered at the table cluster CA_APMDBP_DETAILS instead. This way, any object in Supplier and Category Management that contains personal data of a given subject will be listed in a normal run of the tool.

Application	Provided Deletion Functionality
Supplier and Category Management	Transaction used for deletion: SARA Archiving object relevant for deletion: CA_BUPA

For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at <http://help.sap.com/s4hana> > > <choose your current on-premise release> > *Product Assistance* > *Cross Components* > *Data Protection* > *Archiving* > .

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of customer and supplier master data in Customizing under > *Logistics General* > *Business Partner* > *Deletion of Customer and Supplier Master Data* > .

Display of Blocked Suppliers

If suppliers have been blocked, they can no longer be used in any Supplier and Category Management WebDynpro applications. The supplier data is not deleted, but it is no longer visible. Any supplier-related

entries are displayed as *Blocked Supplier* and all supplier-related links are disabled. Evaluation scorecards for the blocked suppliers are not displayed in the scorecards list in the *Display Scorecards* app.

This change is relevant for the following apps:

- Manage Activities
- Monitor Tasks
- Manage Templates

Supplier blocking via CDS view functions in the following apps:

- Manage Purchasing Categories
- Display Scorecards
- Quick Create for Procurement-Related Activities
- Open Activities card on the Procurement Overview Page
- Monitor Responses
- Evaluate Suppliers
- Monitor Responses

13.8.8 Integration

13.8.8.1 SAP S/4HANA Procurement Hub Integration

SAP S/4HANA currently supports integration with the SAP ERP back-end systems.

13.8.8.1.1 Direct Connectivity

The SAP S/4HANA hub system communicates with the connected SAP ERP back-end systems through XML messages using peer-to-peer connectivity options in an asynchronous mode.

13.8.8.1.2 Mediated Connectivity

For mediated connectivity, the SAP S/4HANA hub system is connected through SAP Process Integration. The communication with the connected SAP ERP back-end systems is performed through XML messages in asynchronous mode.

13.8.8.1.3 Roles and Authorizations in the SAP S/4HANA Hub System

To process messages coming from the SAP ERP back-end systems, a technical user is needed in the SAP S/4HANA hub system.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. To maintain roles for ABAP technology, you use the profile generator (transaction PFCG).

Note

For more information about creating roles, see Role Maintenance.

The table below shows the security-relevant authorization objects that the technical user needs:

Roles and Authorizations in the SAP S/4HANA Hub System

Authorization Object	Field	Value	Description
S_RFC	RFC_TYPE	Function Module	Type of RFC object for which access is to be allowed
	RFC_NAME	/IWNGW/ FM_IN_CREATE_NOTIF	Name of RFC object for which access is allowed
		/IWNGW/ FM_IN_DELETE_NOTIF	
	ACTVT	Execute	Activity
S_SERVICE	SRV_NAME	WS PURCHASEREQUISITION REPLICATIO3/ PURCHASE_REQUISITIO N_REPLICATI	Program, transaction, or function module name
		WS PURCHASEREQUISITION REPLICATION/ PURCHASE_REQUISITIO N_REPLICATI	
		WS PURCHASEREQUISITION SOURCINGNO1/ PURCHASE_REQUISITIO N_SOURCING	

Authorization Object	Field	Value	Description
/AIF/PROC	SRV_TYPE	Hash Value for External Service	Type of check flag and authorization for default values
	ACTVT	Import, Export, Resubmit	Activity
	/AIF/NS	/MMHUB	Namespace
	/AIF/IF	PRRECOIN, PRSRCNOTIN	Interface Name
	/AIF/IFVER	*	Interface Version
	/AIF/VNS	*	Variant Namespace
	/AIF/VNAME	*	Name of Interface Variant

13.8.8.1.4 Roles and Authorizations in the SAP ERP Back-end System

You can activate Forward Error Handling (FEH) to monitor and process purchase requisitions that fail to copy be copied to the SAP ERP back-end system.

Users that process entries in FEH need specific authorizations assigned to their users , as well as the following authorization objects:

Authorization Object	Description
S_FEH_INTF	<i>Interface-specific authorization for FEH</i>
/SAPPO/FLT	<i>Postprocessing Order Filter</i>
/SAPPO/ORD	<i>Postprocessing Order (DISPLAY and EDIT)</i>
/SAPPO/WLA	<i>Assignment of Worklist</i>

13.9 Supply Chain

13.9.1 Inventory

13.9.1.1 Inventory Management

13.9.1.1.1 Deletion of Personal Data

Use

The *Materials Management* application might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
Material Documents	Archiving Material Documents (MM-IM)	Archiving object MM_MATBEL
Physical Inventory Documents	Archiving Physical Inventory Documents (MM-IM)	Archiving object MM_INVBEL
Special Stocks	Archiving Special Stock Records (LO-MD-MM)	Archiving object MM_SPSTOCK
Empties Management	Archiving of Empties Update	Archiving object BEV1_EMFD

Relevant Application Areas and Available EoP Functionality

Application	Implemented Solution	Further Information
<i>Materials Management (MM)</i>	End of purpose check (EoP)	<p>This includes the business in the areas of:</p> <ul style="list-style-type: none"> • External Services Management (MM-SRV) • Inventory Management (MM-IM) • Logistics Invoice Verification (MM-IV) • Empties Management (MM-PUR-EM) <p>For more information about the end of purpose check, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ▶ Product Assistance > Enterprise Business Applications > Supply Chain > Data Management in Supply Chain > Inventory Management and Inventory (MM-IM) > Blocking of Personal Data in Inventory Management > Business Partner End of Purpose (EoP) Check in MM-PUR, MM-IM, and MM-IV ▶.</p>

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management in Customizing for Cross-Application Components under [▶ Data Protection](#) > [Authorization Management](#) ▶. For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for *Cross-Application Components* under [▶ Data Protection](#) > [Blocking and Unblocking](#) > [Business Partner](#) ▶.

13.9.1.2 Direct Store Delivery

13.9.1.2.1 Deletion of Personal Data

Use

The *Direct Store Delivery* application might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
Visit List	Archiving Visit Lists (LE-DSD)	Archiving object /DSD/VL
Settlement Documents	Archiving Settlement Documents (LE-DSD)	Archiving object /DSD/SL
DEX	Archiving DEX Streams (LE-DSD)	Archiving object /DSD/DEX
Route Settlement	Data destruction in Route Settlements (LE-DSD)	Destruction object /DSD/HH_RAHD_DESTRUCTION
DSD Connector	Data destruction in DSD Connector (LE-DSD)	Destruction object /DSD/ME_TOUR_HD_DESTRUCTION
DSD Loading	Data destruction in DSD Loading (LE-DSD)	Destruction object /DSD/SV_LC_HD_DESTRUCTION
Visit Plan	Data destruction in Visit Plants (LE-DSD)	Destruction object /DSD/VC_VPH_DESTRUCTION
Deal Conditions	Data destruction in Deal Conditions (LE-DSD)	Destruction object /DSD/PR_HEAD_DESTRUCTION

Relevant Application Objects and Available EoP Functionality

Application	Implemented Solution (EoP or WUC)	Further Information
<i>Logistics Execution</i> (LE)	EoP check	This includes the business in the areas of: <ul style="list-style-type: none"> Direct Store Delivery (Backend) (LE-DSD)

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management in Customizing for Cross-Application Components under ► *Data Protection* ► *Authorization Management* ». For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for *Cross-Application Components* under ► *Data Protection* ► *Blocking and Unblocking* ► *Business Partner* ».

13.9.1.3 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For Logistics Execution, the following services are needed:

- LECI
- VL31W
- VL32W
- VLPODW1
- VLPODW2

Use the transaction SICF to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information about ICF security, see the respective chapter in the ABAP Platform Security Guide.

13.9.1.4 Deletion of Personal Data in Batch Management

Use

The *Batch Management* application might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ».

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Batch Master	Archiving Batch Master Records (LO-BM)	Archiving object LO_BATCH
Batch Where-Used	Archiving Batch Where-Used Records (LO-BM-WUL)	Archiving object LO_CHVW

Relevant Application Objects and Available End of Purpose (EoP) functionality

Application	Implemented Solution	Further Information
Batch Management (LO-BM)	End of purpose check (EoP)	For more information about the end of purpose check, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► <i>Product Assistance</i> ► <i>Enterprise Technology</i> ► <i>Data Archiving (CA-ARC)</i> ► <i>Logistics General (LO)</i> ► <i>Data Archiving in Batch Management (LO-BM)</i> ► <i>Business Partner End of Purpose (EoP) Check in Batch Management</i> ►

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management in Customizing for Cross-Application Components under ► *Data Protection* ► *Authorization Management* ►. For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for *Cross-Application Components* under ► *Data Protection* ► *Blocking and Unblocking* ► *Business Partner* ►.

13.9.1.5 Returnable Packaging and Empties Management

13.9.1.5.1 Deletion of Personal Data (Returnable Packaging Logistics)

Use

Returnable Packaging Logistics might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Returnable Packaging Logistics (IS-A-RL)	Archiving Object
	VHURL_AC
	VHURL_CP
	VHURL_PO
	VHURL_ST
	VHURL_TR
	Destruction Objects
	VHURL_CP_DESTRUCTION
	VHURL_RR_DESTRUCTION
	ILM Objects
	VHURL_AC
	VHURL_PO
	VHURL_ST
	VHURL_TR
	VHURL_CP_DEST
	VHURL_RR_DEST

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Returnable Packaging Logistics (IS-A-RL)	EoP check	Checks tables: RLACCT, RLPShPA, RLPShP

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components*→*Data Protection*→*Blocking and Unblocking of Data*→*Customer Master/Supplier Master Deletion*.

13.9.1.5.2 Recycling Administration

13.9.1.5.2.1 Authorizations in Recycling Administration

Recycling Administration uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the Application Server ABAP Security Guide also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used by Recycling Administration.

Role	Description
SAP_EP_ISREA_CM	Automatic Role to display ABAP applications for contract handling
SAP_EP_ISREA_DEC	Automatic Role to display ABAP applications for declarations
SAP_EP_ISREA_INFO	Automatic Role to display ABAP applications for the information system
SAP_EP_ISREA_MD	Automatic Role to display ABAP applications for master data management
SAP_ISREA_COMPLIANCE_MANAGER	<i>Compliance Manager for Recycling</i>
SAP_ISREA_HEAD_SUSTAINABILITY	<i>Head of Sustainability and Environment</i>
SAP_ISREA_MASTERDATA_EXPERT	<i>Specialist for Recycling Master Data</i>
SAP_ISREA_PACKAGING_ENGINEER	<i>Packaging Engineer</i>
SAP_ISREA_SPECIALIST	<i>Specialist for Recycling Accounting</i>

Role	Description
com.sap.pct.erp.rea.financial_accountant	SAP Enterprise Portal role <i>Financial Accountant</i>
com.sap.pct.erp.rea.person_responsible_master_data	SAP Enterprise Portal role <i>Person Responsible Master Data</i>
com.sap.pct.erp.rea.superadmin_masterdata	SAP Enterprise Portal role <i>Superadministrator Master Data</i>
com.sap.pct.erp.rea.compliance_manager	SAP Enterprise Portal role <i>Compliance Manager</i>
SAP_SR_REA_COMP_MAN_5	Role in SAP Business Client that corresponds to the SAP Enterprise Portal role Compliance Manager
SAP_SR_REA_FIN_ACCOUNTANT_5	Role in SAP Business Client that corresponds to the SAP Enterprise Portal role <i>Financial Accountant</i>
SAP_SR_REA_PERS_RESP_MD_5	Role in SAP Business Client that corresponds to the SAP Enterprise Portal role <i>Person Responsible Master Data</i>
SAP_SR_REA_SUPER_ADMIN_MD_5	Role in SAP Business Client that corresponds to the SAP Enterprise Portal role <i>Superadministrator Master Data</i>

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by Recycling Administration.

Authorization Object	Name	Description
/J7L/LDE	<i>REA Lean Data Entry</i>	Controls the authorizations for the applications for lean data entry
J_7L_CONF	<i>REA: Authorization for Configuration</i>	Controls the authorizations for the import and export of recycling partner master data
J_7L_VARIA	<i>REA: Authorization for Variants</i>	Controls the access to master data objects in the Recycling Administration component depending on the respective variant
J_7L_CUST	<i>REA: Customizing</i>	Controls the authorizations for Customizing in the Recycling Administration component

Authorization Object	Name	Description
J_7L_INFO	<i>REA: Information System</i>	Controls the authorizations for the applications in the information system of the Recycling Administration component
J_7L_PERIO	<i>REA: Declarations to Recycling Partners</i>	Controls the authorizations for declarations
J_7L_INFNC	<i>REA: Interfaces and Batch Programs</i>	Controls the authorizations for programs for mass processing (background processing)
J_7L_STAMM	<i>REA: Master Data</i>	Controls the authorizations for editing master data in the Recycling Administration component

13.9.1.5.2.2 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that *Recycling Administration* provides to support compliance with the relevant legal requirements and data privacy.

i Note

Recycling Administration (IS-REA) is integrated in the central ILM check processes. If you use REA, the central ILM check processes also take the REA specific privacy related data (supplier, customer) into account. Only when REA reports back that this data is no longer used within this component, the system can block the corresponding REA data.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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 given system landscape and the applicable legal requirements.

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.

13.9.1.5.2.2.1 Deletion of Personal Data

Use

The *Recycling Administration* application might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
REA Declaration	Archiving REA declarations in the Recycling Administration component	Archiving object /J7L/DECL

Relevant Application Areas and Available EoP Functionality

Application	Implemented Solution	Further Information
<i>Supply Chain</i>	End of purpose check (EoP)	<p>This includes the business in the area of:</p> <ul style="list-style-type: none"> Recycling Administration (IS-REA) <p>For more information about the end of purpose check, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► <i>Product Assistance</i> ► <i>Enterprise Business Applications</i> ► <i>Supply Chain</i> ► <i>Logistics - General (LO)</i> ► <i>Returnable Packaging and Empties Management</i> ► <i>Recycling Administration</i> ► <i>Data Management in Recycling Administration</i> ► <i>Blocking of Personal Data in Recycling Administration</i> ► <i>Business Partner End of Purpose (EoP) Check in Recycling Administration</i> ►.</p>

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management in Customizing for Cross-Application Components under [▶ Data Protection ▶ Authorization Management ▶](#). For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for *Cross-Application Components* under [▶ Data Protection ▶ Blocking and Unblocking ▶ Business Partner ▶](#).

13.9.2 Delivery and Transportation

13.9.2.1 Deletion of Personal Data in Delivery Management (LE-SHP)

Use

Delivery Management might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 [▶ Product Assistance ▶ Cross Components ▶ Data Protection ▶](#).

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Deliveries	Archiving object RV_LIKP
Check-In Data of Means of Transport and Visitors	Data destruction object LE_SHP_LECI_DESTRUCTION

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Sales (SD_ERP)	EoP check	For more information about the end of purpose check, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ▶ <i>Product Assistance</i> ▶ <i>Enterprise Business Applications</i> ▶ <i>Supply Chain</i> ▶ <i>Logistics Execution</i> ▶ <i>Delivery Management (LE-SHP)</i> ▶ <i>Data Management in Delivery Management</i> ▶ <i>Blocking and Deletion of Personal Data in Delivery Management</i> ▶ <i>Business Partner End of Purpose (EoP) Check in Delivery Management (LE-SHP)</i> ▶

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of customer and supplier master data in Customizing under ▶ *Logistics* ▶ *General* ▶ *Business Partner* ▶ *Deletion of Customer and Supplier Master Data* ▶.

You execute the rebuild of retention information in Customizing under ▶ *Sales and Distribution* ▶ *Data Transfer* ▶ *Data Aging and Archiving* ▶ *Archiving Data* ▶ *Rebuilding of Retention Information in SD* ▶.

You can enhance the EoP check in Customizing under ▶ *Sales and Distribution* ▶ *System Modifications* ▶ *Business Add-In* ▶ *BAdI: Enhancements for End of Purpose Check* ▶.

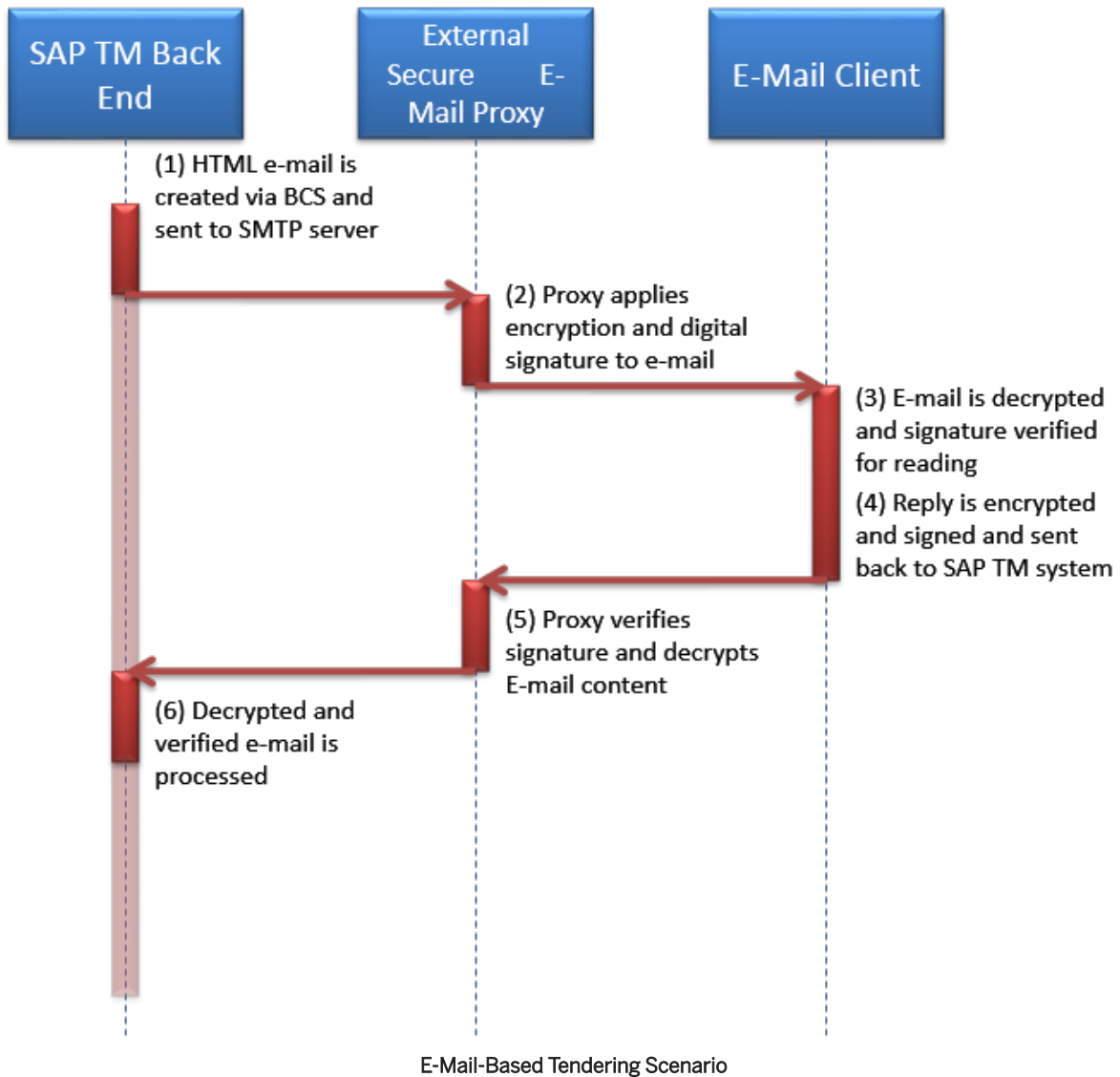
13.9.2.2 Transportation Management

This section of the Operations Guide for SAP S/4HANA, on-premise edition contains information on operations tasks specific to Transportation Management.

13.9.2.2.1 Security Aspects of Data, Data Flow and Processes

E-mail-Based Tendering Scenario

The figure below shows an overview of the e-mail based tendering scenario for Transportation Management (TM).



Steps for E-Mail Based Tendering Scenario

Step	Description	Security Measure
1	HTML e-mail is created via BCS and sent to SMTP server	In Customizing for TM, the use of encryption and digital signatures needs to be enabled. In Customizing for <i>Transportation Management</i> , choose Freight Order Management > <i>Tendering</i> > <i>Define General Settings for Tendering</i> > <i>03 – E-mail and SMS Content</i> > <i>E-Mail Security Settings</i> .

Step	Description	Security Measure
2	Proxy applies encryption and digital signature to e-mail	External secure e-mail proxy needs to be maintained and activated for the TM system. For more information, see SAP Note 149926 . Keys must be exchanged between the sender and recipient prior to sending the e-mail. We highly recommend that you set up the policy for the e-mail proxy in such a way that e-mails can be sent only if encryption and digital signatures are enabled. If this is not possible, for example, due to missing keys, e-mails must not be sent in an insecure way.
3	E-mail is decrypted and signature verified for reading	The e-mail client of the recipient must support encryption and digital signatures, and keys must have been exchanged beforehand by the sender and the recipient.
4	Reply is encrypted and signed and sent back to TM system	Refer to step 3
5	Proxy verifies signature and decrypts e-mail content	Refer to step 2
6	Decrypted and verified e-mail is processed	Not applicable

→ Recommendation

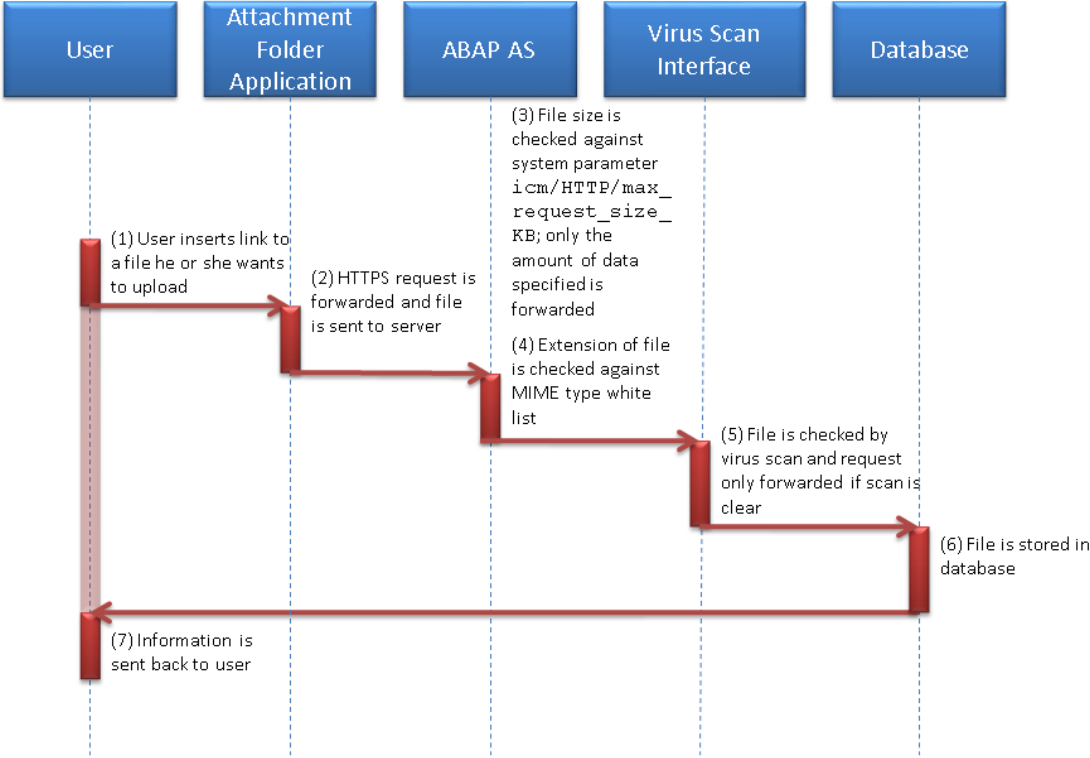
To access the TM system externally, we recommend that you define a system alias in the web dispatcher. The web dispatcher redirects the request to the correct hostname and port so that an external user can use a hyperlink, which contains the alias, to access the system.

You create a tendering notification e-mail in the TM system. The system sends this e-mail to the carrier with a hyperlink to the carrier's worklist in the TM system or in the TM collaboration portal. The hyperlink contains the system alias instead of the physical hostname and port. To use the alias, ensure that you have implemented SAP Note [1748036](#) or [1747651](#), and SAP Note [1783590](#). Subsequently, you need to specify the following settings in the TM system:

1. Create an alias in transaction *SM59*.
2. In the *Target Host* field, enter the system alias as specified in the web dispatcher.
3. Enter the alias in the *03 E-Mail and SMS Content* screen in Customizing for *Transportation Management* under **Freight Order Management > Tendering > Define General Settings for Tendering**.

File Upload Scenario

The figure below shows an overview of the file upload scenario for TM.



File Upload Scenario

The table below shows the security aspects to be considered for the process step and what mechanism applies.

Steps for File Upload Scenario

Step	Description	Security Measure
1	User inserts link to a file he or she wants to upload	User needs to be aware of the file he or she wants to upload
2	HTTPS request is forwarded and file is sent to server	Not applicable

Step	Description	Security Measure
3	File size is checked against system parameter <code>icm/HTTP/max_request_size_KB</code> ; only the amount of data specified is forwarded	<p>Maximum file size needs to be restricted to secure the server.</p> <p>For more information, go to https://help.sap.com/s4hana_op_2020, enter <i>Security Notes for FileUpload UI Elements</i> into the search bar, press <code>Enter</code>, and open the search result with that title.</p>
4	MIME type of file is checked against allowlist	<p>The extension of the uploaded file (but not its content) is checked against MIME type allowlist; as a prerequisite for using the allowlist, SAP Note 1514253 must be implemented.</p>
5	File is checked by virus scan and request only forwarded if scan is clear	<p>Virus scan needs to be active in your system.</p> <p>For more information, go to https://help.sap.com/s4hana_op_2020, enter <i>SAP Virus Scan Interface</i> into the search bar, press <code>Enter</code>, and open the search result with that title.</p> <p>We strongly recommend that you create a virus scan profile with linkage type <i>All steps successful</i>.</p>
6	File is stored in database	Not applicable
7	Information is sent back to user	Not applicable

Caution

Only file extensions are compared to the entries in the allowlist, not the content of the files.

The file upload function can be disabled to prevent users from uploading files to your system. To disable the file upload function, you must implement SAP Note [1514253](#). We recommend that you disable the upload function if it is not required by your business scenarios.

Always ensure that your virus scan is set up and working correctly before enabling file uploads. If your virus scan is not up and running, do not use the file upload.

For information about uploading TACT rates to TM, go to https://help.sap.com/s4hana_op_2020, enter *TACT Rate Upload* into the search bar, press `Enter`, and open the search result with that title.

13.9.2.2 Authorizations

Transportation Management (TM) uses the authorization concept provided by the Application Server ABAP. Therefore, the recommendations and guidelines for authorizations as described in the *Application Server ABAP Security Guide*, *Java Security Guide*, and *ABAP and Java Security Guides* also apply to TM.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF00`) on the AS ABAP and the User Management Engine's user administration console for the AS Java.

Role and Authorization Concept for Transportation Management

Authorization objects are delivered with TM. For more information about the authorization objects and how to use them, see the following section.

Standard Authorization Objects

For TM, there are two kinds of authorization objects:

- Static checks of the technical business objects along with their nodes and actions, or of organizational data objects
- Instance-based authorization objects, with which you can check authorization for the specified business documents or other objects, depending on business-relevant data such as organization information

For instance-based authorization checks, there are two basic concepts. First, you can define authorization values based on identifiers for all profiles or other objects that cannot be classified any further by specific types, but only depending on their identifier. Second, you can define authorization values based on category, type, and further characteristics such as organizational data that can classify business documents beyond their identifier.

Besides the standard activities that can be defined for each authorization object for authorization field `ACTVT`, you can also define whole groups of activities for several authorization actions as an activity area. This means that you can define a distinct activity area, thereby allowing or preventing a whole set of actions related to this area. For example, you do not have to define all actions relating to subcontracting activities separately for a role, but only to define the activity area for subcontracting.

For more information about authorizations in TM, see <http://help.sap.com/s4hana> under ► *Product Assistance* ► *Enterprise Business Applications* ► *Supply Chain* ► *Delivery and Transportation* ► *Transportation Management (TM)* ► *Basic Functions* ► *Authorizations* ►.

If you want to display the authorization objects in TM, on the *SAP Easy Access* screen, choose ► *Tools* ► *ABAP Workbench* ► *Development* ► *Other Tools* ► *Authorization Objects* ► *Objects* ► and open object class `SCTS`.

i Note

You can also create your own authorization objects and implement the corresponding checks in BAdIs *Authorization Check* and *Data Retrieval Before Authorization Check*.

For more information, see Customizing for *Transportation Management* under [Business Add-Ins \(BADIs\) for Transportation Management](#) > [Basic Functions](#) > [Authorizations](#).

In TM, you have a special permission object T_ADMIN. System users who run batch jobs can use this permission object. To use this permission object, you must have all application specific permissions. Note that if you maintain this object in a certain role, all other TM permission objects will not be checked for this role anymore.

The table below shows the security-relevant authorization objects from other components that are used by TM. The list does not include basis authorization objects used for central functions or administration.

Standard Non-TM Authorization Objects

Authorization Object	Field	Value	Description
SAP SCM Basis 7.0			
/SCMB/PESL	ACTVT, USER	(06) Delete (34) Write In the USER field, you can enter the user for which you want to execute the activities in the ACTVT field.	Define Planning Service Manager (PSM) Selection. The authorization object enables the specified user to save and delete his or her selections.
/SCTM/SCU	/SCMB/SCU ACTVT		Use of supply chain units in routes.
C_MD_SCU	/SCMB/SCU, ACTVT		
Business Rules Framework			
FDT_OBJECT	FDT_ACT FDT_APPL FDT_OBJTYP		You use this authorization object to control usage of objects of the specified type in BRFplus.
FDT_WORKB	FDT_WB_ACT		This authorization object controls whether a user is authorized to use the BRFplus workbench and its tools.
APO			
C_APO_DEF	ACTVT, APO_PLNR, APO_DEFT, APO_DEFN	(01) Create or generate (02) Change (03) Display (06) Delete	APO Authorization Object: Master Data, Resource Definitions

Authorization Object	Field	Value	Description
C_APO_LOC	ACTVT, APO_LOC	(01) Create or generate (02) Change (03) Display (06) Delete (16) Execute (32) Save	APO Authorization Object: Master Data, Locations
C_APO_PROD	ACTVT, APO_LOC, APO_PROD	(01) Create or generate (02) Change (03) Display (06) Delete (16) Execute	APO Authorization Object: Master Data, Products
C_APO_RES	ACTVT, APO_PLNR, APO_LOC, APO_RES	(01) Create or generate (02) Change (03) Display (06) Delete (16) Execute	APO Authorization Object: Master Data, Resources
EH&S			
C_EHSP_TPP	ACTVT, LANGUAGE, ESECATPIN, ESEPHRGRP, PPSTAT	(02) Change (03) Display	This authorization is checked in the transactions for phrase management for entry into the hit list.
C_SHEP_TPG	ACTVT, ESECATPIN, ESEPHRGRP	(01) Create or generate (02) Change (03) Display (59) Distribute	This authorization object is checked in the phrase management transactions when entering and leaving the hit list. The activities "change" and "display" are also checked here.

Authorization Object	Field	Value	Description
M_MATE_DGM	ACTVT	(01) Create or generate (02) Change (03) Display (06) Delete (61) Export (82) Supplement	Using the authorization object M_MATE_DGM, you can prevent dangerous goods master data from being displayed or edited.

Formula & Derivation Tool

FDT_OBJECT	FDT_APPL, FDT_OBJTYP, FDT_ACT	(1) Create (2) Change (3) Display (4) Delete (5) Activate	You use this authorization object to control the authorization to display, create, change, or delete objects in the Formula & Derivation Tool (including functions, expressions, expression types, filters, and applications).
------------	----------------------------------	---	--

SAP SCM Optimizer

S_RFC	ACTVT, RFC_NAME, RFC_TYPE	(16) Execute	Required authorization to start the SAP SCM Optimizer and use most of the administrator transactions.
-------	------------------------------	--------------	---

SAP Event Management

X_EM_EH	ACTVT, /SAPTRX/PN, / SAPTRX/PV	(03) Display (10) Post	Event handler authorization
X_EM_EH_CH	ACTVT, /SAPTRX/SO	(01) Create or generate (02) Change (05) Lock (06) Delete (63) Activate (95) Unlock	Event handler changes
X_EM_EVM	ACTVT, /SAPTRX/CS, / SAPTRX/CD	(32) Save the sender code set and sender code ID	Event messages

Cross-Application Authorization Objects

Authorization Object	Field	Value	Description
CA_POWL	POWL_APPID, POWL_QUERY, POWL_CAT, POWL_LSEL, POWL_TABLE, POWL_RA_AL	<p>POWL_QUERY:</p> <p>(01) Users are allowed to create, change, and delete their own queries for all POWL object types assigned to them (compare with Customizing tables POWL_TYPE_USR and POWL_TYPE_ROL).</p> <p>(02) Users are only allowed to create their own queries on the basis of admin queries assigned to them in Customizing tables POWL_QUERY_USR and POWL_QUERY_ROL respectively. (Note: this is also subject to the user – POWL object type assignments.)</p> <p>(03) (and other values): Users are only allowed to change admin queries assigned to them with respect to the select options restrictions of those admin queries (thus creating a separate “derivation” for each admin query transparently)</p> <p>POWL_CAT:</p> <p>(01) Users are allowed to create, change, and delete their own categories and assign queries to them.</p> <p>(02) Users are only allowed to assign queries to the existing categories and change the order of queries.</p> <p>(03) (and other values): Users are not allowed to reassign queries or change the query order. Note: if field POWL_QUERY is set to 01 or 03, setting POWL_CAT to 03 is not advisable. Therefore,</p>	Specifies the authorities for Personal Object Worklist (POWL) iViews

Authorization Object	Field	Value	Description
		the value is implicitly set to 02 in this case.	
S_SERVICE	SRV_NAME, SRV_TYPE		This authorization object is automatically checked when external services are started. This is required for Gateway Services used by the TM Collaboration Portal
S_RFCACL	RFC_SYSID, RFC_CLIENT,RFC_USER, RFC_EQUUSER, RFC_TCODE, RFC_INFO,ACTVT	(16) Execute	Authorization check for RFC users, especially for trusted systems. This is required for Gateway Services used by the TM Collaboration Portal.
S_WFAR_OBJ	ACTVT OAARCHIV OADOKUMENT OAOBJEKTE	(01) Create or generate	This authorization object is used to control access to archived documents.
S_ARCHIVE	ACTVT APPLIC ARCH_OBJ		This authorization object is used in SAP archiving programs to protect the access to archive files
B_BUPA_RLT	ACTVT RLTYP		With this authorization object you define which BP roles can be edited.
B_BUPR_BZT	ACTVT RELTYT		With this authorization object you establish which relationship categories can be processed.
S_DATASET	ACTVT FILENAME PROGRAM		You use this object to assign authorizations for accessing operating system files.
S_WF_WI	TASK_CLASS WFACTVT WI_TYPE		Authorization object for working with work items in SAP Business Workflow
S_SCD0	ACTVT		

→ Recommendation

To segregate duties using roles and authorization values in TM, we recommend that you restrict the authorizations of the different roles to the business-related minimum.

With the authorization concept provided by TM, you can restrict authorization based on business document categories, such as *Freight Order* or *Freight Booking*, or on business document types, which you can create for the supplied business document categories. Furthermore, all critical business-related activities can be restricted for the different roles. These activities include creating business documents, displaying business documents or master data, triggering charge calculations, subcontracting freight documents, requesting customs declarations, and others activities or activity areas for the authorization objects of object class SCTS. Duties can, therefore, be segregated according to your business and scenarios.

Note that we do not recommend providing one role with full authorization for a business document or process, so that one role cannot be used, for example, to create and maintain a business document, add charge data to it, send it to a business partner, and create the invoice for that document. Such activities should be spread over different roles.

In addition, one user must not be assigned to different roles that would provide full authorization for a business document or process as described above.

i Note

If your scenario contains an approval workflow process, you need to create or maintain user WF-BATCH accordingly.

For general information about creating and maintaining the WF-BATCH user, see SAP Note [1251255](#).

13.9.2.2.3 Internet Communication Framework Security

You should only activate those services that are required for the applications running in your system. For Transportation Management, the following services are required:

- `/sap/option`
- `/sap/option/-gui`
- `/sap/option/-stateful`
- `/sap/option/-stateless`
- `/sap/option/-transactional`
- `/sap/public`
- `/sap/public/bc`
- `/sap/public/bc/abap`
- `/sap/public/bc/icf`
- `/sap/public/bc/icf/logoff`
- `/sap/public/bc/icons`
- `/sap/public/bc/icons_rtl`

- /sap/public/bc/its
- /sap/public/bc/its/designs
- /sap/public/bc/its/mimes
- /sap/public/bc/pictograms
- /sap/public/bc/ur
- /sap/public/bc/webdynpro
- /sap/public/bc/webdynpro/adobeChallenge
- /sap/public/bc/webdynpro/mimes
- /sap/public/bc/webdynpro/Polling
- /sap/public/bc/webdynpro/ssr
- /sap/public/bc/webicons/
- /sap/public/bc/workflow
- /sap/public/bsp
- /sap/public/bsp/sap
- /sap/public/bsp/sap/htmlb
- /sap/public/bsp/sap/public
- /sap/public/bsp/sap/
- /sap/public/bsp/sap/alertinbox
- /sap/bc/color_icon
- /sap/bc/fpads
- /sap/bc/gui
- /sap/bc/gui/sap
- /sap/bc/gui/sap/its
- /sap/bc/gui/sap/its/webgui
- /sap/bc/icf
- /sap/bc/nwbc
- /sap/bc/soap
- /sap/bc/srt
- /sap/bc/srt/xip
- /sap/bc/srt/xip/scmtms
- /sap/bc/srt/xip/scmtms/cfirsuite_conf
- /sap/bc/srt/xip/scmtms/exportdeclarationsuite
- /sap/bc/srt/xip/scmtms/gettranspdocuri
- /sap/bc/srt/xip/scmtms/icpy_trq_canceln_rq
- /sap/bc/srt/xip/scmtms/icpy_trq_rq
- /sap/bc/srt/xip/scmtms/icpy_trq_simrc
- /sap/bc/srt/xip/scmtms/inbdlvconf_v1
- /sap/bc/srt/xip/scmtms/invoicenotification_in
- /sap/bc/srt/xip/scmtms/outbdlvbulkconf
- /sap/bc/srt/xip/scmtms/tor_invprepcnf
- /sap/bc/ui5_ui5/sap/tm_scenblds1
- /sap/bc/webdynpro

- /sap/bc/webdynpro/sap
- /sap/bc/webdynpro/scmtms
- /sap/bc/workflow
- /SAPconnect

You must activate the following services if you intend to use the Gantt chart in the transportation cockpit:

- /sap/public/bc/ui5_ui5
- /sap/bc/bsp/scmtms/gantt_proxy

You must activate the following services if you intend to use the map in the transportation cockpit:

- /sap/bc/bsp/scmtms/common
- /sap/bc/ui5_ui5/scmtms/common
- /sap/bc/bsp/scmtms/geomap
- /sap/bc/ui5_ui5/scmtms/geomap

You must activate the following services if you intend to use the 3D load plan in the transportation cockpit:

- /sap/bc/bsp/scmtms/common
- /sap/bc/ui5_ui5/scmtms/common
- /sap/bc/bsp/scmtms/lso3d
- /sap/bc/ui5_ui5/scmtms/lso3d

You must activate the /sap/bc/apc/fpm_apc service if you intend to use multiple windows in the transportation cockpit.

Use transaction SICF to activate these services.

i Note

Services

- /sap/opu/odata/SCMTMS/TENDERING/ (Business process: Tendering)
- /sap/opu/odata/SCMTMS/EVENT_NOT/ (Business Process: Event Notification)
- /sap/opu/odata/SCMTMS/INVOICE_SUBMISSION/ (Business Process: Invoice Submission)
- /sap/opu/odata/SCMTMS/FRT_PROCUREMENT/ (Business Process: Strategic Freight Procurement)
- /sap/opu/odata/SCMTMS/INVOICING/ (Business Process: Self-Billing)
- /sap/opu/odata/SCMTMS/FO_CONFIRMATION/ (Business process: Freight Orders for Confirmation)

If your firewall(s) or Web dispatcher(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Activating and Deactivating ICF Services* into the search bar, press , and open the search result with that title.

For more information about ICF security, go to https://help.sap.com/s4hana_op_2020, enter *RCF/ICF Security Guide* into the search bar, press , and open the search result with that title.

13.9.2.2.4 Deletion of Personal Data

Use

Transportation Management (TM) might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

For more information see also the specific notes for TM:

- [2149395](#) – Deletion and Blocking of cBP in TM
- [2149396](#) – Simplified Data Deletion based on SAP ILM in TM
- [2941705](#) - Information Retrieval Framework (IRF) Enablement in TM for SAP S/4HANA

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. TM uses SAP ILM to support the deletion of personal data as described in the following sections.

SAP delivers an end of purpose check for business partners and locations in TM using a two-step approach:

1. The system fills a new data base table with the Start of Retention Time (SoRT) information per business partner or location business object and application rule variant as soon as a 'completed' document is saved.
2. The system uses the EoP check to decide whether a business partner or location can be blocked. During the EoP check, the system determines the SoRT information relevant for that business partner or location from the database table containing the SoRT information. The SoRT information is required to determine the relevant ILM policies and to calculate the correct end-of-purpose time depending on the defined ILM policies.

For more information, see <http://help.sap.com/s4hana> under ► *Product Assistance* ► *Enterprise Business Applications* ► *Supply Chain* ► *Data Management in Supply Chain* ► *Logistics Execution (LE)* ► *Data Management in Transportation Management* ► *Blocking and Deletion of Personal Data in TM* ► *End-of-Purpose Framework* ►.

SAP delivers a where-used check (WUC) for business partners and locations in TM including master data objects such as transportation charge rates, transportation charge scales, locations, and resources.

TM registers an EoP check in the Customizing settings for the blocking and deletion of business partners and locations and in addition provides a WUC for business partners and locations. For information about the Customizing of blocking and deletion for TM, see below, Configuration: Simplified Blocking and Deletion.

Features

End of Purpose (EoP) Check

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases.

- Phase one: The relevant data is actively used.
- Phase two: The relevant data is actively available in the system.

- Phase three: The relevant data needs to be retained for other reasons. For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- Display: The system does not display personal data of a blocked business partner or location.
- Change: It is not possible to change a completed business document that contains a blocked business partner or location.
- Create: It is not possible to create a business document using a blocked business partner or location. As soon as a blocked business partner or location is entered, the system raises a suitable error message.
- Copy/Follow-Up: It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- Search: The system does not display blocked data in the result list of search helps. The same is true for technical queries based on the business object for business partner (/SCMTMS/BUPA) and the business object for locations (/SCMTMS/LOCATION).

It is possible to display blocked data if a user has special authorization (SAP_CA_BP_DP_ADMIN). However, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

Relevant Application Objects and Available EoP functionality

Application	Implemented solution (EoP or WUC)	Further information
TM	End of Purpose Check (EoP) EoP Function Module: /SCMTMS/DPP_EOP_CHECK	The End of Purpose check (EoP) for business partners includes the following business objects: <ul style="list-style-type: none"> /SCMTMS/BUS_SHARE /SCMTMS/CUSTFREIGHTINVREQ /SCMTMS/FREIGHTAGREEMENT /SCMTMS/SUPPFREIGHTINVREQ /SCMTMS/TOR /SCMTMS/TRQ /SCMTMS/TAL /SCMTMS/WAYBILLNO The End of Purpose check (EoP) for locations includes the following business objects <ul style="list-style-type: none"> /SCMTMS/CUSTFREIGHTINVREQ /SCMTMS/SUPPFREIGHTINVREQ /SCMTMS/TOR /SCMTMS/TRQ

Application	Implemented solution (EoP or WUC)	Further information
TM	Where-Used-Check (WUC)	<p>In addition to the business objects handled in the EoP Check, the Where-Used Check (WUC) for business partners includes also master data objects such as:</p> <ul style="list-style-type: none"> • Transportation Charge Calculation Sheets • Transportation Charge Rates • Transportation Charge Scales • Locations • Resources

Process Flow

1. Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
 - Run transaction `IRMPOL` and maintain the required residence and retention policies for the central business partner (ILM object: `CA_BUPA`) or location . (ILM object `SCMB_LOC`).
 - Run transaction `IRMPOL` and maintain the required retention policies for the ILM objects of TM.
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
3. To determine which business partners or locations have reached end of purpose and can be blocked, you do the following, if you have the necessary authorization:
 - Run transaction `BUPA_PRE_EOP` to execute the end of purpose check function for the central business partner.
 - Run transaction `/SCMB/LOC_PRE_EOP` to execute the end of purpose check function for the location.
4. To unblock blocked business partner or location data, you do the following, if you have the necessary authorization:
 - Request unblocking of blocked business partner data by using the transaction `BUP_REQ_UNBLK`.
 - You can unblock the requested data by running the transaction `BUPA_PRE_EOP`.
 - For unblocking location data you can run the transaction `/SCMB/LOC_UNBLOCK_MD`.
5. You delete data by using the transaction `ILM_DESTRUCTION` for the ILM objects of TM.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of data in Customizing for *Cross-Application Components* under `Data Protection`.

- Define the settings for authorization management under [Data Protection](#) [Authorization Management](#). For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for.
 - Business Partner [Cross-Application Components](#) under [Data Protection](#) [Blocking and Unblocking](#) [Business Partner](#)
 - Location

[Transportation Management](#) ► [Master Data](#) ► [Transportation Network](#) ► [Location](#) ► [Location Master Deletion](#) ►

- Define the Customizing settings for TM. For more information, see <http://help.sap.com/s4hana> under [Product Assistance](#) ► [Enterprise Business Applications](#) ► [Supply Chain](#) ► [Data Management in Supply Chain](#) ► [Logistics Execution \(LE\)](#) ► [Data Management in Transportation Management](#) ► [Blocking and Deletion of Personal Data in TM](#) ► [Customizing Settings for Data Protection and Privacy](#) ►.

13.9.2.2.5 Depersonalization of Data

Transportation Management (TM) may process data (personal data) that is subject to the data protection laws applicable in specific countries.

When you use the scenario builder from your productive system, the scenario builder may process your personal data. Hence you must use the BAdI `/SCMTMS/SB_ADD_TEMPLATE_DATA` to depersonalize data before using it in the scenario builder.

This BAdI contains the method `CHECK_AND_ADJUST_DATA`. This method processes the data that you have selected to use in the scenario builder.

For more information on example implementation of how you can access the data in the BAdI, see `/SCMTMS/SB_ADD_TEMPL_DATA_SMPL`.

13.9.2.2.6 Security-Relevant Logging and Tracing

SAP systems have a variety of logs for system administration, monitoring, problem solving, and auditing purposes. Audits and logs are important for monitoring the security of your system and to track events, in case of problems.

i Note

Auditing and logging for ABAP Platform is described in detail in the *ABAP Platform Security Guide*.

Go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press , open the search result with that title, and navigate to [Auditing and Logging](#).

Security Audit Log Triggered by Virus Scan Interface (VSI)

Class `CL_VSI` automatically creates entries in the Security Audit Log for infections and scan errors found, together with the following information:

- Profile
- Profile step allowing the detection of the scanner-group
- Kind of virus found, with internal virus ID of the scan engine, if available

- User name and timestamp

The messages logged are located in message class `VSCAN` using system log messages BU8 and BU9 (created in transaction `SE92`). The severities are set to *High* and *Medium* respectively. The severity of the audit class is set to *Miscellaneous*.

For more information, see Customizing for SAP Supply Chain Management under ► [SAP Web Application Server](#) ► [System Administration](#) ► [Virus Scan Interface](#) ►.

Audit Information System (AIS)

Information about auditing and logging for the Audit Information System (AIS) is described in detail in the *ABAP Platform Security Guide*.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Audit Information System (AIS)* into the search bar, press `Enter`, and open the search result with that title.

For more information about security logs for the SAP Gateway, go to https://help.sap.com/s4hana_op_2020, enter *Logging in SAP Gateway* into the search bar, press `Enter`, and open the search result with that title.

Transportation Management (TM)

Tracing and Logging of Business Objects

In TM, you can log messages raised by business objects in the application log.

In the standard system, logging is deactivated. To activate logging, in Customizing for *Transportation Management*, choose ► [Basic Functions](#) ► [User Interface](#) ► [Define Message Settings](#) ► (note that this has negative impact on overall system performance; this is why SAP recommends to switch on logging only when required).

To access the application log, on the *SAP Easy Access* or in SAP Business Client screen, choose ► [Application Administration](#) ► [Application Log: Display Logs](#) ►. Alternatively, call transaction `SLG1`.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Logging of Specific Activities* into the search bar, press `Enter`, open the search result with that title, and navigate to [Application Logging](#).

Activating Change Documents

In TM, you can activate change documents to log changes to master data, business objects, and so on.

You must activate change documents in Customizing before the system can store them. For information about the objects for which you can activate change documents and where to activate them, see the corresponding section in the TM documentation:

Object	Customizing Path
Location	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Master Data ▶ Transportation Network ▶ Location ▶ Activate Change Documents ▶
Transportation lane	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Master Data ▶ Transportation Network ▶ Transportation Lane ▶ Activate Change Documents ▶
Product	<ul style="list-style-type: none"> ▶▶ SCM Basis ▶ Master Data ▶ Product ▶ Activate Change Documents ▶
Freight unit	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Planning ▶ Freight Unit ▶ Define Freight Unit Types ▶ (Track Changes checkbox)
Freight order	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Freight Order Management ▶ Freight Order ▶ Define Freight Order Types ▶ (Track Changes checkbox)
Freight booking	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Freight Order Management ▶ Freight Booking ▶ Define Freight Booking Types ▶ (Track Changes checkbox)
Freight agreement	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Master Data ▶ Agreements and Service Products ▶ Define Freight Agreement Types ▶ (Track Changes checkbox).
Forwarding agreement	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Master Data ▶ Agreements and Service Products ▶ Define FWA and Service Product Catalog Types ▶ (Track Changes checkbox).
Forwarding order	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Forwarding Order Management ▶ Forwarding Order ▶ Define Forwarding Order Types ▶ (Track Changes checkbox).
Forwarding quotation	<ul style="list-style-type: none"> ▶▶ Transportation Management ▶ Forwarding Order Management ▶ Forwarding Quotation ▶ Define Forwarding Quotation Types ▶ (Track Changes checkbox).

Object	Customizing Path
Forwarding settlement	▶ <i>Transportation Management</i> ▶ <i>Settlement</i> ▶ <i>Forwarding Settlement</i> ▶ <i>Define Forwarding Settlement Document Types</i> ▶ (Track Changes checkbox).
Freight settlement	▶ <i>Transportation Management</i> ▶ <i>Settlement</i> ▶ <i>Freight Settlement</i> ▶ <i>Define Freight Settlement Document Types</i> ▶ (Track Changes checkbox).
Order-based transportation requirement	▶ <i>Transportation Management</i> ▶ <i>Integration</i> ▶ <i>ERP Logistics Integration</i> ▶ <i>Order-Based Transportation Requirement</i> ▶ <i>Define Order-Based Transportation Requirement Types</i> ▶ (Track Changes checkbox).
Delivery-based transportation requirement	▶ <i>Transportation Management</i> ▶ <i>Integration</i> ▶ <i>ERP Logistics Integration</i> ▶ <i>Delivery-Based Transportation Requirement</i> ▶ <i>Define Delivery-Based Transportation Requirement Types</i> ▶
Service order	▶ <i>Transportation Management</i> ▶ <i>Freight Order Management</i> ▶ <i>Service Order</i> ▶ <i>Define Service Order Types</i> ▶ (Track Changes checkbox).

SAP SCM Optimizer

For information about the trace and log files for the SAP SCM Optimizer, see the *SAP SCM 7.0 Component Security Guide*.

To delete all the data privacy relevant information in log files and the explanation tool tables, you must run the following reports periodically:

- `RCC_CLEANUP` for SAP SCM Optimizer log files
Deletes all log entries made by RCC and all external files on remote engine servers for which the log deletion time parameter is set in `RCC_CUST`.
- `/SCMTMS/PLN_EXP_DELETE` for TM explanation tool
Deletes optimizer explanation logs older than x days.

The general recommendation is to run these reports everyday as stated in the Operations Guide.

For more information about the logging and tracing mechanisms, go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press , open the search result with that title, and navigate to *Auditing and Logging*.

13.9.3 Warehousing

13.9.3.1 Extended Warehouse Management

13.9.3.1.1 Authorizations

Extended Warehouse Management (EWM) uses the authorization concept provided by the AS ABAP or AS Java. Therefore, the recommendations and guidelines for authorizations as described in the Application Server ABAP Security Guide and SAP NetWeaver AS Security Guide Java also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF03`) on the AS ABAP and the User Management Engine's user administration console on the AS Java.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under [User Administration and Authentication](#).

Standard Authorization Objects

To gain an overview of the authorization objects for EWM, proceed as follows:

1. Open transaction `AUTH_DISPLAY_OBJECTS` to display active authorization objects.
2. In the overview, expand the following subtree of authorizations related to EWM.
 1. Authorizations Extended Warehouse Management (SCWM)
 2. Dock Appointment Scheduling (SCDS)
 3. Authorizations SCM Basis (SCMB)
 4. Master Data Authorization Objects (SCMD)

If you want to display the technical names of the authorization objects, choose [Edit](#) [Technical Names On](#).

3. If you want to get a detailed description, choose the [Information](#) button next to the authorization object you are interested in.

Warehouse-Based Authorization

Warehouse-Specific Field in Authorization Objects

If you have multiple warehouses modelled in EWM, you may need people working in one warehouse to be able to access data from another warehouse. Many authorization objects in EWM contain a specific authorization field for this purpose, for example:

- /SCWM/LGNU (*Warehouse Number/Warehouse Complex*)
This is the most commonly used authorization field. It is used, for example, in EWM monitor authorization object /SCWM/MO.
- /SCWM/ORG (*Location/Organizational Unit*)
- /SCMB/LGNU (*Warehouse Number/Warehouse Complex*)

Warehouse in Customizing or Administration

In other cases, such as in administration or Customizing, EWM does not use specific authorization objects. Instead, you can use generic authorization objects to limit the access to tables and views, for example:

- S_TABU_NAM (*Table Access by Generic Standard Tools*)
- S_TABU_LIN (*Authorization for Organizational Unit*)

Example

The Customizing activity *Define Storage Bin Types* has the assigned Customizing object /SCWM/T303. The underlying database table /SCWM/T303 contains field LGNUM (warehouse number) with data element /SCWM/LGNUM (*Warehouse Number/Warehouse Complex*). You can use generic authorization objects to limit the access to tables and views, as follows:

- Use authorization object S_TABU_NAM to limit access to Customizing object /SCWM/T303.
- Use authorization object S_TABU_LIN to limit access based on organizational criteria.
You can also use authorization field ORG_CRIT (*Organization Criterion for Key-Specific Authorization*) and use value /SCWM/LGNU (*Warehouse Number/Warehouse Complex*) to be able to enter a warehouse in ORG_FIELD1.

For more information, see the documentation of authorization objects S_TABU_NAM and S_TABU_LIN in transaction SU21.

BRFplus

BRFplus is sometimes used in EWM, for example, in Labor Management. However, BRFplus does not recognize organizational units such as the warehouse. Therefore, if BRFplus entities should be separated based on warehouse, you must consider this during the implementation phase so that you can use alternative BRFplus mechanisms.

For information about the authorization concept of BRFplus, go to https://help.sap.com/s4hana_op_2020, enter *Services for Application Developers* into the search bar, press , open the search result with that title, and navigate to ► *Business Rule Framework plus (BRFplus)* ► *Concepts* ► *Authorizations* ►

Critical Combinations

Appointment Planner for Carrier

i Note

These authorizations are relevant only if you are using SAP Dock Appointment Scheduling.

SAP Dock Appointment Scheduling offers a collaboration scenario where appointment planners for carriers can log on to the SAP Dock Appointment Scheduling system, and view and maintain appointments for their carrier. Since this potentially means that employees of a different company access SAP Dock Appointment Scheduling from outside the company network, you must put a special focus on authorizations. This kind of user should have very limited authorizations. As well as this, they should be able to access data of their own carrier only, and not be able to access other carriers' data. They should not be able to see internal data, like overall capacities of loading points. Therefore, you must be very careful and restrictive when assigning roles and authorizations to this kind of user.

SAP Dock Appointment Scheduling delivers a special authorization field for this.

i Note

We recommend that you define, in the roles, the loading points for which a user may view or create appointments. You can do this in the *Loading Point* authorization field (`/SCWM/DSLIP`) in the authorization objects Loading Appointment (`/SCWM/DSAP`) and Slot (`/SCWM/DSSL`).

In addition, the authorization field *User Process Scope for Dock Appointment Scheduling* (`/SCWM/DSPS`) is very important. It is available on the Loading Appointment and Slot authorization objects. For appointment planners for carriers, set this field to *Scope for an Appointment Planner for Carrier*. This ensures that this user can create and view appointments only for the carrier that is assigned to him or her. Otherwise such a user could create appointments for any carrier.

Warehouse Management Monitor: General

In the warehouse management monitor (`/SCWM/MON`), you can monitor and access a wide area of application content and also trigger actions. Due to the high amount of different data that can be accessed, this may be critical and you may want to restrict the access to the monitor and to the data and actions which can be used. Therefore, the warehouse management monitor provides a concept to restrict which persons can access which monitor nodes and which actions can be triggered. The corresponding authorization object is `/SCWM/MO`.

Warehouse Management Monitor: Authorization to Display Batch Execution Data

In the warehouse management monitor (`/SCWM/MON`), you can execute selections using batch jobs. You can view the results in the warehouse management monitor. During the selection, the system performs the normal authorization checks and selects and stores only data for which the user has authorization in the data containers for the warehouse management monitor. But if these data containers are then displayed by other users, the system does not perform these authorization checks. Therefore, you should only grant the authorization to display batch execution data for monitor nodes or users where these checks are not critical.

The authorization object used for the authorization to display batch execution data in the warehouse management monitor is `/SCWM/DATC`. For more information about this authorization object and the warehouse management monitor, see SAP Library for SAP S/4HANA at <https://help.sap.com/s4hana>. In SAP Library, choose ► *SAP S/4HANA* ► *Enterprise Business Applications* ► *Supply Chain* ► *Extended Warehouse Management* ► *Monitoring* ► *Warehouse Management Monitor* ►.

Maintaining Authorizations for Integration with SAP Components

Maintaining Authorizations for Integration of EWM Within Supply Chain

i Note

This is not relevant for standalone SAP Dock Appointment Scheduling.

For the integration of EWM within Supply Chain, that is, with Logistics Execution (LE) and Logistics – General (LO), use the authorization roles for the remote function call (RFC) destination users. For more information about these roles, see SAP Library for SAP S/4HANA at <https://help.sap.com/s4hana>. In SAP Library, choose **SAP S/4HANA > Enterprise Business Applications > Supply Chain > Extended Warehouse Management > Roles for Extended Warehouse Management (EWM)**.

For the integration from Supply Chain to EWM, for example, the role `/SCWM/ERP_EWM_INTEGRATION` exists. For the integration from EWM to Supply Chain, the corresponding RFC users also require the proper authorizations. For more information, see SAP Note [2081387](#).

In some cases, for example, for migration functions like transaction `/SCWM/MIG_PRODUCT`, the RFC enabled function module `RFC_READ_TABLE` is called on the Supply Chain side from EWM. For such scenarios, the corresponding RFC user requires this authorization. To avoid misuse, you should restrict the tables to be accessed to a minimum. You can therefore use the authorization objects `S_TABU_NAM` or `S_TABU_DIS`.

If you grant the usage of RFC function `RFC_READ_TABLE` to an RFC user, it is very important that you restrict the tables that can be accessed to a minimum to avoid misuse.

Maintaining Authorizations for Data Transfer to SAP Business Warehouse

i Note

This is not relevant for standalone SAP Dock Appointment Scheduling.

You can exclude DataSources from the extraction to SAP Business Warehouse (SAP BW).

Data that is stored in the extraction structure of this DataSource cannot be transferred to SAP BW.

1. In Customizing for *Extended Warehouse Management*, choose **Integration with Other SAP Components > Data Transfer to Business Warehouse > General Settings > Limit Authorizations for Extraction**.
2. Choose *New Entries* and choose a DataSource that you want to exclude from the extraction.
3. Choose the SAP BW system for which you want no more data for this DataSource to be extracted.
4. In the *Ex. Extr.* field, enter whether or not you want to exclude the DataSource from the extraction.
5. Save your entries and specify a transport request.

Maintaining Authorizations for Data Transfer Between Shipping and Receiving (EWM) and SAP Dock Appointment Scheduling

i Note

This is not relevant for standalone SAP Dock Appointment Scheduling.

SAP Dock Appointment Scheduling and Shipping and Receiving (S&R) are two independent components. But it is also possible to integrate the components, for example, so that the system communicates appointment status changes in SAP Dock Appointment Scheduling to S&R and appointment status changes in S&R to

SAP Dock Appointment Scheduling. For more information, see SAP Library for SAP S/4HANA at <https://help.sap.com/s4hana>. In SAP Library, choose ► *SAP S/4HANA* ► *Enterprise Business Applications* ► *Supply Chain* ► *Extended Warehouse Management* ► *SAP Dock Appointment Scheduling* ► *Integration with SAP EWM*.

For integration between SAP Dock Appointment Scheduling and S&R, the system uses queued RFC (qRFC) technology.

Using Standard Roles for SAP Dock Appointment Scheduling to EWM Integration

For the integration from SAP Dock Appointment Scheduling to S&R, the technical role `/SCWM/DAS_TO_EWM_INTEGRATION` is available. It contains the necessary authorizations to update the relevant S&R objects. The role does not contain any menu entries or transactions, as it is only a technical role for RFC communication. You must assign this role to the SAP Dock Appointment Scheduling user or RFC user, depending on if you use RFC communication, with which the integration is done.

Maintaining RFC Authorizations for Internal Communication in EWM

For RFC communication, users usually require the authorizations for authorization object `S_RFC`. As RFCs are potential security risks, you should be very restrictive in granting them. In certain cases, EWM also uses RFCs for internal purposes, for example for parallel processing or for asynchronous communication. For these purposes, no RFC authorizations have to be granted as these calls are within the SAP S/4HANA system.

EWM also uses specific RFC-enabled function modules, which are used to extract content from qRFCs. For example, these function modules are used to extract the warehouse number or delivery number from qRFCs.

These function modules do not perform data changes in EWM and also do not return data to a caller. They are required for delivery processing and for displaying of message queue entries in the warehouse management monitor.

The function modules are in the following special function groups:

- `/SCWM/CORE_MQ_REPLAY` (*Message Queue Moni: Replay Functions*)
- `/SCWM/CORE_RF_MQ_REPLAY` (*Replay Function Modules for RF*)
- `/SCWM/DELIVERY_MQ_REPLAY` (*Replay Function Modules for Deliveries*)
- `/SCWM/ERP_MQ_REPLAY` (*Replay Function Modules - ERP Interface*)
- `/SCWM/SR_MQ_REPLAY` (*Replay Function Modules - S&R*)
- `/SCWM/VAS_MQ_REPLAY` (*Replay Function Modules for VAS*)
- `/SCWM/WC_SERVICE_MQ_REPLAY` (*Replay Function Modules for Workcenter*)
- `/SCWM/WAVE_MGMT_MQ_REPLAY` (*Replay Function Modules for Wave*)
- `/SCWM/GTS_INT_MQ_REPLAY` (*Replay Function Modules for GTS Interface*)

If you use the message queue monitor node in the warehouse management monitor, you must add these function groups to authorization `S_RFC`. Use the activity Execute (16) and the Function Group (FUGR) type of RFC object.

For delivery and warehouse task processing, for example, confirming and creation of warehouse tasks, you must add the function group `/SCWM/DELIVERY_MQ_REPLAY` (*Replay Function Modules for Deliveries*) to authorization `S_RFC`.

These authorizations are already in the standard roles in EWM, so they are only relevant if you create your own roles.

13.9.3.1.2 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For this area the following services are needed:

- `/sap/bc/gui/sap/its/scwm/rfui`
This service can be used, for example, to allow warehouse workers to use transaction `/SCWM/RFUI` from mobile applications. The service can be accessed from the SAP console or by using ITS mobile. For more information, see SAP Library for SAP S/4HANA at <https://help.sap.com/s4hana>. In SAP Library choose **▶ SAP S/4HANA ▶ Enterprise Business Applications ▶ Supply Chain ▶ Extended Warehouse Management ▶ Radio Frequency Framework ▶ Work Processing Using Radio Frequency ▶ Resource Management Using Radio Frequency ▶**.
- `/sap/bc/webdynpro/scwm/`
In this path various Web Dynpro user interfaces (UIs) for Extended Warehouse Management as well as for SAP Dock Appointment Scheduling are contained.
- `/sap/bc/srt/xip/scwm`
Contains services which are used for SAP Process Integration communication.
- `/sap/bc/srt/rfc/scwm`
Contains services which are used for remote function call (RFC) communication. For example, `RFID_AII_EWM` which is used to exchange radio frequency identification information with SAP Auto-ID Infrastructure (SAP AII).

Use the transaction SICF to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information about ICF security, see the respective chapter in the ABAP Platform Security Guide.

13.9.3.1.3 Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

Extended Warehouse Management (EWM) saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by EWM and for which programs these file names and paths apply:

Logical File Names Used

The following logical file names have been created in order to enable the validation of physical file names:

- **EWM_PI_DOWNLOAD**
 - Transactions or programs using this logical file name and parameters used in this context:
 - Transaction /SCWM/PI_DOWNLOAD
 - Program /SCWM/R_PI_STOCK_DWNLD
 - Parameters used in this context:
 - <PARAM1> = Warehouse number (CHAR 4)
 - <PARAM2> = Counter (NUM2)
 - Logical file path used: **EWM_GLOBAL_PATH**

i Note

The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical filename.

- **EWM_PI_UPLOAD**
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/PI_UPLOAD
 - Program /SCWM/R_PI_FILEUPLD
 - Parameters used in this context:
 - <PARAM1> = Warehouse number (CHAR 4)
 - <PARAM2> = Creation Date (DATS8)
 - <PARAM2> = Counter (NUM2)
 - Logical file path used: **EWM_GLOBAL_PATH**

i Note

The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical filename.

- **EWM_STOCK_UPLOAD**
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/ISU
 - Program /SCWM/R_INITIALSTOCKUPLOAD
 - Parameters used in this context: <PARAM1> = Warehouse number (CHAR 4)
 - Logical file path used: **EWM_STOCK_UPLOAD_PATH**
- **EWM_STOBIN_UPLOAD**

- Transactions or programs using this logical file name:
 - Transaction /SCWM/SBUP
 - Program /SCWM/TLAGP_UPLOAD
- Logical file path used: EWM_STOBIN_UPLOAD_PATH
- EWM_STOBIN_SORT_UPLOAD
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/SRTUP
 - Program /SCWM/TLAGPS_UPLOAD
 - Logical file path used: EWM_STOBIN_SORT_UPLOAD_PATH
- EWM_MS_RESULT
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/MS_RESULT
 - Program /SCWM/R_MS_RESULT_READ
 - Parameters used in this context: <PARAM1> = Warehouse number (CHAR 4)
 - Logical file path used: EWM_GLOBAL_PATH

i Note

The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical filename.

- EWM_ELS_FRML
- EWM_ELS_ST
- EWM_ELS_STE
- EWM_ELS_SEQ
- EWM_ELS_ASS
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/ELS_UPLOAD
 - Program /SCWM/ELS_UPLOAD
 - Logical file path used: EWM_GLOBAL_PATH

i Note

The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical filename.

- EWM_MS_RESULT
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/PI_SAMP_UPDATE
 - Program /SCWM/PI_SAMP_UPDATE_RESULT
 - Parameters used in this context: <PARAM1> = Warehouse number (CHAR 4)
 - Logical file path used: EWM_GLOBAL_PATH

i Note

The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical filename.

- EWM_PRODUCT_UPLOAD
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/MIG_PRODUCT
 - Program /SCWM/R_MIG_PRODUCT
 - Logical file path used: EWM_PRODUCT_UPLOAD_PATH
- EWM_PACKSPEC_UPLOAD
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/MIG_PRODUCT
 - Transaction /SCWM/IPU
 - Program /SCWM/R_MIG_PRODUCT
 - Program /SCWM/R_PS_DATA_LOAD
 - Logical file path used: EWM_PACKSPEC_UPLOAD_PATH
- EWM_PI_COMPL_UPLOAD
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/MIG_PI_COMPL
 - Program /SCWM/R_MIG_PI_COMPL
 - Logical file path used: EWM_PI_COMPL_UPLOAD_PATH
- EWM_TDC_EDGE and EWM_TDC_RSRC
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/TDC_UPLOAD
 - Program /SCWM/TDC_UPLOAD
 - Logical file path used: EWM_GLOBAL_PATH
- EWM_TATT_UPLOAD (*Logical File for Upload of Time and Attendance Events*)
 - Transactions or programs using this logical file name:
 - Transaction /SCWM/TATT_UPLOAD
 - Program /SCWM/R_LM_TATT_UPLOAD
 - Parameters used in this context: <PARAM1> = Warehouse number (CHAR 4)
 - Logical file path used: EWM_GLOBAL_PATH

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information about data storage security, see the respective chapter in the ABAP Platform Security Guide.

13.9.3.1.4 Deletion of Personal Data

Use

Extended Warehouse Management (EWM) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ▾.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
EWM Warehouse Request Processing (for example, inbound deliveries, outbound delivery orders, and production material requests)	Business partner data is stored in the warehouse request. For example: <ul style="list-style-type: none">• Partner data in the warehouse request header/item• Ship-to data and ship-from data• Owner and entitled-to-dispose data on item level	You can delete the objects by using the archiving services. The archiving objects are: <ul style="list-style-type: none">• DLV_INB (Internal Warehouse Request (Inbound Delivery))• DLV_OUT (Internal Warehouse Request (Outbound Delivery))• DLV_PROD (Production Material Request)

Application	Detailed Description	Provided Deletion Functionality
EWM Labor Management	<p>The processor is recorded in several EWM documents in Labor Management, for example, in warehouse orders and executed workload.</p> <p>Time and attendance data such as clock-in and clock-out times of processors can be stored.</p>	<p>You can delete the objects by using the archiving services. The archiving objects are:</p> <ul style="list-style-type: none"> • WME_WO (Warehouse Order) • WME_EWL (Executed Workload) • WME_EPD (Performance Document) • WME_ILT (Indirect Labor Task) <p>You can delete time and attendance data using the destruction report / SCWM/TATT_DES. This report uses the data destruction object EWM_TATT and defined retention periods for time and attendance records.</p>
EWM Shipping and Receiving	In Shipping and Receiving, business partner data may be stored as carrier data in transportation units.	<p>You can delete the objects by using the archiving services. The archiving objects are:</p> <ul style="list-style-type: none"> • WME_TU (TU Activity) • WME_VEH (Vehicle Activity)
EWM Warehouse Order Processing	In warehouse order processing, business partner data may be stored as owner data or entitled-to-dispose data.	You can delete the objects by using the archiving services. The archiving object is WME_TO (Warehouse Order).
EWM Value-Added Services	If you use value-added services (VAS), business partner data may be stored as owner data or entitled-to-dispose data in VAS orders.	You can delete the objects by using the archiving services. The archiving object is WME_VAS (Value-Added Service Order).
EWM Wave Management	In wave management, business partner data may be stored as owner data or entitled-to-dispose data.	You can delete the objects by using the archiving services. The archiving object is WME_WAVE (Wave).
EWM Proof of Delivery	If you use proof of delivery (transaction /SCWM/POD_IMP), business partner data may be stored as carrier data, entitled-to-dispose data, or processor data in the proof of delivery object.	You can delete by using transaction / SCWM/POD_IMP.

Application	Detailed Description	Provided Deletion Functionality
EWM Stock Data	In EWM, stock data may store business partner data as, for example, owner data or entitled-to-dispose data.	You cannot delete directly. You must clear the corresponding stock so that the stock does not exist anymore by using the <i>Delete Obsolete Table Entries</i> (/LIME/BACKGROUND_DELETE_EXEC) report.
SAP Dock Appointment Scheduling	In SAP Dock Appointment Scheduling, business partner data may be stored as carrier data in loading appointments.	You can delete loading appointments by using the destruction report /SCWM/DSAPP_DES. This report uses the data destruction object EWM_DSAPP and defined retention periods for the loading appointments.
Transportation Management in EWM	Business partner data is contained in shipment objects and freight document objects.	You can delete the objects by using the archiving services. The archiving objects are: <ul style="list-style-type: none"> • TM_SHP (Shipment) • TM_FRD (Freight Document)
EWM Warehouse Billing	In Warehouse Billing, snapshots may contain a business partner.	You can delete billing measurements (BOPF object /SCWM/BM) using archiving object EWM_WBM (Warehouse Billing Measurement). You can delete billing measure requests (BOPF object /SCWM/WB_BMR) using deletion report <i>Deletion of WBMR and WBMS</i> (/SCWM/WB_WBMR_DELETION).
Account Assignment Data	Account assignment data can contain a business partner (party entitled to dispose).	You can delete account assignment data using transaction /SCWM/ACC_IMP_ERP.
Express Shipping Interface (ESI)	ESI manifests can contain address, location, or other contact data of a partner.	You can delete the objects by using the archiving services. The archiving objects are: <ul style="list-style-type: none"> • EWM_ESI_MF (ESI Manifest) • EWM_ESI_PA (ESI Parcel)
Global Batch Traceability (GBT) Interfacing	For communication to GBT, the tracking events which get temporarily stored in EWM can contain a business partner.	You can delete the GBT tracking events using report /SCWM/GBT_R_EVENT_DELETION.

Relevant Application Objects and Available EoP/WUC Functionality

Application	Implemented Solution (EoP or WUC)	Further Information
EWM Warehouse Request Processing (for example, inbound deliveries, outbound delivery orders, and production material requests)	An EoP check is implemented for the business partner object.	An EoP check is done for the following documents: <ul style="list-style-type: none"> • Outbound delivery order • Outbound delivery • Inbound delivery notification • Inbound delivery • Production material request
EWM Labor Management	An EoP check is implemented for the business partner object.	An EoP check is done for the following documents: <ul style="list-style-type: none"> • Executed workload • Employee performance document • Warehouse order • Indirect labor task • Time and attendance <p>For indirect labor tasks, the data is stored using order document management (ODM).</p> <p>The ODM data type is ILT. The corresponding header component is ILT with structure /SCWM/S_ILT_ODM.</p>
EWM Shipping and Receiving	An EoP check is implemented for the business partner object.	An EoP check is done for the following documents: <ul style="list-style-type: none"> • Transportation unit • Vehicle • Transportation unit activity • Vehicle activity
EWM Value-Added Services	An EoP check is implemented for the business partner object.	The data is stored using ODM. The ODM data type is VASO. The corresponding item component is VASI with structure /SCWM/S_VAS_ODM_ITM.
EWM Proof of Delivery	A WUC is implemented for the business partner object.	A WUC is done for the /SCWM/POD database table.

Application	Implemented Solution (EoP or WUC)	Further Information
EWM Stock Data	A WUC is implemented for the business partner object.	A WUC is done for the following database tables: <ul style="list-style-type: none"> • /SCWM/STOCK_IW01 • /SCWM/STOCK_IW02 • /SCWM/STOCK_IW03 • /SCWM/STOCK_IW04
SAP Dock Appointment Scheduling	An EoP check is implemented for the business partner (carrier) object.	An EoP check is done for loading appointments.
Transportation Management in EWM	An EoP check is implemented for the business partner object.	An EoP check is done for the following documents: <ul style="list-style-type: none"> • Freight order • Shipment <p>The data is stored using ODM, as follows:</p> <ul style="list-style-type: none"> • For shipments the ODM data type is TMSH. The corresponding header component is TSHD with structure /SCMB/TMDL_ODM_SHP_HDR_STR. • For freight documents the ODM data type is TMFR. The corresponding header component is TMFH with structure /SCMB/TMDL_ODM_FRD_HDR_STR.
Transportation Management in EWM Warehouse Billing	An EoP check is implemented for the business partner object.	An EoP check is done for warehouse billing measurement documents.
Wave Management	An EoP check is implemented for the business partner object.	An EoP check is done for waves.
Physical Inventory	An EoP check is implemented for the business partner object.	An EoP check is done for physical inventory documents.
Warehouse Orders and Warehouse Tasks	An EoP check is implemented for the business partner object.	An EoP check is done for warehouse orders and warehouse tasks.
Account Assignment Data	A WUC is implemented for the business partner object.	A WUC is implemented for the Account Assignment Data which can be replicated using transaction /SCWM/ACC_IMP_ERP.

Application	Implemented Solution (EoP or WUC)	Further Information
Global Batch Traceability (GBT) Interfacing	A WUC is implemented for the business partner object.	A WUC is implemented for the tracking events.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under [Data Protection](#).

13.9.3.1.5 Enterprise Services Security

For general information, see the chapters on Web Services Security in the ABAP Platform Security Guide and in the SAP Process Integration Security Guide.

13.9.3.1.6 Other Security-Relevant Information

Security Aspects of Data Flow and Processes

The following table describes some typical processes and communication channels, along with appropriate security measures:

Process	Security Measure
Mobile devices can be connected using HTTP/ITS mobile (it is also possible to use the SAP console). This is done based on the Internet Communication Framework (ICF) service for RFUI.	For more information, see Internet Communication Framework Security (ICF) [page 712] .
For certain scenarios, such as connecting automated physical processes (for example, conveyor systems) using SAP Plant Connectivity, remote function calls (RFCs) are used. Depending on the scenario, Idocs may also be used (for example, when warehouse control units are used).	For more information, see the SAP NetWeaver Security Guide.

Process	Security Measure
Extended Warehouse Management (EWM) offers the possibility of uploading and downloading data. In many of these transactions it is possible to either choose a local file system (PC) or files on the application server.	Ensure that only a few people can access these transactions and that access to the application server file system is restricted. You should design logical paths and filenames to restrict the access. For more information, see Data Storage Security [page 712] .
EWM offers a collaborative scenario for SAP Dock Appointment Scheduling. This enables appointment planners for carriers to access the system using SAP Gateway or Web Dynpro ABAP technology, for example, from outside the company network.	In this scenario, users outside of the company or firewall may access the system. For such scenarios, special attention must be paid to assigning authorizations to these users, and to the system setup and how the access from outside the company is granted.
EWM offers a scenario for Warehouse Billing where there is an integration with the SAP Transportation Management (SAP TM) system.	In this scenario, EWM can extract billing-relevant information from SAP TM and send order and settlement information back to SAP TM. The communication is performed using enterprise services or Web services.
EWM Fiori apps, for example, for deliveries or returns processing.	In this scenario, SAP Fiori accesses EWM using SAP Gateway. For more information, see SAP Library for SAP Fiori.

Security for Additional Applications

Geocoding

EWM can, in some cases, make use of third party geocoding applications, for example, PTV eServer. The software could be used, for example, to calculate geographical information for the locations or distances for transportation lanes. To connect to the third party software, this software may require an RFC destination on the EWM side. For more information on geocoding, see SAP Library for SAP S/4HANA at <https://help.sap.com/s4hana>. In SAP Library, choose **SAP S/4HANA > Enterprise Business Applications > Supply Chain > SCM Basis > SCM Basis Master Data > Location**. For any security issues regarding the third party application, for example, PTV eServer software, see the third party documentation.

SAP Plant Connectivity for Scale Integration

EWM can, in some cases, integrate an external scale. The software could be used, for example, to calculate the weight of a handling unit. A sample implementation exists for this in the [Determination of HU Weight Using Scale \(/SCWM/EX_WRKC_UI_GET_WEIGHT\)](#) Business Add-In. In this example, the system uses SAP Plant Connectivity to integrate an external scale. This software may require an RFC destination on the EWM side to connect to SAP Plant Connectivity.

For information about SAP Plant Connectivity, see SAP Help Portal at <https://help.sap.com/pco>.

13.9.3.1.7 Security-Relevant Logging and Tracing

Change Documents

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to track the changes made to this data. When these changes are logged, you should be able to check which user made which change, the date and time, the previous value, and the current value. It is also possible to analyze errors in this way.

Change Documents for Delivery Objects

When change documents are activated and used, each field in the delivery documents is linked to change documents. In the following Customizing activities, you can set – per document type – whether a change document is to be written for each delivery document.

- Activate change documents for inbound deliveries in Customizing for *Extended Warehouse Management* under ► *Goods Receipt Process* ► *Inbound Delivery* ► *Define Document Types for Inbound Delivery Process* ►
- Activate change documents for outbound deliveries in Customizing for *Extended Warehouse Management* under ► *Goods Issue Process* ► *Outbound Delivery* ► *Define Document Types for Outbound Delivery Process* ►
- Activate change documents for posting changes in Customizing for *Extended Warehouse Management* under ► *Internal Warehouse Processes* ► *Delivery Processing* ► *Posting Changes* ► *Define Document Types for Posting Change Process* ►
- Activate change documents for stock transfers in Customizing for *Extended Warehouse Management* under ► *Internal Warehouse Processes* ► *Delivery Processing* ► *Stock Transfers* ► *Define Document Types for the Stock Transfer Process* ►

You can view change documents for delivery objects in the transactions *Maintain Inbound Delivery*, *Maintain Outbound Delivery Order*, *Maintain Posting Change*, and *Maintain Internal Stock Transfer*. You can also run reports that retrieve archived documents in the same transactions, using the *Open Advanced Search* pushbutton.

Change Documents for Labor Management Objects

You can activate change documents for the following Labor Management objects in Customizing for *Extended Warehouse Management* under ► *Labor Management* ► *Activate Change Documents* ►:

- Processor
The activation of change documents is at client level. You can display the change documents in either of the following ways:
 - In transaction RSSCD100, in the *Object Class* field enter /SCMB/PRR, and in the *Object ID* field enter the processor.
 - In transaction *Maintain Business Partner*, transaction code BP, via the menu option ► *Extras* ► *Change History* ►.
- Processor (for Shift Sequence Assignment)
The activation of change documents is at client level. You can display the change documents in transaction RSSCD100. In the *Object Class* field, enter /SAPAPO/CD_RES. In the *Object ID* field, enter the <client><processor> without a space in between, for example, 003DOE.

- **Time and Attendance**
The activation of change documents is at warehouse level. You can display the change documents in transaction `RSSCD100`. In the *Object Class* field, enter `/SCWM/TATT`. In the *Object ID* field, enter the `<warehouse number>_<processor>_<date in format YYYYMMDD>_<time in format HHMMSS>` with date and time in the time zone of the warehouse, for example, `EW01_DOE_20180404_092911`.
- **Performance Document**
The activation of change documents is at client level. You can display the change documents in either of the following ways:
 - In transaction `RSSCD100`, in the *Object Class* field enter `/SCWM/EPD`. In the *Object ID* field, enter the document number of the performance document without leading zeroes.
 - In transaction *Employee Performance Overview*, transaction code `/SCWM/EPERF`.

13.9.3.2 Deletion of Personal Data

Use

Location master data may contain personal data that is subject to the data protection laws applicable in specific countries. You can use *SAP Information Lifecycle Management (ILM)* to control the blocking and deletion of personal data. For more information, see the product Assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Enterprise Business Applications* ► *Manufacturing* ► *Production Planning and Detailed Scheduling* ► *Master Data* ► *Location* ► *Data Protection* ►

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
SCM Location	Without ILM	You can run the report <code>/SAPAPO/DELETE_LOCATIONS</code> from the SAP Easy Access menu, under ► <i>SAP Menu</i> ► <i>Logistics</i> ► <i>SCM Extended Warehouse Management</i> ► <i>SCM Basis</i> ► <i>Master Data</i> ► <i>Location</i> ►; select the location, then choose ► <i>Extras</i> ► <i>Delete Location</i> ►
ILM-enabled SCM Location	Refer to What's New for ILM-related Information for SCM Location (SCMB_LOC)	Destruction object <code>/SCMB/LOC</code> ILM object <code>SCMB_LOC</code>

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
SCM Location	End of Purpose (EoP) check	

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of location master data in Customizing for *SCM Extended Warehouse Management* under ► [SCM Basis](#) ► [Master Data](#) ► [Location](#) ► [Location Master Data Deletion](#) ►.

13.9.4 Advanced Order Promising

13.9.4.1 Deletion of Personal Data in advanced Available-to-Promise (aATP)

Use

The applications in advanced Available-to-Promise (aATP) may process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► [Product Assistance](#) ► [Cross Components](#) ► [Data Management](#) ►.

Relevant Application Objects and Available Deletion Functionality

Component	Application	Deletion Functionality	Deletes/Destroys	Program
CA-ATP-ABC	ATP: Alternative-Based Confirmation	ATP_ABC_ALTVCTRL_DESTRUCTION	Alternative controls	ATP_ABC_ALTVCTRL_DES
CA-ATP-BOP	ATP: Backorder Processing	ATP_BOP_CSS_DESTRUCTION	Custom sort sequences	ATP_BOP_CSS_DES

Component	Application	Deletion Functionality	Deletes/Destroys	Program
		ATP_BOP_SEG_DESTRUCTION	Segments	ATP_BOP_SEG_DES
CA-ATP-CTL	ATP: Controller & Central Functions	AATP_CHARC_CTLG_DESTRUCTION	Blocked parent path values of value groups, blocked authorization values groups	AATP_CHARC_CATALOG_DES
		ATP_CHECK_LOG_DESTRUCTION	ATP check logs	ATP_CHECK_LOG_DES
CA-ATP-PAL	ATP: Product Allocation	AATP_PROD_ALLOC_DESTRUCTION	Product allocation data	AATP_PROD_ALLOC_DES
CA-ATP-SUP	SUP: Supply Protection	ATP_SUP_DESTRUCTION	Supply protection objects, supply protection groups	ATP_SUP_DES

Configuration: Simplified Blocking and Deletion

You configure the required Customizing settings for the blocking and unblocking of business partner master data in [SAP Reference IMG > Cross-Application Components > Data Protection > Blocking and Unblocking of Data > Business Partner Master Data](#).

For the deletion of business partner master data, you configure the settings in [SAP Reference IMG > Cross-Application Components > Data Protection > Deletion of Data > Deletion of Business Partner Data](#).

13.10 Cross-Line-of-Business

13.10.1 Commodity Management

13.10.1.1 Commodity Procurement

13.10.1.1.1 Deletion of Personal Data in Commodity Procurement

Use

The Commodity Procurement might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see https://help.sap.com/s4hana_op_2020 under [▶ Product Assistance](#) [▶ Cross Components](#) [▶ Data Protection](#) [▶](#).

See also the documentation under SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 [▶ Product Assistance](#) [▶ Enterprise Business Applications](#) [▶ Cross-Line-of-Business](#) [▶ Commodity Management](#) [▶ Commodity Procurement](#) [▶ Data Management in Commodity Procurement](#) [▶](#).

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
BRFplus Decision Table Entries for CPE Formula Assembly	See section <i>BRFplus Decision Table Entries for CPE Formula Assembly</i> below
Pricing Condition Records in CPE Formula Assembly	See section <i>Pricing Condition Records for CPE Formula Assembly</i> below
Records of Versioned Logistics Pricing Data Persistency	See section <i>Versioned Logistics Pricing Data Persistency</i> below
Period-End Valuation	Archiving Object <code>LO_CMM_AD</code> for accrual documents, and <code>MM_EKKO</code> for purchasing documents

BRFplus Decision Table Entries for CPE Formula Assembly

In the *Commodity Pricing Engine* (CPE), the *Formula Assembly* (FA) is used for logistics document items like sales order items or purchase order items to create default settings as, for example, the formula ID. These settings depend on properties of the underlying logistics document such as the vendor/customer, organizational and material data.

The *Business Rules Framework plus* (BRFplus) is used to implement rules for entering these settings. To use decision tables in BRFplus (as recommended by SAP), the required BRFplus content is provided (BRFplus application, BRFplus functions which use BRFplus decision tables). The standard content includes, for

example, decision tables, which require customer or vendor, material and other input fields, and the formula ID as result field. Decision tables can contain customer or vendor data, which eventually need to be deleted.

In the deletion report `RCPE_BRF01` (*Delete BRFplus Decision Table Entries for CPE Formula Assembly*) you enter a selected customer or vendor. When selecting the test mode, the report checks, whether the entered customer or vendor exists in the system, and whether he is blocked. After this, the report checks all BRFplus decision tables in BRFplus applications used for the *Formula Assembly*, and displays the respective row numbers of the BRFplus decision tables and the column containing the selected customer or vendor. If the *Test Mode* flag is not set, the report deletes all entries found, and creates an application log entry for object `CMM` and subobject `DPP_FA_BRF` (transaction `SLG1`).

The Customizing settings can be found in the *SAP Implementation Guide* under ► *Sales and Distribution* ► *Basic Functions* ► *Commodity Pricing* ► *Settings for Formula Assembly* ► *Assign BRFplus Application to Pricing Procedure* or ► *Materials Management* ► *Purchasing* ► *Commodity Pricing* ► *Settings for Formula Assembly* ► *Assign BRFplus Application to Pricing Procedure*.

Pricing Condition Records in CPE Formula Assembly

To delete entries for a single customer or vendor, use report `RCPE_CT01`. First, choose the test mode, to see all entries of the selected table, which would be deleted.

If you perform this transaction in productive mode, the selected entries will be deleted, and a log of transaction `SLG1` for object `CMM` and subobject `DDP_FA_AP` is displayed.

Note: Condition tables used for the *CPE Formula Assembly* must be selected and processed individually.

Versioned Logistics Pricing Data Persistency

Transaction `CMM_DEL_DOC_VERSIONS` allows you to update all records of the versioned logistic pricing data persistency (table `CMM_VLOGP`), which are stored for a certain blocked customer/vendor in a way that the identifier of the respective customer/vendor is masked with a blank space.

The authorization to perform this transaction is checked by the authorization object `S_TCODE`, and explicitly in the underlying report. It is ensured that, even if the report is performed by transaction `SA38`, only authorized experts can execute it. In addition, the authorization object `CMM_VLOGP` is checked by activity `06` (*Delete*). This enables the authorized user to delete records from the versioned logistic pricing data persistency (table `CMM_VLOGP`).

Note: It is checked, whether the entered customer is used as *Sold-to-Party* and/or *Ship-to-Party*. Records are deleted and masked accordingly.

This transaction must be performed to mask or to delete records as soon as a certain customer or vendor is blocked.

13.10.1.1.2 Business Partner End Of Purpose (EoP) Check

Use

Commodity Procurement and *Commodity Sales* provide information about stored personal data in the *Period-End Valuation (PEV)*, in the *Versioned Persistency of Logistics Pricing Data (VLOGP)*, *BRFplus Decision Table Entries for CPE Formula Assembly*, and in *Pricing Condition Records in CPE Formula Assembly*.

Period-End Valuation (PEV)

With transaction `CMM_PEV_WL` a worklist is created for a selected valuation key date and company code. The worklist shows accrual amounts of open logistics documents, which are not finally invoiced/billed yet.

The period-end valuation is registered for the EoP process. Whenever a customer or vendor needs to be blocked due to the EoP check, the period-end valuation is considered.

The PEV prevents blocking a customer or vendor until the respective PEV worklists are archived.

Vice versa, a check against the customer or vendor blocking indicator is performed, when a new PEV worklist is created. If a customer or vendor is blocked, the worklist will not be created.

The EoP check function module used is `CPE_PEV_EOP_CHECK`.

Versioned Persistency of Logistics Pricing Data

To display information about stored personal data in in the versioned persistency of logistics pricing data (`VLOGP`) of *Commodity Procurement* and *Commodity Sales*, run transaction `CMM_DEL_DOC_VERSIONS`.

The authorization to perform this transaction is checked by the authorization object `S_TCODE`, and in the underlying report. It is ensured that, even if the report is launched by transaction `SA38`, only authorized experts can execute it.

In case of blocked customers, vendors, business partners, the authorization object `B_BUP_PCPT` (activity 03) is additionally checked.

Table / Business Object	Archiving Object	Personal Data
<code>CMM_VLOGP</code>	n/a	LIFNR, KUNNR, KUNWE

BRFplus Decision Table Entries for CPE Formula Assembly

In the *Commodity Pricing Engine* (CPE), the *Formula Assembly* (FA) is used for logistics document items like sales order items or purchase order items to create default settings as, for example, the formula ID. These settings depend on properties of the underlying logistics document such as the vendor/customer, organizational and material data.

The *Business Rules Framework plus* (BRFplus) is used to implement rules for entering these settings. To use decision tables in BRFplus (as recommended by SAP), the required BRFplus content is provided (BRFplus application, BRFplus functions which use BRFplus decision tables). The standard content includes, for example, decision tables, which require customer or vendor, material and other input fields, and the formula ID as result field. Decision tables can contain customer or vendor data, which eventually need to be deleted.

To display information about stored personal data in the BRFplus decision tables for CPE formula assembly and perform report `RCPE_BRF01`, enter a selected customer or vendor. When selecting the test mode the report checks, whether the entered customer or vendor exists in the system, and whether he is blocked. After this, the report checks all BRFplus decision tables in BRFplus applications used for the *Formula Assembly*, and displays the respective row numbers of the BRFplus decision tables and the column containing the selected customer or vendor.

The Customizing settings can be found in the *SAP Implementation Guide* under [Sales and Distribution > Basic Functions > Commodity Pricing > Settings for Formula Assembly > Assign BRFplus Application to Pricing Procedure](#) or [Materials Management > Purchasing > Commodity Pricing > Settings for Formula Assembly > Assign BRFplus Application to Pricing Procedure](#).

Pricing Condition Records in CPE Formula Assembly

To check the tables used for the formula assembly, whether there is a certain customer or vendor used, perform transaction `MCPE_FA_GCM` (for *Commodity Procurement*) or `VCPE_FA_GCM` (for *Commodity Sales*).

Note: Condition tables used for the *CPE Formula Assembly* must be selected and processed individually.

Note: Tables behind these transactions are replaced by BRFplus tables.

13.10.1.2 Commodity Risk Management

13.10.1.2.1 Deletion of Personal Data

Use

Commodity Risk Management might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* .

See also the documentation under SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Enterprise Business Applications* ► *Cross-Line-of-Business* ► *Commodity Management* ► *Commodity Risk Management* ► *Data Management in Commodity Risk Management* .

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Order Request	Archiving Order Requests (FSCM-FIN-CDOTE)	Archiving object CMMFODOF_OF
Order Fill	Archiving Order Fills (FSCM-FIN-CDOTE)	Archiving object CMM_FSA_SA, ILM object CMMFODOF_OF
Commodity Subaccount	Archiving Commodity Subaccounts (FSCM-FIN-CDOTE)	Archiving object CMMFSA_SA, ILM object CMMFODOF_SUB_ACCOUNT

Archiving and deletion of data is performed as follows:

1. Archiving objects are created with transaction AOBJ.
2. For each archiving object, the ILM object is defined with transaction IRM_CUST.
3. Start transaction SARA and proceed as follows:
 - Perform action *Preproc*. The data relevant for archiving is identified and marked for archiving.
 - Perform action *Write*. The data marked for archiving is written to an archive file.
 - Perform action *Read*. The archived data is displayed.
 - Perform action *Delete*. The archived data is removed from the archive as well as from the database. This data is not available for any post processing anymore.

13.10.1.2.2 Change Logging

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to track the changes that have been made to this data.

A change log is provided for the following fields of *Commodity Derivative Order and Trade Execution* (FSCM-FIN-CDOTE):

- Reference Account (Broker)
- Broker
- Creation Time
- Creation Date
- Changed By
- Decided By
- Decided On

To get change information for the following documents, run transaction `SE38`, and perform the program `RSSCD200`:

Change Document Object	Description
CMM_AD_BO	Commodity Management: Accrual Document
CMMFDOF_CD_FILL	Commodity Order Fill Change Document
CMMFDOF_FL_PKT	Change Document for Commodity Order Fill Packet
CMMFDOR_OR_DOC	Commodity Derivative Order Assigned Documents
CMMFDOR_OR_LEG	Commodity Derivative Order Assigned Legs
CMMFDOR_OR_REQ	Commodity Derivative Order Request
CMMFSA_CDO_SA	Commodity Subaccount Change Structure

13.10.1.3 Commodity Sales

13.10.1.3.1 Deletion of Personal Data in Commodity Sales

Use

The *Commodity Sales* might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

See also the documentation under SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Enterprise Business Applications* ► *Cross-Line-of-Business* ► *Commodity Management* ► *Commodity Sales* ► *Data Management in Commodity Sales* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
BRFplus Decision Table Entries for CPE Formula Assembly	See Section <i>BRFplus Decision Table Entries for CPE Formula Assembly</i> below
Pricing Condition Records in CPE Formula Assembly	See section <i>Pricing Condition Records for CPE Formula Assembly</i> below
Records of Versioned Logistics Pricing Data Persistency	See section <i>Versioned Logistics Pricing Data Persistency</i> below

BRFplus Decision Table Entries for CPE Formula Assembly

In the *Commodity Pricing Engine* (CPE), the *Formula Assembly* (FA) is used for logistics document items like sales order items or purchase order items to create default settings as, for example, the formula ID. These settings depend on properties of the underlying logistics document such as the vendor/customer, organizational and material data.

The *Business Rules Framework plus* (BRFplus) is used to implement rules for entering these settings. To use decision tables in BRFplus (as recommended by SAP), the required BRFplus content is provided (BRFplus application, BRFplus functions which use BRFplus decision tables). The standard content includes, for example, decision tables, which require customer or vendor, material and other input fields, and the formula ID as result field. Decision tables can contain customer or vendor data, which eventually need to be deleted.

In the deletion report `RCPE_BRF01` (*Delete BRFplus Decision Table Entries for CPE Formula Assembly*) you enter a selected customer or vendor. When selecting the test mode, the report checks, whether the entered

customer or vendor exists in the system, and whether he is blocked. After this, the report checks all BRFplus decision tables in BRFplus applications used for the *Formula Assembly*, and displays the respective row numbers of the BRFplus decision tables and the column containing the selected customer or vendor. If the *Test Mode* flag is not set, the report deletes all entries found, and creates an application log entry for object CMM and subobject DPP_FA_BRF (transaction SLG1).

The Customizing settings can be found in the *SAP Implementation Guide* under ► [Sales and Distribution](#) ► [Basic Functions](#) ► [Commodity Pricing](#) ► [Settings for Formula Assembly](#) ► [Assign BRFplus Application to Pricing Procedure](#) ► or ► [Materials Management](#) ► [Purchasing](#) ► [Commodity Pricing](#) ► [Settings for Formula Assembly](#) ► [Assign BRFplus Application to Pricing Procedure](#) ►.

Pricing Condition Records in CPE Formula Assembly

To delete entries for a single customer or vendor, use report RCPE_CT01. First, choose the test mode, to see all entries of the selected table, which would be deleted.

If you perform this transaction in productive mode, the selected entries will be deleted, and a log of transaction SLG1 for object CMM and subobject DDP_FA_AP is displayed.

Note: Condition tables used for the *CPE Formula Assembly* must be selected and processed individually.

Versioned Logistics Pricing Data Persistency

Transaction CMM_DEL_DOC_VERSIONS allows you to update all records of the versioned logistic pricing data persistency (table CMM_VLOGP), which are stored for a certain blocked customer/vendor in a way that the identifier of the respective customer/vendor is masked with a blank space.

The authorization to perform this transaction is checked by the authorization object S_TCODE, and explicitly in the underlying report. It is ensured that, even if the report is performed by transaction SA38, only authorized experts can execute it. In addition, the authorization object CMM_VLOGP is checked by activity 06 (*Delete*). This enables the authorized user to delete records from the versioned logistic pricing data persistency (table CMM_VLOGP).

Note: It is checked, whether the entered customer is used as *Sold-to-Party* and/or *Ship-to-Party*. Records are deleted and masked accordingly.

This transaction must be performed to mask or to delete records as soon as a certain customer or vendor is blocked.

13.10.1.3.2 Business Partner End Of Purpose (EoP) Check

Use

Commodity Procurement and *Commodity Sales* provide information about stored personal data in the *Period-End Valuation (PEV)*, in the *Versioned Persistency of Logistics Pricing Data (VLOGP)*, *BRFplus Decision Table Entries for CPE Formula Assembly*, and in *Pricing Condition Records in CPE Formula Assembly*.

Period-End Valuation (PEV)

With transaction `CMM_PEV_WL` a worklist is created for a selected valuation key date and company code. The worklist shows accrual amounts of open logistics documents, which are not finally invoiced/billed yet.

The period-end valuation is registered for the EoP process. Whenever a customer or vendor needs to be blocked due to the EoP check, the period-end valuation is considered.

The PEV prevents blocking a customer or vendor until the respective PEV worklists are archived.

Vice versa, a check against the customer or vendor blocking indicator is performed, when a new PEV worklist is created. If a customer or vendor is blocked, the worklist will not be created.

The EoP check function module used is `CPE_PEV_EOP_CHECK`.

Versioned Persistency of Logistics Pricing Data

To display information about stored personal data in in the versioned persistency of logistics pricing data (`VLOGP`) of *Commodity Procurement* and *Commodity Sales*, run transaction `CMM_DEL_DOC_VERSIONS`.

The authorization to perform this transaction is checked by the authorization object `S_TCODE`, and in the underlying report. It is ensured that, even if the report is launched by transaction `SA38`, only authorized experts can execute it.

In case of blocked customers, vendors, business partners, the authorization object `B_BUP_PCPT` (activity 03) is additionally checked.

Table / Business Object	Archiving Object	Personal Data
<code>CMM_VLOGP</code>	n/a	LIFNR, KUNNR, KUNWE

BRFplus Decision Table Entries for CPE Formula Assembly

In the *Commodity Pricing Engine* (CPE), the *Formula Assembly* (FA) is used for logistics document items like sales order items or purchase order items to create default settings as, for example, the formula ID. These settings depend on properties of the underlying logistics document such as the vendor/customer, organizational and material data.

The *Business Rules Framework plus* (BRFplus) is used to implement rules for entering these settings. To use decision tables in BRFplus (as recommended by SAP), the required BRFplus content is provided (BRFplus application, BRFplus functions which use BRFplus decision tables). The standard content includes, for example, decision tables, which require customer or vendor, material and other input fields, and the formula ID as result field. Decision tables can contain customer or vendor data, which eventually need to be deleted.

To display information about stored personal data in the BRFplus decision tables for CPE formula assembly and perform report `RCPE_BRF01`, enter a selected customer or vendor. When selecting the test mode the report checks, whether the entered customer or vendor exists in the system, and whether he is blocked. After this, the report checks all BRFplus decision tables in BRFplus applications used for the *Formula Assembly*, and displays the respective row numbers of the BRFplus decision tables and the column containing the selected customer or vendor.

The Customizing settings can be found in the *SAP Implementation Guide* under [▶ Sales and Distribution ▶ Basic Functions ▶ Commodity Pricing ▶ Settings for Formula Assembly ▶ Assign BRFplus Application to Pricing Procedure](#) or [▶ Materials Management ▶ Purchasing ▶ Commodity Pricing ▶ Settings for Formula Assembly ▶ Assign BRFplus Application to Pricing Procedure](#).

Pricing Condition Records in CPE Formula Assembly

To check the tables used for the formula assembly, whether there is a certain customer or vendor used, perform transaction `MCPE_FA_GCM` (for *Commodity Procurement*) or `VCPE_FA_GCM` (for *Commodity Sales*).

Note: Condition tables used for the *CPE Formula Assembly* must be selected and processed individually.

Note: Tables behind these transactions are replaced by BRFplus tables.

13.11 Analytics Technology

13.11.1 Process Performance Monitoring

13.11.1.1 Process Observer

13.11.1.1.1 Roles for Process Observer

Process Observer uses the authorization concept provided by the SAP NetWeaver for Application Server ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under *User Administration and Authentication*.

Standard Roles

SAP delivers the following standard roles for Process Observer. You can use these roles as a template for your own roles.

Role	Description
Administration (SAP_POC_ADMINISTRATION)	This single role contains all the functions that you need to set up process monitoring: <ul style="list-style-type: none">• Maintain Customizing• Implement tracing in the application• Schedule jobs• Delete log entries and execute mass deletion of log entries• Update the master registry• Carry out configuration activities
Define Process (SAP_POC_MODEL)	This single role contains all the functions that you need to create a process definition: <ul style="list-style-type: none">• Define a process• Define BRFplus rules• Create a process simulation

Role	Description
View Process (SAP_POC_MONITOR)	This single role contains all the functions that you need to view process details in the Process Monitor SAP GUI screen: <ul style="list-style-type: none"> • Display process details
Analytics (SAP_POC_ANALYTICS)	This single role contains all the functions that you need to access the process-monitoring-relevant analytics content in the SAP Business Information Warehouse: <ul style="list-style-type: none"> • Display analytics information
Launchpad for Order to Cash Dashboard (SAP_BW_POC_O2C_ANALYTICS)	This single role contains all the functions required to launch the Dashboard for O2C Scenario.
Side Panel for Process Observer Data (SAP_POC_SIDE_PANEL)	This single role enables the user to see Process Observer data for standard transactions such as display sales order, display enquiry etc in a sidepanel using SAP Business Client.
Administration (SAP_POC_ADMIN)	This composite role contains all the functions that you need to set up process monitoring.
Business Process Expert (SAP_POC_BPX)	This composite role contains all the functions that you need, as a business process expert, to set up process definitions: <ul style="list-style-type: none"> • Define a process • Define BRFplus rules • Create a process simulation • Display process details

Standard Authorization Object

The basis for all roles used for data security for Process Observer is the authorization object POC_AUTH.

13.11.1.1.2 Data Protection and Privacy in Process Observer

⚠ Caution

If you configure Process Observer in a way that it stores personal data, you are responsible for ensuring that you are compliant with the data protection laws applicable in the relevant countries.

For more information about configuring Process Observer, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Process Observer \(CA-EPT-POC\)](#) ► [Process Monitoring and Analytics](#) ► [Process Monitoring Setup](#) ►.

13.11.1.1.3 Deletion of Personal Data in Process Observer

Depending on your configuration, Process Observer might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use the following transactions to delete process log data:

- POC_DELETE_LOG
- POC_MASS_DELETE

For more information about the deletion and mass deletion of process log data, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Process Observer (CA-EPT-POC)* ► *Operations* ► *Reports* ► *Reports Used in Operations for Process Monitoring* ►.

13.12 Enterprise Technology

13.12.1 Master Data Maintenance

13.12.1.1 Deletion of Personal Data

The business partner, customer and supplier master data might process data (personal data) that is subject to the data protection laws applicable in specific countries.

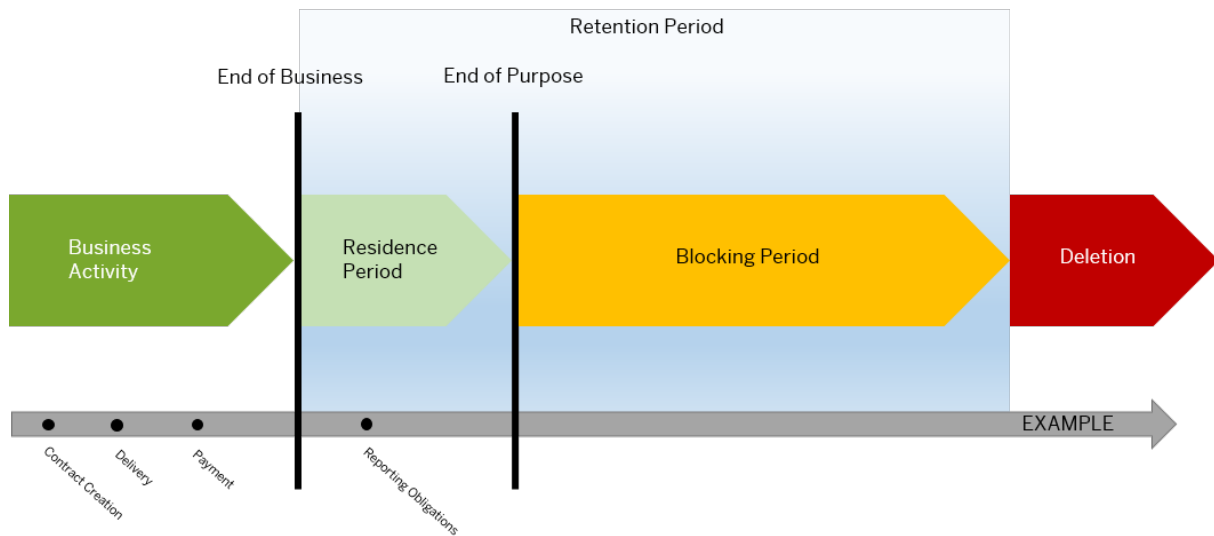
The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. The business partner, customer and supplier master data uses SAP ILM to support the blocking and deletion of personal data as described in the following sections.

Personal data collected in business partner, customer and supplier master data can be blocked as soon as business activities for which this data is needed are completed and the residence time for this data has elapsed. After this time, only users who are assigned additional authorizations can access this data. After the retention period for data expires, personal data can be destroyed completely such that it can no longer be retrieved. Residence and retention periods are defined in the customer system. For information about the Customizing of blocking and deletion, see [Configuration: Simplified Blocking and Deletion](#).

End of Purpose Check (EoP)

An end of purpose (EoP) check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period is part of the overall lifecycle of personal data which consists of the following phases:

- **Business activity:** The relevant data is used in ongoing business, for example contract creation, delivery or payment.
- **Residence period:** The relevant data remains in the database and can be used in case of subsequent processes related to the original purpose, for example reporting obligations.
- **Blocking period:** The relevant data needs to be retained for legal reasons. During the blocking period, business users of SAP applications are prevented from displaying and using this data; it can only be processed in case of mandatory legal provisions.
- **Deletion:** The data is deleted and no longer exists in the database.



Personal Data Lifecycle

Blocking of data can impact system behavior in the following ways:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change a business object that contains blocked data.
- **Create:** It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up:** It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- **Search:** It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable the end of purpose check, see sections [Process Flow](#) and [Configuration: Simplified Blocking and Deletion](#).

Relevant Application Objects and Available Deletion Functionality

Application Object	Provided Deletion Functionality
<i>Business Partner Data</i>	Archiving object: CA_BUPA ILM object: CA_BUPA Prerequisites: <ul style="list-style-type: none">• Business function BUPA_ILM_BF is activated• To use ILM enablement, the EoP check is mandatory before archiving or deletion (transaction BUPA_PRE_EOP).
<i>Customer Master Data</i>	Archiving object: FI_ACCRECV ILM object: FI_ACCRECV Prerequisites: <ul style="list-style-type: none">• Business function ERP_CVP_ILM_1 is activated.• To use ILM enablement, the EoP check is mandatory before archiving or deletion (transaction CVP_PRE_EOP).
<i>Supplier Master Data</i>	Archiving object: FI_ACCPAYB ILM object: FI_ACCPAYB Prerequisites: <ul style="list-style-type: none">• Business function ERP_CVP_ILM_1 is activated.• To use ILM enablement, the EoP check is mandatory before archiving or deletion (transaction CVP_PRE_EOP).
<i>Contact Person related to business partner, customer and supplier master data</i>	Destruction object: FI_ACCKNVK ILM object: FI_ACCKNVK Prerequisites: <ul style="list-style-type: none">• Business function ERP_CVP_ILM_1 is activated.• To use ILM enablement, the EoP check is mandatory before archiving or deletion (transaction CVP_PRE_EOP).

Relevant Application Objects and Available EoP functionality

Application	Implemented Solution	Further Information
<i>Business Partner</i> (BUP)	End of purpose (EoP) check	EoP is determined based on the last change date of the business partner master data (from database table BUT000).
<i>Business Partner Relationship</i> (BUB)	End of purpose (EoP) check	EoP is determined based on the Valid-To field of the relationship.
<i>ERP Customer Master</i> (ERP_CUST)	End of purpose (EoP) check	EoP is determined based on the last change date of the customer master data (from database table KNA1 or change document object DEBI), last change date of assigned credit cards (change document object VCNUM) or last change date of assigned addresses of the customer or contact persons.
<i>ERP Supplier Master</i> (ERP_VEND)	End of purpose (EoP) check	EoP is determined based on the last change date of the supplier master data (from database table LFA1 or change document object KRED) or the last change date of assigned addresses of the supplier or contact persons.
<i>ERP Contact Persons</i> (ERP_CONTACT_PERSON)	End of purpose (EoP) check	EoP is determined based on the last change date of the contact person (from the contact person related change documents of the customer or supplier) or the last change date of assigned addresses of the contact person.

Process Flow

- Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
 - Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA)
 - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and supplier master (ILM objects: FI_ACCPAYB, FI_ACCRECV, FI_ACCKNVK).
- You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.

3. To determine which business partners have reached end of purpose and can be blocked, you do the following:
 - Run transaction `BUPA_PRE_EOP` to execute the end of purpose check for the central business partner and the dependent customer master and supplier master.
 - Run transaction `CVP_PRE_EOP` to enable the end of purpose check function for the customer master and supplier master.
4. To unblock a blocked business partner data, you do the following:
 - Request unblocking of the blocked data by using the transaction `BUP_REQ_UNBLK`.
 - If you have the needed authorization for unblocking business partner data, you can unblock the requested data by running the transaction `BUPA_PRE_EOP` for the central business partner data and `CVP_UNBLOCK_MD` for the customer master and supplier master.
5. You delete data by using the transaction `ILM_DESTRUCTION` for the ILM objects of business partner data.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner, customer and supplier master data in Customizing (transaction `SPRO`) using the following path:

► [SAP Customizing Implementation Guide](#) ► [Cross-Application Components](#) ► [Data Protection](#) ► [Blocking and Unblocking of Data](#) ►

For more information, go to https://help.sap.com/s4hana_op_2020 under ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

13.12.1.2 Specific Read Access Logging Configurations

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions.

SAP delivers sample configurations for applications.

The OData and web services for Business Partner (`LO-MD-BP`) logs data in order to protect and restrict access to sensitive data of business partners.

The customer and supplier master data displays and maintains log data in order to track the disclosure of the supplier minority indicator.

You can find the configurations as described in the [Read Access Logging \[page 33\]](#) chapter.

OData for Business Partner

This table describes RAL configuration for API_BUSINESS_PARTNER.

Entity Type	Fields Logged	Business Context
A_BuPaIdentification	BPIDENTIFICATIONNUMBER BPIDENTIFICATIONTYPE	Log read access to the data referring to identification fields
A_BusinessPartnerBank	BANKACCOUNT BANKACCOUNTHOLDERNAME BANKACCOUNTNAME BANKACCOUNTREFERENCETEXT BANKCONTROLKEY BANKCOUNTRYKEY BANKIDENTIFICATION BANKNAME BANKNUMBER BUSINESSPARTNER CITYNAME COLLECTIONAUTHIND IBAN IBANVALIDITYSTARTDATE SWIFTCODE VALIDITYENDDATE VALIDITYSTARTDATE	Log read access to the data referring to bank related fields

Web Services for Business Partner

This table describes RAL configuration for Business Partner Web Services:

- BusinessPartnerSUITEBulkReplicateRequest_Out
- BusinessPartnerSUITEBulkReplicateRequest_In

Service Node	Fields Logged	Business Context
BankDetails	@actionCode	Log read access to the data referring to bank fields
Path:	BankAccountExternalID	
Request/BusinessPartnerSUITEBulk-ReplicateRequest/ BusinessPartner-SUITEReplicateRequestMessage[]/ BusinessPartner/BankDetails[]/	BankAccountHolderName	
	BankAccountID	
	BankAccountStandardID	
	BankControlKey	
	CollectionAuthorisationIndicator	
	ID	
	Name	
	SpecificationsDescription	
	SubstituteBusinessPartnerBankDetailsID	
	SubstituteDate	
	BankControlKey@listAgencyID	
	BankControlKey@listAgencySchemeAgencyID	
	BankControlKey@listAgencySchemeID	
	BankControlKey@listID	
	BankControlKey@listVersionID	
	BankDirectoryReference/ BankCountryCode	
	BankDirectoryReference/ BankInternalID	
	BankDirectoryReference/ BankStandardID	
	BankDirectoryReference/ BankInternalID@schemeAgencyID	
	SpecificationsDescription@ languageCode	

Service Node	Fields Logged	Business Context
	ValidityPeriod/EndDate	
	ValidityPeriod/StartDate	
Identification	BusinessPartnerID	Log read access to the data referring to identification fields
Path: Request/BusinessPartnerSUITE-BulkReplicateRequest/ BusinessPartnerSUITEReplicateRequestMessage[]/ BusinessPartner/Identification[]/	PartyIdentifierTypeCode	
	PartyIdentifierTypeCode@listAgencyID	
	PartyIdentifierTypeCode@listAgencySchemeAgencyID	
	PartyIdentifierTypeCode@listAgencySchemeID	
	PartyIdentifierTypeCode@listID	
	PartyIdentifierTypeCode@listVersionID	

Service Node	Fields Logged	Business Context
PaymentCardDetails	@actionCode	Log read access to the data referring to payment card related fields
Path: Request/BusinessPartnerSUITEBulkReplicateRequest/ BusinessPartnerSUITEReplicateRequestMessage[]/ BusinessPartner/PaymentCardDetails[]/	@blockCompleteTransmissionIndicator DefaultIndicator ID Block[]@actionCode Block[]/BlockingReasonCode Block[]/ BlockingReasonCode@listAgencyID Block[]/ BlockingReasonCode@listAgencySchemeAgencyID Block[]/ BlockingReasonCode@listAgencySchemeID Block[]/ BlockingReasonCode@listID Block[]/ BlockingReasonCode@listVersionID Block[]/ValidityPeriod/EndDate Block[]/ValidityPeriod/StartDate PaymentCard/CategoryCode PaymentCard/Description PaymentCard/ExpirationDate PaymentCard/HolderName PaymentCard/ID PaymentCard/IssueDateTime PaymentCard/IssuerName PaymentCard/NickName PaymentCard/ReferenceID	

Service Node	Fields Logged	Business Context
	PaymentCard/SequenceID	
	PaymentCard/TypeCode	
	PaymentCard/ValidFromDate	
	PaymentCard/ Description@languageCode	
	PaymentCard/ ID@schemeAgencyID	
	PaymentCard/ ID@schemeAgencySchemeAgenc yID	
	PaymentCard/ ID@schemeAgencySchemeID	
	PaymentCard/ID@schemeID	

Customer and Supplier Master Data

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Configuration	Fields Logged	Business Context
VEND_MINDK	LFB1-MINDK LFB1-LIFNR LFB1-BUKRS	Log access to minority indicator only if all fields are shown together.

13.12.2 Enterprise Contract Management

13.12.2.1 Authorizations and Roles Used by Enterprise Contract Management

Enterprise Contract Management (formerly known as Legal Content Management) uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the Application Server ABAP Security Guide also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_BR_ADMINISTRATOR_LCM	Administrator - Enterprise Contract Management
SAP_BR_EMPLOYEE_LEGAL_CONTENT	Employee - Enterprise Contract Management
SAP_BR_LEGAL_COUNSEL	Legal Counsel

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
LCM_GEN	General Activities
LCM_CTX	Auth. Obj. for LCM Context
LCM_CTXADM	Auth. Obj. for Task in LCM Context Admin. actions

Authorization Object	Description
LCM_LT	Auth. Obj. for LCM Legal Transaction
LCMDOCSTMP	Auth. object for Stamps in LCM Document
LCMSTMPACT	Auth. object for Stamp activities in LCM Document
LCM_LTACT	Auth. Obj. for Task in LCM Legal Transaction Actions
LCM_DOCHDR	Auth. Obj. for Document Header
LCM_DOCLT	Auth. Obj. for Document header for LT attributes
LCM_LTENCC	Auth. Obj. for Company Code in Legal Transaction
LCM_LTENPO	Auth. Obj. for Purchasing Organization in Legal Transaction
LCM_LTENSO	Auth. Obj. for Sales Organization in Legal Transaction

Authorization for DocuSign Integration

The functions for DocuSign integration use the authorization concept provided by ABAP platform. Therefore, the recommendations and guidelines for authorizations as described in the ABAP Platform Security Guide also apply to DocuSign integration. The ABAP platform authorization concept is based on assigning authorizations to users based on roles. For the role maintenance for ABAP technology, use the profile generator (transaction PFCG).

For more information on Authorization for DocuSign integration, please refer to the Set Up Guide of Enterprise Contract Management (1XV) available in the SAP Best Practices Explorer at <https://rapid.sap.com/bp/>.

i Note

We recommend you to also refer to the Security Guide of DocuSign and align with both the information to set-up a consistent security concept in this integration. Refer to the DocuSign security guide at <https://www.docusign.com/how-it-works/security> and <https://www.docusign.com/trust>.

13.12.2.2 Blocking of Personal Data

The SAP S/4HANA for Enterprise Contract Management (CM) (formerly known as Legal Content Management) applications might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under **Product Assistance** > **Cross Components** > **Data Protection**.

For this solution, data protection and privacy (DPP) is implemented for the following data:

- Entity types *Customer* and *Supplier*
- External contact type *Business Partner*

The DPP checks are enabled in DCL files which inherit the authorization of the respective standard DCL files. If the user uses in a legal transaction the value help for a customer, supplier or business partner, the DCL authorization check is executed and the blocked data is filtered out from the list that is shown in the value help. If the user enters a customer, supplier or business partner directly, without using the value help, the Business Object Processing Framework (BOPF) validation methods check the data against the CDS views and the blocked data is not displayed.

The same logic is applied in the API. If an API call creates or updates data for a legal transaction, the BOPF validation is done based on the DPP authorization checks.

The following field indicates if the legal transaction is blocked:

- `IsEndOfPurposeBlocked` - if set to X (true)

End of Purpose Check

The End of Purpose (EoP) check identifies if all business applications have completed their purpose in use of master data, so that it can be later blocked. Basically, the check is performed to see if a master data (customer, supplier or business partner) can be blocked. In LCM, the EoP check is reached when the legal transaction has reached one of the following status:

- Canceled
- Terminated
- Expired

and when the context has reached one of the following status:

- Inactive
- Expired
- Replaced

The central EoP check report calls the CM modules to check if any business data is in use. And the CM module checks the data in legal transaction and returns the respective status back. Whether or not the customer, supplier or business partner is blocked, is determined based on the following scenarios, which can coexist in the same installation:

CM determines the EoP. The business logic is hosted in CM and as long as any of the data is still in use, it cannot be removed or blocked.

i Note

When the legal transaction is blocked, all the documents assigned to this legal transaction will also be blocked.

Configuration

You configure the settings related to the blocking and deletion of customer, supplier, and business partner master data in Customizing under ► [Cross Application Components](#) ► [Data Protection](#) ► [Blocking and Unblocking of Data](#) ► [Business Partner](#) and ► [Cross Application Components](#) ► [Data Protection](#) ► [Blocking and Unblocking of Data](#) ► [Customer Master/Supplier Master Deletion](#) . For more information, see the documentation of the respective Customizing activities.

The application name for the EoP check is LCM-LT. You need to configure the blocking for the following objects:

Object	Type	EoP Check Object
Legal Transaction	External contact type / Business partner	LCM_LEGALTR_BUPA_EOP_CHECK
Legal Transaction	Entity type / Customer or supplier	CL_LCM_LEGALTR_CVP_EOP_CHECK
Context	Customer or Supplier	CL_LCM_CTX_CVP_EOP_CHECK
Context	Business partner	LCM_CTX_BUPA_EOP_CHECK

More Information

https://help.sap.com/s4hana_op_2020 under ► [Product Assistance](#) ► [Enterprise Technology](#) ► [SAP S/4HANA for Enterprise Contract Management](#) ► [Data Management in SAP S/4HANA for Enterprise Contract Management](#) .

13.12.2.3 Version Management of Legal Documents Sent for e-Signature

For e-Signature of legal documents, Enterprise Contract Management provides integration with DocuSign. However, you can use different service providers other than DocuSign.

i Note

It is very important to note that SAP does not validate the content of the document sent for e-Signature to any providers including DocuSign. SAP is not responsible for content modifications in the version of the document sent by the e-Signature provider/signor.

13.12.3 Geographical Enablement Framework

13.12.3.1 Authorizations

The framework uses the authorization concept provided by the Application Server ABAP and SAP HANA Platform. Therefore, the recommendations and guidelines for authorizations as described in the SAP Netweaver Application Server, ABAP Security Guide and HANA platform also apply to SAP Geographical Enablement Framework. The SAP authorization concept is based on assigning authorizations to users based on roles. For role maintenance in application server ABAP (AS ABAP), use the profile generator transaction **PFCG** in the backend system.

Standard Roles

The table below provides the standard roles that are used by the framework.

Roles	Description
<code>sap.gef.data::gef_user</code>	Delivered in SAP HANA DU for the SAP Geographical Enablement Framework; it provides basic authorization to access the framework schema in SAP HANA (SAP_GEF). You can assign this role to <code>SAP_GEF_USER</code> or other reference users that are created.
<code>sap.gef.data::gef_admin</code>	In addition to all the authorizations provided in the <code>gef_user</code> role, this admin role provides advanced authorizations for administrative tasks.

For AS ABAP, the **PFCG** role template, `SAP_GEF_USR` is delivered. This template provides basic authorizations for the framework. Other authorization roles, if needed for accessing application data, need to be added to create **PFCG** roles for consuming the framework services.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization	Object	Field Value
<code>G_GEF_GEOM</code>	<code>GEF_BO_ID</code>	Business Object ID
	<code>GEF_CONTXT</code>	Geometry Context ID
	<code>ACTVT</code>	Activity

13.12.3.2 Internet Communication Framework Security (ICF)

You should only activate the services that are needed for the applications running in your system. For this area the following services are needed:

- /default_host/sap/ca/GEF/arcgis/rest/services
In this path, the framework can provide services that conform to the specifications of different GIS service providers, if a custom GIS plug-in is developed and customized. For more information, see the Application Implementation section in the Geographical Enablement Framework documentation.
- /default_host/sap/ca/GEF/rest/config
In this path, the framework provides configuration information. This service is independent from any GIS service providers.
- /default_host/sap/bc/ui5_ui5/sap/gef_ui
The UI (Geometry Explorer and Geometry Editor) has been delivered to work with our framework. The UI starts from this path.

Use transaction **SICF** to activate these services.

If your firewall(s) uses URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information about ICF security, see the respective chapter in the ABAP Platform Security Guide.

13.12.3.3 Data Protection and Privacy

The SAP Geographical Enablement Framework does not collect, store, or process users' personal data. However, applications built on it may. Therefore, SAP recommends activating secure session management. We also recommend that you use SSL to protect the network communications where these security-relevant cookies are transferred.

Read access logging (RAL) monitors and logs read access to sensitive data, if any. It is required for applications to comply with legal regulations or public standards such as data privacy. In most cases, applications rely on the underlying business suite to save sensitive data. Therefore, it is also recommended to refer to the documents of the underlying platforms and activate the RAL based on the needs.

13.12.3.4 Enterprise Services Security

A technical limitation (tracked in security message 1670119508) has been identified; not all the user controlled inputs are sufficiently validated or encoded. This may cause security issues like Cross-Site Scripting (XSS).

This issue has been investigated and a solution is being implemented at this time. Contact SAP for the availability of this solution.

13.12.4 Master Data Governance

13.12.4.1 Deletion of Personal Data in Master Data Governance

Use

For personal data processed in the Master Data Governance (MDG) application, you can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal under [▶ Product Assistance ▶ Cross Components ▶ Data Protection ▶](#).

Relevant Application Object

Application	Provided Deletion Functionality
MDG Change Requests	Archiving object USMD_CR

For more information about the application object, see the product assistance for SAP S/4HANA on the SAP Help Portal under [▶ Product Assistance ▶ Cross Components ▶ Master Data Governance ▶ Data Protection in Master Data Governance ▶ Data Archiving in Master Data Governance ▶](#).

Configuration: Simplified Blocking and Deletion

- You configure the settings related to the blocking and deletion of business partner, customer, and supplier master data in Customizing under [▶ Cross-Application Components ▶ Data Protection ▶ Deletion of Data ▶ Deletion of Business Partner Data ▶](#).
- For information on defining ILM rules, see the product assistance for SAP S/4HANA on the SAP Help Portal under [▶ Product Assistance ▶ Cross Components ▶ SAP Information Lifecycle Management ▶ Using ILM Retention Management in the Application System ▶ Editing ILM Policies ▶ Editing Retention Rules ▶](#).
- For information on defining End of Purpose checks, see the product assistance for SAP S/4HANA on the SAP Help Portal under [▶ Product Assistance ▶ Cross Components ▶ Data Protection ▶ Simplified Blocking and Deletion ▶ End of Purpose \(EoP\) Check ▶](#).

End of Purpose

Master Data Governance for Business Partner (MDG-BP), Master Data Governance for Supplier (MDG-S), and Master Data Governance for Customer (MDG-C) are applications that are providing a workflow-based governance process for business partners. Within this process, the applications MDG-BP, MDG-S, and MDG-C do not store business partners permanently. In any case, MDG-BP, MDG-S, and MDG-C do not process business partners with the end of purpose indicator assigned.

For Master Data Governance, consolidation and Master Data Governance, mass processing, we recommend to use only business partner records that are not selected for End of Purpose (EoP).

The MDG, consolidation application and the MDG, mass processing application do not process business partners with the end of purpose indicator assigned.

For MDG, consolidation, we recommend to delete source data after the end of the consolidation process.

Storage of Personal Data

All Master Data Governance applications store data only temporarily.

Changes to Personal Data

The system logs changes to personal data using change documents.

Read Access Logging for MDG

For information on read access logging, see *Read Access Logging* under *Data Protection* of this Security Guide.

Enhancements

- For Master Data Governance for Custom Objects, we do not recommend to enhance personal data in your own objects. If it is necessary, you need to ensure to archive and delete enhanced data for the End of Purpose (EoP) goal.
- For Master Data Governance, central governance, we recommend to use backend tables of SAP-BP for enhancements and enhance the MDG data model accordingly. .

13.12.5 Agent Framework

13.12.5.1 Deletion of Personal Data in Agent Framework

The *Agent Framework* might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

The Agent Framework works in conjunction with the *Change Notification Service* (CA-GTF-TS-CNS). The Change Notification Service represents an Agent Framework Event (such as a limit change to an account) in the form of a change pointer. Each change pointer is based on an export object.

In addition to the change pointers generated for an export object, the CNS can be configured to also provide images of the export object events. Depending on the export object type, these images might contain personal data. For data protection reasons, you must delete the image data at regular intervals. You should therefore schedule a regular job to call one of the two deletion reports CNS_CP_DELETE or CNS_DP_DELETE_MULT. For this, you can use the simplified, integrated job control in the Agent Framework available in Customizing for [► Cross-Application Components ► General Application Functions ► Agent Framework ►](#).

More Information

For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 and go to

- [► Cross Components ► Data Protection ►](#).

13.13 SAP S/4HANA Industries

13.13.1 Consumer

13.13.1.1 Agriculture

13.13.1.1.1 Agricultural Contract Management

13.13.1.1.1.1 Read Access Logging

Read Access Logging (RAL) is used to monitor and log read access to sensitive data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy. These common questions might be of interest for an application that uses Read Access Logging:

- Who accessed the data of a given business entity, for example a bank account?
- Who accessed personal data, for example of a business partner?
- Which employee accessed personal information, for example religion?
- Which accounts or business partners were accessed by which users?

These questions can be answered using information about who accessed particular data within a specified time frame. Technically, this means that all remote API and UI info structures (that access the data) must be enabled for logging.

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions. SAP delivers sample configurations for applications. The application component scenario logs data in order to describe business processes. You can find the configurations as described in this chapter.

For the following configurations, fields are logged in combination with additional fields in the following business contexts:

Configuration	Fields Logged	Business Context
/ACCGO/LDC_WC	Driver ID, License, Vehicle ID	If any person accesses the information about these fields using transaction /ACCGO/LDC_WC either in Change Mode or Display Mode

Read Access Logging is currently limited to the following channels, however:

- Remote Function Calls (sRFC, aRFC, tRFC, qRFC, bgRFC)
- Dynpro (dynpro fields, ALV Grid, ABAP List, F4)
- Web Dynpro
- Web services
- Gateway (for oData)

13.13.1.1.1.2 Deletion of Personal Data

Agricultural Contract Management might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

To enable even complex scenarios, SAP simplifies existing deletion functionality to cover data objects that are personal data by default. For this purpose, SAP uses SAP Information Lifecycle Management (ILM) to help you set up a compliant information lifecycle management process in an efficient and flexible manner. The functions that support the simplified blocking and deletion of personal data are not delivered as a big bang implementation but in several waves. Scenarios or products that are not specified in the notes [1825608](#) (Simplified Blocking and Deletion of Central Business Partner) and [2007926](#) (Simplified Blocking and Deletion of Customer / Vendor Master Data) are so far not subject of simplified blocking and deletion. Nevertheless, it is also possible to destroy personal data for these scenarios or products. In these cases, you have to use existing archiving or deletion functionality or implement an individual retention management of relevant business data along its entire lifecycle.

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. Agricultural Contract Management uses SAP ILM to support the deletion of personal data as described in the following sections:

- SAP delivers an end of purpose check for Agricultural Contract Management.
- All applications register an end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the customer and vendor master. For information about the Customizing of blocking and deletion for Agricultural Contract Management, see Configuration: Simplified Blocking and Deletion.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases:

- **Phase one:** The relevant data is actively used.
- **Phase two:** The relevant data is actively available in the system
- **Phase three:** The relevant data needs to be retained for other reasons.

For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked.

Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change a business object that contains blocked data.
- **Create:** It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up:** It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data
- **Search:** It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see Process Flow and Configuration: Simplified Blocking and Deletion.

If you still want to block the data, the dependent data must be deleted by using the existing archiving and deletion tools or by using any other customer-specific solution.

13.13.1.1.1.3 Change Log

Person-related data is subject to frequent changes. Therefore, for revision purposes or because of legal regulations, it may be necessary to be able to track the changes made. If these changes are logged, at any time you can check which employee made which change and when.

Change log has been enabled for the following fields in the Agricultural Contract Management process:

1. Driver ID
2. License Number
3. Vehicle ID
4. Customer
5. Vendor

You can execute program `RSSCD200` to get the change information of these documents.

13.13.1.2 Retail and Fashion

13.13.1.2.1 Network and Communication Security

The following information is relevant for specific SAP S/4HANA Retail solutions. For general information about network and communication security in SAP S/4HANA, see [Network and Communication Security \[page 19\]](#).

Communication Paths for SAP Forecasting and Replenishment

For information about the security of communication paths for integration with SAP Forecasting and Replenishment, see the Security Guide for SAP Forecasting and Replenishment.

Other Communication Paths for SAP S/4HANA Retail

The following table shows the communication paths for all remaining system connections for SAP S/4HANA Retail solutions.

Application	Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Store physical inventory	SAP S/4HANA – <i>store system</i>	RFC (or other protocol that supports IDocs)	Application data	-
POS interface	SAP S/4HANA – <i>POS system</i>	RFC (or other protocol that supports IDocs)	Application data	Credit card information
	SAP S/4HANA – <i>POS system</i>	SOAP	Application data	-
Interface to space management systems	SAP S/4HANA – <i>space optimization system</i>	RFC	Application data	-

13.13.1.2.2 Authorizations in Retail

Note

For general information about the authorization concept used by SAP S/4HANA, see [User Administration and Authentication \[page 10\]](#).

SAP S/4HANA Retail uses the authorization concept provided by the ABAP platform. Therefore, the recommendations and guidelines for authorizations as described in the *ABAP Platform Security Guide* also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF09`) on the AS ABAP and the User Management Engine's user administration console on the AS Java.

Standard Roles

For information about the standards roles that are available for

- SAP S/4HANA Retail for merchandise management, see <https://help.sap.com/s4hana> choose your version and go to [Product Assistance](#) > [Industries](#) > [Consumer Industries](#) > [Retail \(Retail and Fashion\)](#) > [Retail for Merchandise Management](#).
- SAP S/4HANA for fashion and vertical business solutions, see <https://help.sap.com/s4hana> choose your version and go to [Product Assistance](#) > [Industries](#) > [Consumer Industries](#) > [Retail \(Retail and Fashion\)](#) > [Fashion and Vertical Business](#).

Standard Authorization Objects

For information about the standard authorization objects that are used in

- SAP S/4HANA Retail for merchandise management, see <https://help.sap.com/s4hana> choose your version and got to ► *Product Assistance* ► *Industries* ► *Consumer Industries* ► *Retail (Retail and Fashion)* ► *Retail for Merchandise Management* ► *Marketing and Merchandising* ► *Master Data Management* ► *Authorization Objects for Merchandise Management* ►.
- SAP S/4HANA for fashion and vertical business solutions, see <https://help.sap.com/s4hana> choose your version and got to ► *Product Assistance* ► *Industries* ► *Consumer Industries* ► *Retail (Retail and Fashion)* ► *Fashion and Vertical Business* ► *Brand Management and Merchandising* ► *Brand Management and Merchandising* ► *Marketing and Brand Data and Insights* ► *Authorization Objects for Fashion and Vertical Business* ►.

13.13.1.2.3 Deletion of Personal Data in Retail

SAP S/4HANA Retail solutions might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on SAP Help Portal at https://help.sap.com/viewer/product/SAP_S4HANA_ON-PREMISE/. Choose a version and then go to ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects (Data) and Available Deletion Functionality

Application	Application Objects	Provided Deletion Functionality
Allocation	Application-specific data used in the following transactions: WA01 WA02 WA03 WA04 WA08 WA30 WA35	Transaction WA09

Application	Application Objects	Provided Deletion Functionality
Alternate Historical Data	<p>Application-specific data used in the following transactions:</p> <p>MDRD1 - MDRD3</p> <p>MAHD1 - MAHD3</p>	<p>Transaction MAHD4 can be used to delete entries in the Alternate Historical Data tables.</p> <p>Transaction MDRD4 can be used to delete delivery relationships.</p>
Article Discontinuation	<p>Application-specific data used in the following transactions:</p> <p>WRF_DIS_SEL</p> <p>WRF_DIS_MON</p>	ILM object MM_MATNR
Assortment	<p>Application-specific data used in the following transactions:</p> <p>WSOA1</p> <p>WSOA2</p> <p>WSOA3</p> <p>WSO1</p> <p>WSO2</p> <p>WSO3</p> <p>WSO4</p> <p>WSO5</p> <p>Tables:</p> <p>WRSZ</p> <p>WLK1</p> <p>WSOH</p>	<p>Transaction WSOA4 can be used to delete assortments.</p> <p>Transactions WSOA2/WSOA6 can be used to delete assortment users (customers).</p>
Assortment List	<p>Application-specific data used in the following transactions:</p> <p>WDBM_HPR</p> <p>WJB5</p> <p>WBBS</p> <p>WBBS_ALV</p>	Assortment List Reorganization: report RWDPOSRS
Automatic Document Adjustment	Transactions MEI1 - MEI5	ILM object MM_EKKO

Application	Application Objects	Provided Deletion Functionality
Investment Buying	Application-specific data used in the following transactions: WLB1 WLB2 WLB6	Report RWF FW _DELETE_CUSTOMERS
Load Building	Application-specific data used in the following transactions: WLB4 WLB5 WLB7 WLBA WLBB WLB13	Report RWVLB_DELETE_LOGTABLES
Merchandise Distribution	Application-specific data used in the following transactions: WF10 WF10A WF20 WF30 WF60 WF70	Transaction WA40 can be used to delete FRET entries that have status <i>Completed</i> .
Planning Workbench	Transaction WWP1	For non-application-specific data, functionality is provided by other relevant applications.
POS Interface – Inbound		For non-application-specific data, functionality is provided by other relevant applications.
POS Interface – Monitor		Deletion reports RWPUDTST and RWPUDLST
POS Interface – Outbound		For non-application-specific data, functionality is provided by other relevant applications.

Application	Application Objects	Provided Deletion Functionality
Price Catalog Processing – Inbound	W_PRICAT_MAINTAIN W_SYNC	Reports: W_PRICAT_DELETE (<i>Delete Inbound Price Catalogs</i>) W_PRICAT_DELPOS (<i>Delete PRICAT Items</i>)
Price Planning Workbench		Reports for the deletion of budgets and price plans: RWRP_PPW_BUDG_DELETE RWRP_PPW_PPD_DELETE RWRP_PPW_PPD_DELETE_DIRECT Destruction object: RWRP_PPW_PPD_DESTRUCTION
Promotions	Table WALE Transaction WAK5	ILM objects: W_PROMO_AD W_MARKDOWN
Replenishment	Application-specific data used in the following transactions: WRMO WR60	ILM object MM_MATNR
Sales Price Calculation	Application-specific data used in the following transactions: VKP1-VKP8 VKPB	ILM object W_KALK
Site Master	Transactions WB01-WB03	ILM object WS_ACSITE

Application	Application Objects	Provided Deletion Functionality
Subsequent Settlement	Application-specific data used in the following transactions: MEB2 MEB3 MEB5 MEB6 MEB8 MEB9 MEBS MEBB MEBV MEB7 MEU3	ILM object SD_AGREEM
Tickets and Additionals	Application-specific data used in the following transactions: WTAM WTR1	ILM object WTADDI
Vendor Managed Inventory	Application-specific data used in the following transactions: WVM1 WVM2 WVM3 WVM4	Report RWVMI_DELETE_EDMMS

Relevant Application Objects and Available Deletion Functionality Provided by Other Applications Used by SAP S/4HANA Retail solutions

- **Sales**
For information, see [Deletion of Personal Data in Order and Contract Management \[page 589\]](#).
- **Sourcing and Procurement**
For information, see [Deletion of Personal Data \[page 659\]](#).
- Customer and supplier master data
For information, see [Deletion of Personal Data \[page 739\]](#).

Relevant Application Areas and Available EoP/WUC Functionality

Application	Solution Implemented for Application-Specific Data	Further Information
Allocation	End of purpose (EoP) check	CL_ALLOCATION_CV_EOP_CHECK CVP_IF_APPL_EOP_CHECK~CHECK_PARTNERS
Alternate Historical Data	not applicable	Tables do not contain any customer or supplier data.
Article Discontinuation	not applicable	For non-application-specific data, functionality is provided by Sourcing and Procurement.
Assortment	not applicable	An end of purpose (EoP) check is not provided because customer and supplier numbers used in the tables do not indicate any business relationships.
Assortment List	not applicable	An end of purpose (EoP) check is not provided because supplier numbers used in the tables do not indicate any business relationships.
Automatic Document Adjustment	not applicable	For non-application-specific data, functionality is provided by Sourcing and Procurement.
Investment Buying	not applicable	For non-application-specific data, functionality is provided by Sales.
Load Building	not applicable	For non-application-specific data, functionality is provided by Sales.
Merchandise Distribution	End of purpose (EoP) check	CL_ALLOCATION_CV_EOP_CHECK CVP_IF_APPL_EOP_CHECK~CHECK_PARTNERS
Planning Workbench	not applicable	For non-application-specific data, functionality is provided by Sales.

Application	Solution Implemented for Application-Specific Data	Further Information
POS Interface – Inbound	not applicable	<p>POS interface uses documents that already exist in other SAP applications. These documents can be archived using the relevant archiving objects and deleted using the solutions (and end of purpose (EoP) checks) provided by the other SAP applications. For example, documents used in POS interface inbound SOAP service can be archived using application interface framework (AIF).</p> <p>An end of purpose (EoP) check for Customizing is not provided because partner information is stored anonymously in Customizing tables.</p>
POS Interface – Monitor	not applicable	<p>POS interface uses documents that already exist in other SAP applications. These documents can be archived using the relevant archiving objects and deleted using the solutions (and end of purpose (EoP) checks) provided by the other SAP applications.</p>
POS Interface – Outbound	not applicable	<p>POS interface uses documents that already exist in other SAP applications. These documents can be archived using the relevant archiving objects and deleted using the solutions (and end of purpose (EoP) checks) provided by the other SAP applications.</p> <p>An end of purpose (EoP) check for log tables is not provided because partner information is not shown in the application at this time, a deletion report exists, and there is no business need to archive the log status of data preparation.</p>
Price Catalog Processing – Inbound	End of purpose (EoP) check	<p>CL_PRICAT_EOP_CHECK_CV</p> <p>CVP_IF_APPL_EOP_CHECK~CHECK_PARTNERS</p>

Application	Solution Implemented for Application-Specific Data	Further Information
Price Planning Workbench	not applicable	An end of purpose (EoP) check is not provided because supplier numbers in pricing documents represent supply source information but do not indicate any business relationship to the supplier.
Promotions	End of purpose (EoP) check	CL_PROMOTION_CV_EOP_CHECK CVP_IF_APPL_EOP_CHECK~CHECK_PARTNERS
Replenishment	not applicable	For non-application-specific data, functionality is provided by Sourcing and Procurement.
Sales Price Calculation	not applicable	An end of purpose (EoP) check is not provided because supplier numbers in pricing documents represent supply source information but do not indicate any business relationship to the supplier.
Site Master	Where-used check (WUC)	CL_T001W_WUC
Subsequent Settlement	End of purpose (EoP) check	CVP_SD_EOP_CHECK_MM_REBATE
Tickets and Additional	not applicable	For non-application-specific data, functionality is provided by Sourcing and Procurement.
Vendor Managed Inventory	not applicable	For non-application-specific data, functionality is provided by Sourcing and Procurement.

Configuration: Simplified Blocking and Deletion

- You define the settings or authorization management in Customizing for *Cross-Application Components* under ► *Data Protection* ► *Authorization Management* ►. For more information, see the Customizing documentation.
- You configure the settings related to the blocking and deletion of customer and supplier master data in Customizing for *Logistics - General* under ► *Business Partner* ► *Deletion of Customer and Supplier Master Data* ►.

13.13.1.2.4 Deletion of Personal Data in Fashion and Vertical Business

Use

SAP S/4HANA for fashion and vertical business fashion might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on SAP Help Portal at https://help.sap.com/viewer/product/SAP_S4HANA_ON-PREMISE/.

Choose a version and then go to ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►

For more information about the deletion of personal data that might be used in fashion and vertical business applications refer to [Deletion of Personal Data in Retail \[page 762\]](#).

Relevant Application Objects (Data) and Available Deletion Functionality

Application	Application Objects	Provided Deletion Functionality
Configure Release Check Variant	ARUN_RC_RUN	Report ARUN_RC_RUN_DES
Schedule Alignment	RFM_DRS_ALIGNMENT_DESTRUCTION	Report RFM_DRS_ALIGNMENT_DESTRUCTION
Configure Demand Sorting Rule	ARUN_DSORT_RULE_DESTRUCTION	Report ARUN_SORT_RULE_DES
Configure Demand Grouping Rule	ARUN_DGROUP_RULE_DESTRUCTION	Report ARUN_GROUP_RULE_DES

Relevant Application Areas and Available EoP/WUC Functionality

Application	Solution Implemented for Application-Specific Data	ILM Object
Stock requirements/Pegging (MD04P)	Not applicable	Not Applicable
	<p>i Note</p> <p>An End of Purpose (EoP) check is not provided because customer and supplier information displayed do not indicate any business relationships.</p>	
Season Workbench	EoP check	Not Applicable
Mass Repricing Report	EoP check	SD_VBAK MM_EKKO
Mass ATP Report	EoP check	SD_VBAK MM_EKKO
Season Redetermination Report for Sales Order	EoP check	SD_VBAK
Season Redetermination Report for Purchase Order	EoP check	MM_EKKO
Season Redetermination Report for Stock Transport Order	EoP check	MM_EKKO
VAS Redetermination Report for Sales Order	EoP check	SD_VBAK
VAS Redetermination Report for Purchase Order	EoP check	MM_EKKO
VAS Redetermination Report for Stock Transport Order	EoP check	MM_EKKO
Multi Ship to Order (MSO) Explosion Report for Sales Order	EoP check	SD_VBAK
Split and Change of Purchase Orders	EoP check	MM_EKKO
Transportation Chain – Dateline Workbench Report	EoP check	MM_EKKO

Application	Solution Implemented for Application-Specific Data	ILM Object
Maintain Release Determination Rule	EoP check	CVP_IF_APPL_EOP_CHECK
Configure Release Check Variant	EoP check	CVP_IF_APPL_EOP_CHECK
Define Default Segment Values	EoP check	CVP_IF_APPL_EOP_CHECK
Configure Demand Sorting Rule	EoP check	CVP_IF_APPL_EOP_CHECK
Configure Demand Grouping Rule	EoP check	CVP_IF_APPL_EOP_CHECK

13.13.1.2.5 Payment Card Security According to PCI-DSS

Note

The Payment Card Industry Data Security Standard (PCI-DSS) was jointly developed by major credit card companies in order to create a set of common industry security requirements for the protection of cardholder data. Compliance with this standard is relevant for companies processing credit card data. For more information, see the official website of the PCI Security Standards Council at <https://www.pcisecuritystandards.org>.

This section of the security guide supports you in implementing payment card security aspects and outlines steps that need to be considered to be compliant with the PCI-DSS.

Please note that the PCI-DSS covers more than the following steps and considerations. Complying with the PCI-DSS lies completely within the customer's responsibility, and we cannot guarantee the customer's compliance with the PCI-DSS.

For current information about PCI-DSS, see also SAP Note [1609917](#).

PCI-relevant POS (Point-of-Sale) sales can be processed in SAP S/4HANA Retail for merchandise management for financial postings and inventory management. Depending on the configuration of the POS solution, the data transferred to SAP S/4HANA Retail for merchandise management can contain credit card information that needs to be handled according to the PCI Standard. In this case, the card data has to be encrypted during inbound processing. The relevant asynchronous communication methods are the IDocs with the message type `WPUBON` (Upload Sales Documents per Receipt), and message type `WPUTAB` (Upload End-of-Day Closing POS).

For more information about **Archiving**, **RFC Debugging**, **Forward Error Handling (FEH)** and **Card Verification Values (CVV)**, see [Payment Card Security According to PCI-DSS \[page 132\]](#).

Interfaces (IDoc/Services)

i Note

Note that IDoc segments cannot store credit card numbers in clear text due to the PCI security standard compliance. Once an IDoc is being processed within the IDoc Framework, all values are temporarily stored, including the clear text credit card number.

For more information about how to process customer-specific IDocs containing credit card information, go to https://help.sap.com/s4hana_op_2020, enter *Handling Sensitive Data in IDocs* into the search bar, press , and open the search result with that title.

Encryption/Decryption and Storage of the Encrypted Number

IDoc Encryption/Encryption process: IDoc data records are sent to the BAdI implementation `IDOC_PCI_ENCR_IM` that is used for the PCI DSS inbound IDoc encryption. The process of encrypting the credit card number starts by identifying the segment with credit card information in the IDoc record structure. The data from the relevant segments `E1WPZ02` and `E1WPB06` is mapped to the internal record structure in order to retrieve the card GUID, the name of the credit card institution number, and the credit card number. After this, the security level of the credit card institution is verified in Customizing:

- If the security level is set to 2, the credit card number is encrypted.
- If the security level is set to 1, the credit card number is masked.

The card GUID and the encryption type are mapped to the structure for decryption and a message is displayed that informs the user whether the encryption was successful. After this, the final check for consistency is performed.

Decryption process: The process of decrypting the credit card number starts by identifying the segment in the IDoc record structure that contains the credit card information. The data from the relevant segments `E1WPZ02` and `E1WPB06` is mapped to the internal record structure in order to retrieve the card GUID, the type of encryption, and the credit card number. The encryption type is set to the fixed value 2. The credit card number is decrypted and a message is displayed that informs the user whether the encryption was successful.

- The BAdI implementation name for PCI DSS inbound IDoc decryption is `IDOC_PCI_DECRYPTION_IM`.
- One of the IDoc database encryption/decryption (`IDOC_DATA_MAPPER`, `IDOC_DATA_CRYPTION`) is called before saving to the IDoc database and the other after reading from it.

Customizing

Maintain the following settings in Customizing:

- The basic settings for payment cards: In Customizing for *SAP Customizing Implementation Guide* under [▶ Cross-Application Components ▶ Payment Cards ▶ Basic Settings ▶ Assign Checking Rule ▶](#).
- The settings for the encryption save mode: Define whether existing GUIDs for credit cards are reused. The default setting is set to reuse the existing GUID. You can adapt the default with a customer-specific BAdI implementation, using the enhancement spot `ES_WPOS_PCA_SECURITY` and the BAdI definition `WPOS_PCA_SECURITY`.
- The security settings for the credit card institute: In Customizing for *SAP Customizing Implementation Guide* under [▶ Cross-Application Components ▶ Payment Cards ▶ Basic Settings ▶ Make Security Settings for Payment Cards ▶](#). For an example for security settings for payment cards, refer to the following entries:
 - Security Level: *Masked Display* and *Encrypted When Saved*

- Access Log: *Logging of unmasked display*
- Visible Characters for Masking:
At start: 4
At end: 4
- The settings for masking the credit card number: In the customizing table of the transaction WECRYPTDISPLAY, maintain the settings for the *Assignment of Encrypted Segment* field as follows:
 - *Message Type*: WPUBON
 - *Segment Type*: E1WPB06
 - *Field Name*: KARTENNR
 and
 - *Message Type*: WPUTAB
 - *Segment Type*: E1WPZ02
 - *Field Name*: KARTENNR

13.13.1.3 Last Mile Distribution (LMD)

13.13.1.3.1 Deletion of Personal Data

Use

Last Mile Distribution (LMD) might process data (personal data) that is subject to the data protection laws applicable in specific countries/regions. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Last Mile Distribution (LMD)	<p>For more information, see https://help.sap.com/s4hana, choose your version, and go to ► <i>Product Assistance</i> ► <i>Industries</i> ► <i>Consumer Industries</i> ► <i>Consumer Products</i> ► <i>Last Mile Distribution for Direct Distribution</i> ►</p>	<ul style="list-style-type: none"> • Route Header Data (table LMD_COM_ROUTES) • Route Status (table LMD_SM_OBJ_STAT) • Route Status History (table LMD_SM_HISTORY) • Stops (table LMD_COM_STOPS) • Document Headers (table LMD_COM_DOC_HDRS) • Document Items (table LMD_COM_DOC_ITMS) • Collections (table LMD_COM_COLS) • Collected Payments (table LMD_COM_COL_PAYS) • Collection Assignments (table LMD_COM_COL_PASS) • Check-Out/Check-In for Payments (table LMD_COM_COCIPAYS) • Check-Out/Check-In for Products (table LMD_COM_COCIPRDS)

Relevant Application Objects and Available EoP/WUC Functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Last Mile Distribution	<p>The following references to business partners are available in LMD route data database tables:</p> <ul style="list-style-type: none"> • Main driver and co-driver in route header data (table LMD_COM_ROUTES) • Ship-to party in stops (table LMD_COM_STOPS) • Ship-to party and sold-to party in document headers (Table LMD_COM_DOC_HDRS) <p>The following references to user data are available in LMD route data database tables:</p> <ul style="list-style-type: none"> • Information about changes ("Changed by") in route status table (Table LMD_SM_OBJ_STAT) • Information about changes ("Changed by") in route status history (Table LMD_SM_HISTORY) 	<p>A business partner end of purpose (EoP) check is supported for this data.</p> <p>For more information, go to https://help.sap.com/s4hana, enter <i>Business Partner End of Purpose (EoP) Check in Last Mile Distribution</i> into the search bar, start the search, and open the search result with that title.</p>

13.13.1.3.2 Virus Scanning

With Last Mile Distribution, you are enabled to upload attachments from mobile devices. To prevent the upload of malicious files to the back-end, you can activate and set up one or more virus scanner based on the Virus Scanner Interface (VSI). The use of external virus scanning solutions and the blocking of MIME types is supported. External virus scanning solutions can be used with different Virus Scan Adapters.

For general information about virus scanning in SAP S/4HANA, see the [Virus Scanning \[page 24\]](#) section.

Additional information about the virus scan profile `/SCMS/KPRO_CREATE` is available in the [Virus Scanning in File Uploads \[page 24\]](#) topic in the *Virus Scanning* section.

For more information about virus scanners in Product Lifecycle Management (PLM), see the *API Implementation* topic.

Go to https://help.sap.com/s4hana_op_2020, enter *Product Lifecycle Management (PLM)* into the search bar, press , and open the search result with that title. Within the document, search for *API Implementation*.

For technical information about virus scan profiles and the `KPRO` virus scan profile configuration for `/SCMS/KPRO_CREATE`, see [1764839](#) and [851789](#).

13.13.1.4 Prepayment Agreements

13.13.1.4.1 Information Retrieval

Personal data can be retrieved by creating models in the *Information Retrieval Framework* (IRF).

Data subjects have the right to get information regarding their personal data that is undergoing processing. The information retrieval feature supports you in complying with the relevant legal requirements for data protection by allowing you to search for and retrieve all personal data for a specified data subject. The search results are displayed in a comprehensive and structured list containing all personal data of the data subject specified, subdivided according to the purpose for which the data was collected and processed.

Follow the instructions below to set up your data model.

Apart from setting up a data model, you must also maintain the purposes relevant to your organization.

- To generate the data model for your ILM object, execute transaction *DTINF_ADJUST_MODEL*. In the *ILM Object* field, enter *PPMG_AGR* and click *Generate*.
- To maintain the purpose relevant to your ILM object, execute transaction *DTINF_MAINTAIN_PURP*. Select *Assign ILM Objects* and from the *Assign ILM Objects* table, choose *PPMG_AGR*.
- To trigger the automated retrieval of all personal data, execute transaction *DTINF_START_COLL*. Enter the *Data Subject ID Type*, *Data Subject ID*, *Language* and *Purpose* and click *Execute*.
- To display and download the search results of the data collection process, execute transaction *DTINF_PROC_COLL*.

More Information

For more information about setting up and using the IRF, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Enterprise Technology* ► *ABAP Platform* ► *Administering the ABAP Platform* ► *Administration Concepts and Tools* ► *Solution Life Cycle Management* ► *Information Retrieval Framework (IRF)* ►.

For more information about data protection, see https://help.sap.com/s4hana_op_2020 under ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

13.13.2 Discrete Industries

13.13.2.1 Automotive

13.13.2.1.1 Vehicle processes for Wholesale and Retail

13.13.2.1.1.1 Authorizations

Vehicle Processes for Wholesale and Retail uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the Application Server ABAP Security Guide also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
C_AUTO_VMS	Vehicle Management System (VMS): Controls whether a user is allowed to execute VMS actions
C_AUTO_DPV	Dealer Portal VMS: Controls whether a user is allowed to execute dealer portal functions, for example, create a sales order without a vehicle

13.13.2.1.1.2 Deletion of Personal Data

Use

The Vehicle Management System (VMS) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Vehicle Management System (IS-A-VMS)	Archiving Object VEHICLE ILM Object VEHICLE

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Vehicle Management System (IS-A-VMS)	EoP	Check table VLCVEHICLE

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for [Cross-Application Components](#)→[Data Protection](#).

i Note

Vehicle Management System delivers two business events, which are exposed along with the Vehicle Identification Number (VIN). The VIN can indirectly refer to a person if information such as purchase order or sales order is attached to it. This must be kept in mind to restrict unknown subscriptions to the event and to thereby avoid security issues.

13.13.3 Energy & Natural Resources

13.13.3.1 Oil and Gas

13.13.3.1.1 Upstream Operations Management

13.13.3.1.1.1 Authorizations

SAP Oil & Gas uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also applies.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Roles - Backend

SAP delivers standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

In Oil & Gas, PFCG delta roles are used to access content in the application. To make the end-user role complete these roles must be used along with other roles delivered by SAP. Example roles are included in the table below. These roles are designed to support your IS-OIL business processes. The following roles are delivered:

Software Component IS-PRA

Role	Description
SAP_UPS_ALLOC_RES_APP	SAP Upstream Allocation Results
SAP_UPS_ALLOC_STAT_APP	SAP Upstream Network Allocation Status
SAP_UPS_BULKUPLOAD_APP	SAP UPS Upload Production Data
SAP_UPS_DEFER_EVT_APP	SAP Upstream View Deferment Events Application Role
SAP_UPS_DEFER_RES_APP	SAP Upstream Analyze Deferment Application Role
SAP_UPS_DEFER_WOEVN_APP	SAP Upstream Deferment Events for Work Orders Application Role

Role	Description
SAP_UPS_DTIMPORT	SAP Upstream Operations Management Data Import Role
SAP_SR_UOM_S4	NWBC Upstream Operations Management Role
SAP_UPS_FC_ACCESS_APP	SAP UOM Manage Access
SAP_UPS_FC_CALFCST_APP	SAP UOM Calculate Forecast
SAP_UPS_FC_GTHDATA_APP	SAP UOM Gather Data
SAP_UPS_FC_MNGPROJ_APP	SAP UOM Manage Projects
SAP_UPS_FC_RESULTS_APP	SAP UOM View Forecasting Results
SAP_UPS_FDC_APP	SAP Upstream Field Data
SAP_UPS_FIXERRORS_APP	SAP Upstream Fix Errors
SAP_UPS_MNGHIER_APP	SAP UPS Manage Hierarchy
SAP_UPS_FC_APFCSST_APP	SAP UOM Approve and Publish Forecast
SAP_UPS_NTWK_MODEL_APP	SAP Upstream Network Modeling

Critical Combinations

Roles Creation in PFCG

1. Copy the standard role (SAP_UPS_DEFER_RES_APP) to a new role and change the authorization as required by the user.
For example, role created is Z_RES_CREATE, and the authorizations provided to this role are to view particular production network (HK_PN) and to create and display the event for this particular production network. The user, to which this role is assigned, will only be able to view or create the event for this particular production network.
2. Assign the role to the user.
3. Log in with the same user in the application.
4. Create event for the same.

Standard Fiori Business Roles

The following table shows the standard Fiori business roles used in Upstream Operations Management:

Software Component UIS4HOP1 (UI for S/4HANA On Premise)

Role	Description
SAP_BR_BUSINESS_ANALYST_IOG	Business Analyst (IOG)
SAP_BR_DEFERMENT_ANALYST_IOG	Deferment Analyst (IOG)
SAP_BR_FC_ANALYST_PROD_IOG	Forecast Analyst - Production (IOG)
SAP_BR_FIELD_OPERATOR_IOG	Field Operator (IOG)
SAP_BR_FORECAST_MANAGER_IOG	Forecast Manager (IOG)
SAP_BR_FORECAST_SPECIALIST_IOG	Forecast Specialist (IOG)
SAP_BR_HYDROCARBON_ANALYST_IOG	Hydrocarbon Analyst (IOG)
SAP_BR_PROD_DATA_SPEC_IOG	Production Data Specialist (IOG)
SAP_BR_MASTER_DATA_IOG	Master Data Specialist (IOG)

13.13.3.1.1.2 Internet Communication Framework Security (ICF)

For Oil and Gas, Upstream Operations Management (UOM) module the following services are needed:

- Allocation
 - GHO_WDA_ALLOC_MC_OIF (Capture Measurements)
 - GHO_WDA_ALLOC_RESULTS_OIF (Display Allocation Results)
 - GHO_WDA_ALLOC_RULES_OIF (Process Allocation Rules)
 - GHO_WDA_ALLOC_MRH_OIF (Process MRH Rules)
- Network Object
 - GHO_WDA_NETOBJ_OIF (Create a Network Object)
 - GHO_WDA_NETOBJ_OIF (Change a Network Object)
 - GHO_WDA_NETOBJ_OIF (Display a Network Object)
 - GHO_WDA_OG_ENTITY (Create an Oil & Gas Entity)
 - GHO_WDA_OG_ENTITY (Change an Oil & Gas Entity)
 - GHO_WDA_OG_ENTITY (Display an Oil & Gas Entity)
- Ownership
 - Division of Interest
 - GHO_WDA_OWN_OIF (Create a Division of Interest (DOI))

- GHO_WDA_OWN_OIF (Change a Division of Interest (DOI))
- GHO_WDA_OWN_OIF (Display a Division of Interest (DOI))
- GHO_WDA_OWN_NET_ASG_OIF (Assign a Division of Interest to Network Objects)
- Scale Method
 - GHO_WDA_OWN_SM_OIF (Create a Sliding Scale Method)
 - GHO_WDA_OWN_SM_OIF (Change a Sliding Scale Method)
 - GHO_WDA_OWN_SM_OIF (Display a Sliding Scale Method)
- Business Partner
 - Process Business Partner
- Owner Transfer Request
 - GHO_WDA_OWN_TRO_GAF (Create an Owner Request)
 - GHO_WDA_OWN_TRO_GAF (Change an Owner Request)
 - GHO_WDA_OWN_TRO_GAF (Display an Owner Request)
- Reports (Display Only)
 - GHO_WDA_OWN_RPT_OIF (Oil & Gas Business Partner Report)
 - GHO_WDA_OWN_RPT_OIF (Division of Interest Owners)
 - GHO_WDA_OWN_RPT_OIF (Well Completions Assigned to Division of Interest)
 - GHO_WDA_OWN_RPT_OIF (Division of Interest History Report)
 - GHO_WDA_OWN_RPT_OIF (Ownership Entitlement Results)

For running SAP Fiori applications for Upstream Operations Management, please activate some of the common SICF nodes on the front-end server (SAP Gateway).

Activate the following SICF nodes specific to Upstream Operations Management SAP Fiori applications:

- UIS4HOP1 - UI for S/4HANA On Premise
 - /sap/bc/ui5_ui5/sap/ups_alloc_ress1
 - /sap/bc/ui5_ui5/sap/ups_alloc_stas1
 - /sap/bc/ui5_ui5/sap/ups_blkuploads1
 - /sap/bc/ui5_ui5/sap/ups_commonss1
 - /sap/bc/ui5_ui5/sap/ups_defer_evts1
 - /sap/bc/ui5_ui5/sap/ups_defer_ress1
 - /sap/bc/ui5_ui5/sap/ups_def_woevts1
 - /sap/bc/ui5_ui5/sap/ups_fc_accesss1
 - /sap/bc/ui5_ui5/sap/ups_fc_apfcsts1
 - /sap/bc/ui5_ui5/sap/ups_fc_calfcts1
 - /sap/bc/ui5_ui5/sap/ups_fc_cmpress1
 - /sap/bc/ui5_ui5/sap/ups_fc_ghdatas1
 - /sap/bc/ui5_ui5/sap/ups_fc_mngpross1
 - /sap/bc/ui5_ui5/sap/ups_fc_results1
 - /sap/bc/ui5_ui5/sap/ups_fdcs1
 - /sap/bc/ui5_ui5/sap/ups_fixerrorss1
 - /sap/bc/ui5_ui5/sap/ups_mnghiers1
 - /sap/bc/ui5_ui5/sap/ups_md_mpns1

- Activate the following SICF nodes of OData services used by SAP Fiori applications:
 - /sap/opu/odata/sap/ups_bulk_upld
 - /sap/opu/odata/sap/ups_common
 - /sap/opu/odata/sap/ups_def_event
 - /sap/opu/odata/sap/ups_def_result
 - /sap/opu/odata/sap/ups_def_work_order
 - /sap/opu/odata/sap/ups_fc_appr_pub
 - /sap/opu/odata/sap/ups_fc_calc_fcst
 - /sap/opu/odata/sap/ups_fc_gatherdata
 - /sap/opu/odata/sap/ups_fc_mng_access
 - /sap/opu/odata/sap/ups_fc_mng_project
 - /sap/opu/odata/sap/ups_fc_view_res
 - /sap/opu/odata/sap/ups_field_data_capture
 - /sap/opu/odata/sap/ups_fix_error
 - /sap/opu/odata/sap/ups_hca_result
 - /sap/opu/odata/sap/ups_hca_status
 - /sap/opu/odata/sap/ups_mng_hierarchy
 - /sap/opu/odata/sap/ups_model_production_network

13.13.3.1.1.3 Other Security-Relevant Information

The following table shows an overview of the data flow in UOM in a two system DMZ environment. Data access is separated from the presentation layer, which is running on the second machine. The UI is accessed using HTTP or HTTPS.

Step	Description	Security Measure
User Interface: FPM-based ABAP Web-Dynpro with Unified Rendering	Data requests, updates, and actions are triggered from the UI.	ABAP WebDynpro, unified rendering, access using HTTP or HTTPS
PLM UI Framework	Infrastructure for communication between GUIBBs/WebDynpro context and SPI connector	
SPI Connector (DMZ System)	Acting like a proxy for the back end SPI connector.	Metadata is read from back end only
RFC	RFC based data transfer between DMZ system and ERP back end system; xstring based data transfer	Protocol switch to RFC; Allowlist for table based data transfer; Sync with meta data model in connector

Step	Description	Security Measure
SPI Connector (Back End System)	A standardized interface that is used to transfer data from the application service provider to the UI framework consumer.	Validation against metadata definition during data transfer
Application Service Provider	Implementation	Additional metadata definition

13.13.3.1.1.4 Information Report

Prerequisites

i Note

You need to implement the following notes to use Data Protection and Privacy in UOM:

- Data Privacy Requirement (DPP) DDIC: 2560898
- Data Privacy Requirement (DPP): 2586829

Vendor and Business Partner Where-Used Information Report (GHO_R_DPP_MAP_PERS_DATA)

This report shall provide a detailed where used list for the given vendor and business partner in UOM. For this, the report needs to be run with option `<Find Where-used Personal Data>`. The following technical details shall be provided:

- Table Name and description
- Field Name and description
- Personal Data identifier (V, B)
- Personal Data object ID

13.13.3.1.1.5 Deletion of Personal Data

Prerequisites

i Note

You need to implement the following notes to use Data Protection and Privacy in UOM:

- Data Privacy Requirement (DPP) DDIC: 2560898
- Data Privacy Requirement (DPP): 2586829

Simplified Blocking and Deletion: When considering compliance with data protection regulations, it is also necessary to consider compliance with industry-specific legislation in different countries. A typical potential scenario in certain countries is that personal data shall be deleted after the specified, explicit, and legitimate

purpose for the processing of personal data has ended, but only as long as no other retention periods are defined in legislation, for example, retention periods for financial documents. Legal requirements in certain scenarios or countries also often require blocking of data in cases where the specified, explicit, and legitimate purposes for the processing of this data have ended, however, the data still has to be retained in the database due to other legally mandated retention periods. In some scenarios, personal data also includes referenced data. Therefore, the challenge for deletion and blocking is first to handle referenced data and finally other data, such as business partner data.

Deletion of personal data: The processing of personal data is subject to applicable laws related to the deletion of this data when the specified, explicit, and legitimate purpose for processing this personal data has expired. If there is no longer a legitimate purpose that requires the retention and use of personal data, it must be deleted. When deleting data in a data set, all referenced objects related to that data set must be deleted as well. Industry-specific legislation in different countries also needs to be taken into consideration in addition to general data protection laws. After the expiration of the longest retention period, the data must be deleted.

Upstream Operations Management might process data that is subject to the data protection laws applicable in specific countries as described in SAP Note 1825544.

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. Upstream Operations Management uses SAP ILM to support the deletion of personal data as described in the following sections.

- SAP delivers an end of purpose check for the Upstream Operations Management
- SAP delivers a where-used check (WUC) for the Upstream Operations Management

13.13.3.1.1.5.1 End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases:

Phase one: The relevant data is actively used.

Phase two: The relevant data is actively available in the system.

Phase three: The relevant data needs to be retained for other reasons:

For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked.

Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

Display: The system does not display blocked data.

Change: It is not possible to change a business object that contains blocked data.

Create: It is not possible to create a business object that contains blocked data.

Copy/Follow-Up: It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.

Search: It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

13.13.3.1.1.5.1.1 Vendor/Business Partner Replacement Utility for End of Purpose

A replacement utility is provided to make the original vendor and business partner (BP), who have met EoP with a dummy vendor or BP, anonymous. The mapping between the original and the dummy vendor and business partner is retained temporarily (until retention period) in an audit table (GHO_DPP_T_MAP). The audit record is erased at the end of retention period. You have to run it when you decide to end the purpose for a vendor or business partner in UOM.

Following are the steps to execute the Utility report:

- Once a decision is made to end the purpose of a UOM vendor/business partner, the End of Purpose Utility report GHO_R_DPP_MAP_PERS_DATA with option <Execute End of Purpose> can be initiated.
- The report presents you with a selection screen offering two fields for input: MULTIDRAG
 - Type of Personal data object as Vendor or Business partner
 - Original Personal data ID (Vendor/BP Number to be replaced in UOM)
 - With option *Execute End of Purpose*
 - New Dummy Personal data ID (Vendor/BP Number by which Original Vendor/BP is to be replaced)
- On providing these mandatory inputs, you can continue with the execution of the report, which replaces the original vendor or business partner in the UOM database tables with the dummy vendor/BP.

The report output gives a confirmation of replacement of Original Vendor/BP Number by the Dummy Vendor/BP Number.

The report ends by recording the timestamps of this replacement run in a database table (GHO_DPP_T_MAP) for auditing purposes.

Make sure that you should replace one Vendor/BP at a time. During this process, there should not be made any changes in transactional data for a Vendor/BP which is being replaced.

i Note

If EoP for a certain vendor has been met, that is, you have run Vendor Replacement Utility to replace vendor, the application will show the end-of-purpose indicator and the start-of-retention-time date based on the ILM configuration.

- If vendor is not found in UOM, the system will bring up the following status: *PURPOSE_COMPLETION_STATUS* as 1 = (no business made with Vendor at all).
- If the vendor is found in UOM and not found in the audit table (filled by UOM vendor replacement utility), application the system will bring up the following status: *PURPOSE_COMPLETION_STATUS* as 2 = (business is ongoing with Vendor).
- If vendor is not found in UOM and is found in the audit table, the system will bring up the following status: *PURPOSE_COMPLETION_STATUS* as 3 = (business is completed with Vendor).

13.13.3.1.1.5.2 Where-Used Check (WUC)

i Note

The Where-Used Check functionality can be used only if you have used the *Vendor/Business Partner Replacement Utility for End of Purpose* tool utility tool, before you block data.

A where-used check is a simple check to ensure data integrity in case of potential blocking. The WUC for this product checks whether any dependent data for a vendor or central business partner (cBP) exists in the respective table. If dependent data exists, that is, if the data is still required for business activities, the system does not block that specific vendor or cBP.

If you still want to block the data, the dependent data must be first replaced (End of Purpose) by the replacement utility.

13.13.3.1.1.5.3 Process Flow

- Before destruction data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
- You do the following:
 - Run transaction IRMPOL and maintain the required residence and retention policies for the vendor (audit area: GENERAL)/business partner(audit area: BUPA_DP) with ILM object GHO_DPP_DES_MAP_DELETE).
 - Run transaction BUPA_PREPARE_EOP to enable the end of purpose check function for the business partner.
 - Run transaction CVP_PREPARE_EOP to enable the end of purpose check function for the vendor master.
- You delete data from mapping table and change documents by using the report GHO_DPP_DES_MAP_DELETE_DES for the ILM objects of Upstream Operations Management.

13.13.3.1.1.5.4 Change Log

Person-related data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to be able to track the changes made. If these changes are logged, at any time you can check which employee made which change and when.

Change log has been enabled for Vendor Specific fields in UOM. You can execute program RSSCD200 to get the change information of these documents.

Related Information

- Go to https://help.sap.com/s4hana_op_2020, enter *Services for Application Developers* into the search bar, press `Enter`, open the search result with that title, and navigate to [Change Documents](#).
- Go to https://help.sap.com/s4hana_op_2020, enter *Security Aspects for Lifecycle Management* into the search bar, press `Enter`, open the search result with that title, and navigate to [Auditing and Logging](#).

13.13.3.1.2 IS-OIL Downstream

13.13.3.1.2.1 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For the Fiori apps in the TSW area, following services are needed:

- My Nominations - TSW_MYNOMINATIONS_SRV_01
- Regional Inventory View - SW_REGIONAL_INVENTORY_SRV_01
- Mass Change Events - TSW_MYEVENTS_SRV
- TSW Tickets - TSW_TICKETS_SRV
- My Nomination Tickets - TSW_NOMINATIONTICKETS_SRV
- Supply Chain Visualization - TSW_VISUAL_SHIPMENT_SRV, VBI_APPL_DEF2_SRV
- Physical Inventory Capture IOG - Volume/Mass Reading - OIL_HPM_DS_PHYINVVMRAPP_SRV
- Physical Inventory Capture IOG - Gauge Reading - OIL_HPM_DS_PHYINV_GR_SRV
- Mobile Ticket Data Capture - TSW_MULTI_CHANNEL_TICKET
- Laytime and Demurrage - CMH_LAYTIMEDEMURRAGE_SRV
- Schedule Hydrocarbon Trips - CMH_SCHEDULEHYCTRIPS_SRV
- Scheduling Assistant - TSW_SCHEDULINGASSISTANT_SRV
- Mobile Event Data Capture - TSW_MOBILE_EVENTS_SRV

Use the transaction SICF to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information about ICF security, see the respective chapter in the ABAP Platform Security Guide.

13.13.3.1.2.2 Deletion of Personal Data

The *IS-OIL Downstream* might process data that is subject to the data protection laws applicable in specific countries as described in SAP Note 1825544.

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. The *IS-OIL Downstream* uses SAP ILM to support the deletion of personal data as described in the following sections.

- SAP delivers an end of purpose check for the *IS-OIL Downstream*
- SAP delivers a where-used check (WUC) for the *IS-OIL Downstream*

All applications register either an end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the customer and vendor master or a WUC. For information about the Customizing of blocking and deletion for *IS-OIL Downstream* application, see Configuration: Simplified Blocking and Deletion.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases.

- **Phase one:** The relevant data is actively used.
- **Phase two:** The relevant data is actively available in the system.
- **Phase three:** The relevant data needs to be retained for other reasons.
For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change a business object that contains blocked data
- **Create:** It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up:** It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- **Search:** It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see Process Flow and Configuration: Simplified Blocking and Deletion.

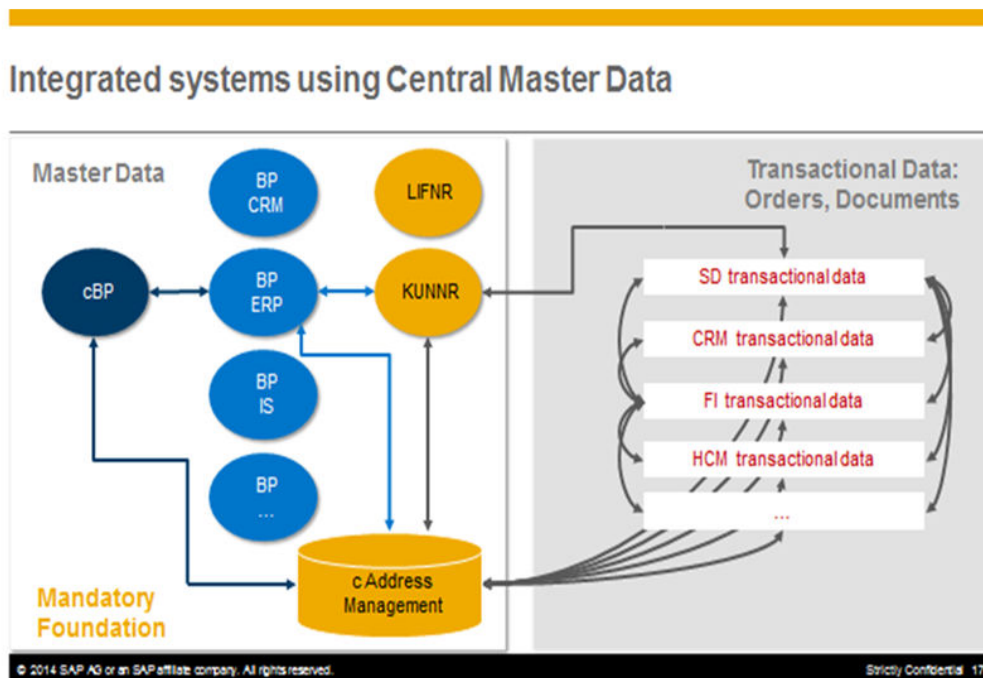
IS-OIL Downstream provides the following functionality for the EoP check of the Vehicle/Driver/Transport Unit:

- The application searches for the following data with relation to vehicle:
 - There are no open TD shipments where the vehicle is scheduled
 - There are no open nominations
 - Any shipment yet to be settled for shipment costing (VFKK- STBER)
 - If any of the transportation units are linked to a Vehicle (in OIGVTU table) is not blocked for EoP
 - Vehicle blocking checks if it is used in any Load ID which is not marked for deletion
 - Vehicle cannot be blocked if any document having this vehicle in TSW details tab (OIJ_EL_CP_LAYT-VEHICLE) is still not complete
- The application searches for the following data with relation to driver:
 - There should be no open TD shipments where the driver is assigned

- Driver blocking checks if it is used in any Load ID which is not marked for deletion.
- The application searches for the following data with relation to transport unit:
 - Vehicles linked to the transport unit has any open shipments
 - Vehicles linked to the transport unit has any open nominations
 - Vehicles linked to the transport unit has any shipment yet to be settled for shipment costing

Integration with Other Solutions

In the majority of cases, different installed applications run interdependently as shown in following graphic.



Relevant Application Objects and Available Deletion Functionality



Application	Detailed Description	Provided Deletion Functionality
IS-OIL Downstream	<p>The customer/vendor blocking report will check the consuming application to determine end of purpose of the customer/vendor.</p> <p>In an IS-OIL system, in addition to the EOP checks performed by SD,MM ,FI application the checks for usage of the customer/vendor in <i>IS-OIL Downstream</i> application has to be made.</p> <p>The IS-OIL application has to register itself under the customer master data and vendor master data as consuming applications that need to be checked for EoP . EOP. Check logic in IS-OIL will be delivered in the class <code>CVP_OIL_EOP_CHECK</code> .</p> <p>When destroying data from the database or archives, the links to GOS attachments are destroyed using central BAdI implementations. These links are determined using entries maintained in the ILM object-specific Customizing for BOR object type and BOR key determination. For more information, see 2935406</p>	<p>ILM Enabled Archiving objects:</p> <ul style="list-style-type: none"> OIG_DRIVER OIG_VEHICLE OIG_TPUNIT OIJ_NOMIN OIJ_TICKET IS_OIFSPBL <p>Data Destruction objects:</p> <ul style="list-style-type: none"> OIJ_SCHED_DESTRUCTION OIJ_PARTNER_DESTRUCTION OIA_EXGDOCU_DESTRUCTION OIL_TAS_TPI_DESTRUCTION
Decoupled TSW TSW_ECC	<p>The customer/vendor blocking report will check the consuming application to determine end of purpose of the customer/vendor.</p> <p>In a Decoupled TSW scenario , the checks for usage of customer/vendor in TSW application specific documents like nomination is made.</p> <p>The <code>TSW_ECC</code> application has to register itself under the customer master data and vendor master data as consuming applications that need to be checked for EoP . EOP Check logic in <code>TSW_ECC</code> will be delivered in the class <code>CVP_TSW_ECC_CHECK</code>.</p>	<p>ILM Enabled Archiving objects:</p> <ul style="list-style-type: none"> OIG_VEHICLE OIG_TPUNIT OIJ_NOMIN OIJ_TICKET IS_OIFSPBL <p>Data Destruction objects:</p> <ul style="list-style-type: none"> OIJ_SCHED_DESTRUCTION OIJ_PARTNER_DESTRUCTION

Process Flow

1. Before archiving data, you must define residence time and retention periods in *SAP Information Lifecycle Management* (ILM).
 - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and vendor master in SAP S/4HANA (ILM objects: FI_ACCPAYB, FI_ACCRECV, FI_ACCKNVK).
 - Run transaction IRMPOL and maintain the required retention policies for the ILM objects of *IS OIL Downstream*, application or *Decoupled TSW*.
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available
3. To determine which business partners have reached end of purpose and can be blocked, you do the following:
 - Run transaction CVP_PRE_EOP to execute the end of purpose check function for the customer master and vendor master in SAP S/4HANA.
4. To unblock blocked business partner data, you do the following
 - Request unblocking of blocked data by using the transaction BUP_REQ_UNBLK.
 - If you have the needed authorization for unblocking business partner data, you can unblock the requested data by running the transaction CVP_UNBLOCK_MD for customer master data and vendor master data in SAP S/4HANA.
5. You delete data by using the transaction ILM_DESTRUCTION for the ILM objects of *IS OIL Downstream* or *Decoupled TSW*.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management under [Data Protection](#) > [Authorization Management](#)  For more information, see the Customizing documentation.
- Define the settings for blocking under [Data Protection](#) > [Blocking and Unblocking](#) > [Business Partner](#) 

IS-OIL Downstream provides the following reports for blocking Vehicle, Driver and Transport Unit:

- **OIG_BLOCK_VEHICLE - Block Vehicle Master Data**
 You can use this report to block IS-OIL vehicle master data that are no longer required for any business purpose. As it is still within the retention period, the data is blocked, but not, deleted. The blocked data is no longer available for any business transactions or business use and is no longer displayed in existing business objects. You can neither create nor edit new business objects or conduct follow-up activities on blocked data.
 The determination of whether data can be blocked is in accordance with the end of purpose (EoP) check. When all applications confirm that there is either no business related to the data or that its original purpose is completed, the master data can be blocked. Once the vehicle master data is blocked, only users that have a role based on the following attributes can display blocked data:
 - Authorization object O_OIG_VEH
 - Activity 03, DISPLAY
- **OIG_BLOCK_DRIVER- Block Driver Master Data**
 You can use this report to block IS-OIL driver master data that are no longer required for any business purpose. As it is still within the retention period, the data is blocked, but not, deleted. The blocked data is no longer available for any business transactions or business use and is no longer displayed in existing

business objects. You can neither create nor edit new business objects or conduct follow-up activities on blocked data.

The determination of whether data can be blocked is in accordance with the end of purpose (EoP) check. When all applications confirm that there is either no business related to the data or that its original purpose is completed, the master data can be blocked. Once the driver master data is blocked, only users that have a role based on the following attributes can display blocked data:

- Authorization object O_OIG_DRV
 - Activity 03, DISPLAY
- **OIG_BLOCK_TRANS_UNIT - Block Transport Unit Master Data**
You can use this report to block IS-OIL transport unit master data that are no longer required for any business purpose. As it is still within the retention period, the data is blocked, but not, deleted. The blocked data is no longer available for any business transactions or business use and is no longer displayed in existing business objects. You can neither create nor edit new business objects or conduct follow-up activities on blocked data.
The determination of whether data can be blocked is in accordance with the end of purpose (EoP) check. When all applications confirm that there is either no business related to the data or that its original purpose is completed, the master data can be blocked. Once the transport unit master data is blocked, only users that have a role based on the following attributes can display blocked data:
 - Authorization object O_OIG_VTU
 - Activity 03, DISPLAY

13.13.3.1.2.3 Read Access Logging

If no trace or log is stored that records which business users have accessed data, it is difficult to track the person(s) responsible for any data leaks to the outside world. The *Read Access Logging* (RAL) component can be used to monitor and log read access to data and provide information such as which business users accessed personal data, for example, of a business partner, and in which time frame.

IS-OIL Downstream provides Read Access Logging configuration for IS-OIL TD Driver License Number. For more information, see SAP Note 2609910.

Read Access Logging is activated for the Display Driver transaction.

In RAL, you can configure which read-access information to log and under which conditions.

For general information on Read Access Logging, go to https://help.sap.com/s4hana_op_2020, open the product assistance, and navigate to ► *Cross Components* ► *Data Protection* ► *Security Safeguards Regarding Data Protection* ► *Read Access Logging (RAL)* ►.

13.13.3.1.2.4 Information Retrieval

Data subjects have the right to get information regarding their personal data undergoing processing. The information retrieval feature supports you to comply with the relevant legal requirements for data protection by allowing you to search for and retrieve all personal data for a specified data subject. The search results are displayed in a comprehensive and structured list containing all personal data of the data subject specified, subdivided according to the purpose for which the data was collected and processed.

More Information

For more details on the implementation of Information Retrieval for *IS- OIL Downstream*, refer to the steps in the SAP Note [2959312](#), to create and enable IRF models.

13.13.3.1.3 Remote Logistics Management

13.13.3.1.3.1 Deletion of Personal Data

The *Remote Logistics Management (RLM)* might process data that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. The *Remote Logistics Management* uses SAP ILM to support the deletion of personal data as described in the following sections.

- SAP delivers an end of purpose check for the *Remote Logistics Management*

All applications register either an End of Purpose (EoP) check in the Customizing settings for the blocking and deletion of the customer and vendor master or a Where Used Check (WUC). For information about the Customizing of blocking and deletion for *Remote Logistics Management* application, see Configuration: Simplified Blocking and Deletion.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases.

- **Phase one:** The relevant data is actively used.
- **Phase two:** The relevant data is actively available in the system.
- **Phase three:** The relevant data needs to be retained for other reasons. For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change a business object that contains blocked data
- **Create:** It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up:** It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- **Search:** It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see Process Flow and Configuration: Simplified Blocking and Deletion.

End of Purpose Check in RLM

The end-of-purpose check for RLM ensures data integrity in the event of potential blocking. It checks whether the Vendor or Customer passed is present in the RLM specific tables and returns the following status:

- If there is no data present in the RLM tables the system returns a status of '1' (No business made with Vendor or Customer) back to the blocking report.
- If there is data present in the RLM tables the system returns a status of '2' (Business is ongoing with Vendor or Customer) back to the blocking report.

End of Purpose Check in ERP Customer or Vendor

Application	Rule	Check
RLM-P Shipping and Container Management	Do not block the customer or vendor if there are any open status containers which have the customer or vendor as a partner.	Checks table OIO_CNTNR for any open status containers.
RLM-R Returns Management	Do not block the customer or vendor if there are any open material returns or container returns which have the customer or vendor as a partner.	Checks table OIO_RT_RTDOC for any open status return documents.

Relevant Application Objects and Available Deletion Functionality

Archived business data is destroyed after the retention time has expired. This applies to the following application objects:

Application	Archive Objects	Requirement
RLM-P Shipping and Container Management	OIO_CTHST: RLM Container History Data OIO_CNTNR: RLM Container Master Data OIO_VOYAGE: RLM Voyage Data	Need to be ILM enabled



Application	Archive Objects	Requirement
RLM-R Returns Management	OIO_RTDOC: Returns Document OIO_OBJFLW: RLM Document Flow Index	Need to be ILM enabled

Process Flow

- Before archiving data, you must define residence time and retention periods in [SAP Information Lifecycle Management \(ILM\)](#).
 - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and vendor master in SAP S/4HANA (ILM objects: FI_ACCPAYB, FI_ACCRECV, FI_ACCKNVK).
 - Run transaction IRMPOL and maintain the required retention policies for the ILM objects of [Remote Logistics Management](#), application.
- You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
- To determine which business partners have reached end of purpose and can be blocked, you do the following:
 - Run transaction CVP_PRE_EOP to execute the end of purpose check function for the customer master and vendor master in SAP S/4HANA.
- To unblock blocked business partner data, you do the following:
 - Request unblocking of blocked data by using the transaction BUP_REQ_UNBLK.
 - If you have the needed authorization for unblocking business partner data, you can unblock the requested data by running the transaction CVP_UNBLOCK_MD for customer master data and vendor master data in SAP S/4HANA.
- You delete data by using the transaction ILM_DESTRUCTION for the ILM objects of [Remote Logistics Management](#).

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for [Cross-Application Components](#) under [Data Protection](#).

- Define the settings for authorization management under [Data Protection](#) > [Authorization Management](#)  For more information, see the Customizing documentation.
- Define the settings for blocking under [Data Protection](#) > [Blocking and Unblocking](#) > [Business Partner](#) 

13.13.3.2 Utilities

This chapter lists security-relevant aspects that have to be considered when using the SAP Utilities solution.

i Note

In addition to the topics below, please also see the chapter [Billing and Revenue Innovation Management \[page 141\]](#) in this guide.

13.13.3.2.1 Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

The `Industry Solution Migration Workbench` (ISMW) saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

Logical File Names / Path Names Used

The Migration Workbench (ISMW) uses the logical file name `ISMW_FILE` with the logical file path `ISMW_ROOT` to enable the validation of physical file names.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see about data storage security, see the respective chapter in the `SAP NetWeaver Security Guide`.

13.13.3.2.2 Enterprise Services Security

For general information, see the chapters on Web Services Security in the `SAP NetWeaver Security Guide`. For Utilities-specific processes, during which system-to-system communication (A2A communication) takes

place within a system landscape and processes that prepare for market communication with other market participants as part of intercompany data exchange, note the following:

i Note

If, as part of your company-specific processes, you have communication interfaces with other systems, you must also take their recommended security measures into account.

A2A Communication Within a System Landscape

During A2A communication, data is exchanged between an SAP system and an external system. This communication is based on enterprise services and can flow via a PI system as a data hub or directly between the respective systems (point-to-point). As identifying parameters, the SAP system uses internal values (such as the profile number) or parameters that are generally understood in the market (such as external point of delivery IDs). For information about the security measures relevant to A2A communication, see the *SAP NetWeaver Security Guide*. The authorization objects of the respective transactions provide these processes with additional security.

Market Communication in Intercompany Data Exchange

As part of intercompany data exchange, messages are sent from an SAP Utilities system to a PI system or a comparable upstream system to prepare for market communication with other market participants. The messages are then converted into a universally valid market format and sent on to other systems. As identifying parameters, the SAP system uses values that are generally understood in the market (such as external point of delivery IDs). Communication can take place using enterprise services or IDocs (ALE communication).

For more information about the necessary security measures, see the *SAP NetWeaver Security Guide*. The authorization objects of the respective transactions provide these processes with additional security.

13.13.3.2.3 Deletion of Personal Data

It may be necessary for SAP Utilities to process data that is subject to the data protection laws that are applicable in specific countries, as described in SAP Note [1825544](#).

The *SAP Information Lifecycle Management (ILM)* component supports the entire software lifecycle, including the storage, retention, blocking, and deletion of data. SAP Utilities uses SAP ILM to support the deletion of personal data. SAP delivers end of purpose checks for objects that are specific to SAP Utilities.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period for data consists of the following phases.

- **Phase one:** The relevant data is actively used.
- **Phase two:** The relevant data is actively available in the system.
- **Phase three:** The relevant data needs to be retained for other reasons. For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior as follows:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change a business object that contains blocked data
- **Create:** It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up:** It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- **Search:** It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three phase-based end of purpose check, see [Process Flow and Configuration: Simplified Blocking and Deletion](#).

Integration with Other Solutions

The end of purpose checks for SAP Utilities are based on those in the [Contract Accounts Receivable and Payable \(FI-CA\)](#) solution. You use transaction `FPDPR1` in the SAP menu under [Contract Accounts Receivable and Payable > Periodic Processing > For Data Protection > Check If Business Partner Can Be Blocked](#) to check the business partners for which the end of purpose has been reached.

SAP Utilities is also integrated with [SAP Sales and Distribution \(SD\)](#) and [SAP Customer Relationship Management \(CRM\)](#). Cross-system and cross-application end of purpose checks exist in both cases.

If for example a business partner is used in SAP Utilities (as part of SAP S/4HANA) and in SAP CRM, the end of purpose checks cover both applications, meaning that data for a blocked business partner cannot be accessed in either application.

Relevant Application Objects and Available Deletion Functionality

SAP Utilities uses SAP ILM to support the deletion of personal data. For more information, see the documentation for Information Lifecycle Management.

Relevant Application Objects and Available EoP Functionality

The following end of purpose checks exist:

- Check for open contracts without any open items in their contract account
- Check if all invoicing documents have been printed
- Check if all billing documents have been invoiced
- Check if the business partner is used in a franchise fee contract
- Check if the business partner is used in a loyalty account
- Check if the business partner is used as a service provider
- Check if the business partner is used as an owner
- Check for open disconnection documents for business partner
- Check if the business partner is used in the role `ISUI` (installer)
- Check for open error messages for the business partner in CRM replication monitoring

The checks for the SAP Utilities-specific object types are included in the enhancement spot `ISU_DPP_EOP_CHECK`. For more information, see the documentation for the Business Add-Ins in the system.






The functions for deleting and blocking the addresses of connection objects and device locations are provided by the report `RE_DPP_EOP_TECH_OBJ` (see Note [2615585](#)).

Process Flow

1. Before archiving data, you must define residence time and retention periods in *SAP Information Lifecycle Management* (ILM).
The protection of meter reading documents and EDM values related to blocked business partners requires a specific handling. Activate the new archiving features for meter reading documents and, if SAP EDM is in use, EDM profile values. To suppress any access to archived meter reading results and profile values, maintain the archiving object `S_ARCHIVE` with the objects `ISU_EABL` and `ISU_PROFV`. Further details are provided in the SAP Notes [2516189](#) and [2542233](#).
2. You choose whether data deletion is required for data stored in archive files or data stored in the database. This is also defined by the type of deletion functionality available
3. Proceed as follows:
 - Run transaction `IRMPOL` and maintain the required residence and retention policies for the central business partner (ILM object: `CA_BUPA`).
 - Run transaction `BUPA_PRE_EOP` to enable the end of purpose check function for the central business partner.
 - Run transaction `IRMPOL` and maintain the required residence and retention policies for the customer master and vendor master in SAP S/4HANA (ILM objects: `FI_ACCPAYB`, `FI_ACCRECV`, `FI_ACCKNVK`).
 - Run transaction `CVP_PRE_EOP` to enable the end of purpose check function for the customer master and vendor master in SAP S/4HANA.
 - Business users can request unblocking of blocked data using the transaction `BUP_REQ_UNBLK`.
 - If you have the required authorizations, you can unblock data by running transactions `BUPA_PRE_EOP` and `CVP_UNBLOCK_MD`.
 - You delete data using the transaction `ILM_DESTRUCTION` for the ILM objects in SAP Utilities.
 - For blocking or deleting technical addresses (connection objects and device locations), run report `RE_DPP_EOP_TECH_OBJ` (see SAP Note [2615585](#)).
 - If you use *SAP AMI Integration for Utilities*, schedule the replication report `REAMI_SIMPLEMDSYNC` (transaction `EAMISMDS`) in SAP IS-U on a regular basis.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management under [Data Protection](#) > [Authorization Management](#) . For more information, see the Customizing documentation.
- Define the settings for blocking under [Data Protection](#) > [Blocking and Unblocking](#) > [Business Partner](#) .
- If you use CDS view-based analytics or SAP Fiori apps for IS-Utilities, the enhancement implementation ISU_DPP_EOP_BP_UPD_ACT (BAI implementation BUPA_PURPOSE_EXPORT) must be activated in the enhancement spot / BAI BUPA_PURPOSE_EXPORT. Further details are provided in Note [2551390](#) .
- If you use SAP AMI Integration for Utilities, the external MDUS system must be informed about the end of purpose (see note [2538445](#) ). This is achieved using the AMI device replication enterprise service. Activate the business function ISU_AMI_5. Activate the feature for sending the corresponding section to the device replication service by setting the BAI enhancement implementation ISU_DPP_EOP_DEVICE_UPD_ACT to active (using transaction SE19). Run the initialization report REISU_DPP_AMI_DEVICE_USAGE to determine and store the data usage status for the devices determined. Activate the Customizing settings for simplified master data synchronization under the following Customizing path (Transaction SPRO):
SAP Utilities > Advanced Metering Infrastructure > Basic Settings > Define Simplified Master Data Synchronization.
- The Customizing for the reference customer in tables BCONTCONF and TEKND must not have any real equivalents, meaning that no real personal data can be used. See SAP Note [2630383](#)  for details.


Deletion of Machine Learning Data

Machine Learning for IS-U Meter Reading and IS-U Billing is fully embedded in SAP S/4HANA OP Utilities. No additional system is involved.

Machine Learning for IS-U Meter Reading and IS-U Billing creates and stores machine learning-related data in additional database tables. This data relates to meter reading documents and billing documents respectively. The database tables are ILM enabled and integrated with the ILM objects ISU_EABL (for IS-U Meter Reading) and ISU_BILL (for IS-U Billing). You must apply these ILM objects for data deletion.

13.13.3.2.4 Read Access Logging

The *Read Access Logging* (RAL) component can be used to monitor and log read-access to data and provide information such as which business users accessed personal data, for example, for a business partner, and when they did so.

In RAL, you can configure which read-access information is to be logged and the conditions under which you should do so. SAP delivers sample configurations for applications. To use these configurations, save the ZIP attachments from the SAP Note [2370371](#) . Extract these ZIP files and import the RAL configurations using the import function for configurations in transaction SRALMANAGER.

For general information on Read Access Logging, go to https://help.sap.com/s4hana_op_2020, open the product assistance, and navigate to ► *Cross Components* ► *Data Protection* ► *Security Safeguards Regarding Data Protection* ► *Read Access Logging (RAL)* ►.

13.13.3.2.5 SAP Waste & Recycling


13.13.3.2.5.1 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For SAP Waste and Recycling the service `EHVW_WASTE` is needed. Use the transaction `SICF` to activate the service.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information about Internet Communication Framework Services, go to https://help.sap.com/s4hana_op_2020, enter *Activating and Deactivating ICF Services* into the search bar, press , and open the search result with that title.

13.13.3.2.5.2 Deletion of Personal Data

SAP Waste and Recycling might process data that is subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#) .

The SAP *Information Lifecycle Management (ILM)* component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. SAP Waste and Recycling uses SAP ILM to support the deletion of personal data as described in the following sections.

SAP provides a check for the end of the usage and WUC (Where use Check) for SAP Waste and Recycling. The business partner assignments at the waste disposal facility (transaction `EWAELO4`) are checked (debtor, vendor and cBP for the owner of the waste disposal facility) due to the fact that waste disposal facilities are not part of the ILM implementation. If the assignment of the business partner data to the waste disposal facility is no longer valid, this data has to be removed from the waste disposal facility. After the removal of the business partner data from the waste disposal facility, this data is not further considered at the WUC.

All applications register either an end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the customer, vendor and central business partner.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases:

- Phase one: The relevant data is actively used.
- Phase two: The relevant data is actively available in the system.

- Phase three: The relevant data needs to be retained for other reasons. For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- Display: The system does not display blocked data.
- Change: It is not possible to change a business object that contains blocked data.
- Create: It is not possible to create a business object that contains blocked data.
- Copy/Follow-Up: It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- Search: It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see Process Flow and Configuration: Simplified Blocking and Deletion.

Integration with Other Solutions

In the majority of cases, different installed applications run interdependently as shown in following graphic.

Relevant Application Objects and Available Deletion Functionality

SAP Utilities uses SAP ILM to support the deletion of personal data. For more information, see the documentation for Information Lifecycle Management at <https://help.sap.com>.

Deletion Functionality

Application	Description	Deletion Functionality
Transaction EWAORDER	Standard application for changing waste disposal orders	ILM object ISU_EORDER
Transaction EWAWA01	Standard application for maintaining single position weighing processes	ILM object ISU_WPROC
Transaction EWAWA_MULTI	Standard application for maintaining multi position weighing processes	ILM object ISU_MWPROC
Transaction ELOC	Maintaining service time slices for containers	ILM Object ISU_SERVFQ

Relevant Application Objects and Available EoP/WUC Functionality

The following end of purpose checks exist:

- Check for customer and vendor assignments for waste disposal facilities
- Check for partner assignment of bulky orders

The checks for the SAP Waste and Recycling object types can be enhanced in the enhancement spot `EEWA_BF_DPP`. For more information, see the documentation for the Business Add-Ins in the system.





Process Flow

1. Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
3. You do the following:
 - Run transaction `IRMPOL` and maintain the required residence and retention policies for the central business partner (ILM object: `CA_BUPA`).
 - Run transaction `BUPA_PRE_EOP` to enable the end of purpose check function for the central business partner.
 - Run transaction `IRMPOL` and maintain the required residence and retention policies for the customer master and vendor master in SAP ERP (ILM objects: `ISU_ROUTE`, `ISU_SERVFQ`, `ISU_WPROC`).
 - Run transaction `CVP_PRE_EOP` to enable the end of purpose check function for the customer master and vendor master in SAP ERP.
4. Business users can request unblocking of blocked data by using the transaction `BUP_REQ_UNBLK`.
5. If you have the needed authorizations, you can unblock data by running the transaction `BUPA_PRE_EOP` and `CVP_UNBLOCK_MD`.
6. You delete data by using the transaction `ILM_DESTRUCTION` for the ILM objects of <application, component, scenario>.

For information about how to configure blocking and deletion for <application, component, scenario>, see Configuration: Simplified Blocking and Deletion.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for Cross-Application Components under Data Protection.

- Define the settings for authorization management in under Data Protection Authorization Management. For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for Cross-Application Components under  [Data Protection](#)  [Blocking and Unblocking](#)  [Business Partner](#) .

13.13.3.2.6 Multichannel Foundation for Utilities and Public Sector

13.13.3.2.6.1 Authorizations

The Multichannel Foundation for Utilities and Public Sector solution uses the authorization concept provided by the Application Server ABAP.

Therefore, the recommendations and guidelines for authorizations as described in the *Application Server ABAP Security Guide* also apply to the Multichannel Foundation for Utilities and Public Sector solution. The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator transaction on the Application Server ABAP (AS ABAP).

Reference Role Templates and Authorizations in SAP CRM

You create a reference user (UMC_REF_USR) during system installation. The reference user provides the necessary authorizations for each online user. This means the reference user can access data in the back end systems and Gateway.

PFCG role templates (SAP_CRM_UMC_ODATA and SAP_ISU_UMC_ODATA for SAP CRM and SAP S/4HANA, respectively) are delivered with SAP CRM and SAP S/4HANA, which can be used (together with role templates delivered by Gateway, for example, /IWBEP/RT_USS_INTUSR) to create the PFCG role for the reference user.

Reference Role Templates and Authorizations in SAP S/4HANA

For SAP S/4HANA, the PFCG role template (SAP_ISU_UMC_ODATA) is delivered with the SAP S/4HANA system, which can be used together with role templates delivered by Gateway, for example, /IWBEP/RT_USS_INTUSR to create the PFCG role for the reference user.

Service Role Templates and Authorizations in SAP CRM

In addition to the reference user, you create a service user (UMC_SRV_USR) during installation. The service user is responsible for creating the application users. Since the service user is used for anonymous logon, the user should be granted minimum authorizations.

PFCG role templates (SAP_CRM_UMC_SRV and SAP_ISU_UMC_SRV for SAP CRM and SAP S/4HANA, respectively) are delivered in SAP CRM and SAP S/4HANA systems, which can be used (together with role templates delivered by Gateway, for example, /IWBEP/RT_USS_SRVUSR) to create the PFCG role for the service user.

For more information, go to https://help.sap.com/s4hana_op_2020, enter *Roles in the SAP Gateway Landscape* into the search bar, press , and open the search result with that title.

Service Roles and Authorizations in SAP S/4HANA

For SAP S/4HANA, the PFCG role template `SAP_ISU_UMC_SRV` is delivered in SAP S/4HANA system, which can be used together with role templates delivered by Gateway, for example, `/IWBEP/RT_USS_SRVUSR` to create the PFCG role for the service user.

Creating and Assigning Roles in SAP CRM

To create the required users (`UMC_SRV_USR`, `UMC_REF_USR`), you must perform the following steps in SAP S/4HANA, SAP CRM, and the Gateway systems.

i Note

In role maintenance, choose **Utilities > Templates** to display the available templates, copy templates delivered by SAP, change the copies, and create templates for yourself. You will need the authorization *User Master Record Maintenance: User Groups (S_USER_GRP)* with value `*` in the fields `CLASS` and `ACTVT`. SAP template names start with the letter **S**; therefore, templates that you create must not start with **S**.

You require administrator authorizations to create roles and users, and to assign roles to users.

1. Create a role and enter a description.
2. Insert the authorizations using the role templates.
Depending on the system and the role type, you can combine different role templates; see the following table:

Templates	SAP CRM System	SAP S/4 HANA System	Gateway
UMC_SRV_USR	SAP_CRM_UMC_SRV	SAP_ISU_UMC_SRV	/IWFND/RT_GW_USR
	/IWBEP/RT_USS_SRVUSR	/IWBEP/RT_USS_SRVUSR	/IWBEP/RT_USS_SRVUSR
UMC_REF_USR	SAP_CRM_UMC_ODATA	SAP_ISU_UMC_ODATA	/IWBEP/RT_USS_INTUSR
	/IWBEP/RT_USS_INTUSR	/IWBEP/RT_USS_INTUSR	

i Note

Add additional required authorization objects `/IWFND/SRV`, `S_SECPOL` and `S_TCODE`

3. You must manually add authorization object `CRM_IUPROC` to the reference user in the SAP CRM system. The recommendation is to add activity 16 (execute) on all the processes (*) as shown below:
4. Verify and edit the authorizations, if necessary.
For the `UMC_SRV_USR`, check role access to the following services (authorization object: `S_SERVICE`):
 - Activate OData Services in the Gateway system.
 - `CRM_UTILITIES_UMC_URM` (SAP CRM and Gateway)
 - `CRM_UTILITIES_UMC_PUBLIC_SRV` (SAP CRM and Gateway)
 - `/IWBEP/USERMANAGEMENT` (SAP CRM and Gateway)

For the UMC_REF_USR, check role access to the following services (authorization object: S_SERVICE):

- Activate OData Services in the Gateway system.
- CRM_UTILITIES_UMC (for SAP CRM system and Gateway)
- ERP_UTILITIES_UMC (for SAP S/4HANA system and Gateway)
- /IWBEP/USERMANAGEMENT (for SAP CRM system and Gateway)

This is especially true when some function enhancements are carried out.

5. Generate the authorizations.
A profile is automatically generated for the role.
6. Assign the role to users (UMC_SRV_USR, UMC_REF_USR) and run a user master comparison to enter the generated profile into the user master record.

Creating and Assigning Roles in SAP S/4HANA

To create the required users (UMC_SRV_USR, and UMC_REF_USR), you must perform the following steps in SAP S/4HANA and the Gateway systems.

i Note

In role maintenance, choose **Utilities > Templates** to display the available templates, copy templates delivered by SAP, change the copies, and create templates for yourself. You will need the authorization *User Master Record Maintenance: User Groups (S_USER_GRP)* with value * in the fields CLASS and ACTVT. SAP template names start with the letter S; therefore, templates that you create must not start with S.

You require administrator authorizations to create roles and users, as well as to assign roles to users.

1. Create a role and enter a description.
2. Insert the authorizations using the role templates.
Depending on the system and the role type, you can combine different role templates; see the following table:

Templates	SAP S/4HANA System	Gateway System
UMC_SRV_USR	SAP_ISU_UMC_SRV	/IWFND/RT_GW_USR
	/IWBEP/RT_USS_SRVUSR	/IWBEP/RT_USS_SRVUSR
UMC_REF_USR	SAP_ISU_UMC_ODATA	/IWBEP/RT_USS_INTUSR
	/IWBEP/RT_USS_INTUSR	

i Note

Add additional required authorization objects /WFND/SRV, S_SECPOL and S_TCODE

3. Verify and edit the authorizations, if necessary.
For the UMC_SRV_USR, check role access to the following services (authorization object: S_SERVICE):
 - ERP_UTILITIES_UMC_URM (SAP S/4HANA and Gateway)

- `/IWBEP/USERMANAGEMENT` (SAP S/4HANA and Gateway): This only applies to the standalone SAP S/4HANA scenario

For the `UMC_REF_USR`, check role access to the following services (authorization object: `S_SERVICE`):

- `ERP_UTILITIES_UMC` (for SAP S/4HANA system and Gateway)
- `/IWBEP/USERMANAGEMENT` (for SAP S/4HANA system and Gateway)

This is especially true when some function enhancements are carried out.

4. Generate the authorizations.
A profile is automatically generated for the role.
5. assign the role to users (`UMC_SRV_USR`, `UMC_REF_USR`) and run a user master comparison to enter the generated profile into the user master record.

Related Information

- SAP Gateway Foundation Security Guide
Go to https://help.sap.com/s4hana_op_2020, enter *SAP Gateway Foundation Security Guide* into the search bar, press `Enter`, and open the search result with that title.
- User and Role Administration of Application Server ABAP
Go to https://help.sap.com/s4hana_op_2020, enter *User and Role Administration of Application Server ABAP* into the search bar, press `Enter`, and open the search result with that title.

13.13.3.2.6.2 Internet Communication Framework Security (ICF)

Security for the Multichannel Foundation for Utilities and Public Sector solution consists of SAP Gateway OData services and HTML5/SAP UI5-based Web-enabled content managed by the Internet Communication Framework (ICF) (transaction `SICF`).

You must activate the ICF services required for the applications you want to use.

i Note

You can also activate these services during the technical configuration.

The Multichannel Foundation for Utilities and Public Sector solution relies on the following services in SAP CRM:

- `UMCUI5`: An HTML5/SAP UI5-based Web-enabled interface to access the OData services
- `CRM_UTILITIES_UMC`: OData services from the SAP CRM system
- `CRM_UTILITIES_UMC_URM`: Multichannel Foundation for Utilities and Public Sector extension of the SAP Gateway `USERREQUESTMANAGEMENT` OData service
- `CRM_UTILITIES_UMC_PUBLIC_SRV`: Anonymous OData Service for products in SAP CRM
- `ERP_UTILITIES_UMC_URM` (logon user `UMC_SRV_USR`): OData services from the SAP S/4HANA system

In addition, the application also uses service `USERMANAGEMENT` from SAP Gateway.

The Multichannel Foundation for Utilities and Public Sector S/4HANA stand-alone solution relies on the following services:

- `ERP_ISU_UMC` (logon user/current user): Multichannel Foundation for Utilities and Public Sector extension of the Gateway `USERREQUESTMANAGEMENT` OData Service
- `ERP_UTILITIES_UMC`: OData services from the SAP S/4HANA system
- `ERP_ISU_UMC_PUBLIC` (logon user `UMC_SRV_USR`)

In addition, the application also uses the service `USERMANAGEMENT` from SAP Gateway.

Related Information

Go to https://help.sap.com/s4hana_op_2020, enter *Security Guides for Connectivity and Interoperability Technologies* into the search bar, press `Enter`, and open the search result with that title.

13.13.3.2.6.3 Data Protection and Privacy

Data Protection and Privacy

Use

The Multichannel Foundation for Utilities and Public Sector application uses session cookies. For more information, see [ICF and Session Security \[page 21\]](#).

→ Recommendation

You are recommended to activate secure session management and to use SSL to protect the network communications where these security-relevant cookies are transferred.

User request data is stored in SAP Gateway for processing. Depending on business needs and local regulations, you can delete some user requests after certain periods of time.

The Multichannel Foundation for Utilities and Public Sector solution is built upon SAP Gateway. To ensure your data is protected and cannot be accessed by anyone, we recommend that you refer to the [SAP Gateway Foundation Security Guide](#).

Go to https://help.sap.com/s4hana_op_2020, enter *SAP Gateway Foundation Security Guide* into the search bar, press `Enter`, open the search result with that title, and navigate to [Auditing and Logging](#).

13.13.3.2.6.4 Read Access Logging

Read Access Logging

Use

The **Read Access Logging** (RAL) component can be used to monitor and log read-access to data and provide information such as which business users accessed personal data, for example, for a business partner, and when they did so.

In RAL, you can configure which read-access information is to be logged and the conditions under which you should do so. SAP delivers sample configurations for applications. To use these configurations, save the ZIP attachments from the SAP Note [2370371](#). Extract these ZIP files and import the RAL configurations using the import function for configurations in transaction SRALMANAGER.

SAP Note [2373081](#) provides example content for RAL in Multichannel Foundation for Utilities and Public Sector that allows you to choose the attributes relating to bank account data or payment card data that are to be logged for each read access.

For general information on Read Access Logging, go to https://help.sap.com/s4hana_op_1909, open the product assistance, and navigate to ► [Cross Components](#) ► [Data Protection](#) ► [Security Safeguards Regarding Data Protection](#) ► [Read Access Logging \(RAL\)](#) ►.

13.13.3.2.7 SAP S/4HANA Utilities Integration with SAP Marketing Cloud

13.13.3.2.7.1 Consent

It is the responsibility of the utility company that uses the SAP S/4HANA Utilities integration with SAP Marketing Cloud solution to request and obtain consent of the data subjects (a natural person such as a customer, contact, or account) to use their personal data before replicating their business partner data from SAP S/4HANA Utilities to SAP Marketing Cloud. It is assumed that the users of SAP Marketing Cloud (for example, customers of SAP for Utilities solutions) have consent from their data subjects to transfer data from SAP S/4HANA Utilities to SAP Marketing Cloud for the purpose of marketing.

Before data gets transmitted from SAP S/4HANA Utilities for replication, the SAP S/4HANA Utilities integration with SAP Marketing Cloud offers the possibility to perform consent checks for the replication of the following objects:

- Contracts
- Interactions
- General data
- Sales contracts
- Utilities customer scores data




- Installation data

By enabling consent checks for those objects, data replication will only be performed on data that belongs to data subjects who have granted consent for marketing purposes. Consent checks for those objects can be enabled through Customizing.

The SAP S/4HANA Utilities integration with SAP Marketing Cloud only performs the consent checks against the consent records that are stored in Consent Administration of SAP S/4HANA. Therefore, you are required to maintain the consent records in Consent Administration of SAP S/4HANA. If you use another consent administration application, you must make sure to regularly import the consent records from that consent administration application into Consent Administration of SAP S/4HANA. For more information, see [Consent Administration \[page 36\]](#).

Important SAP Notes

The following table lists important SAP Notes about consent:

Title	SAP Note
Profiling Consent Check for Utilities Customer Score for SAP S/4HANA Utilities Integration with SAP Marketing Cloud	3057102 
Consent Withdrawal for Interaction Contacts Originating from Business Partner and Contract Account Data	3074944 
Consent Check for Business Partner and Contract Account for SAP S/4HANA Integration with SAP Marketing Cloud	3048468 

13.13.3.2.7.2 Deletion of Personal Data

Users can ask for deletion of their personal data. In addition, data can also automatically be deleted after a certain retention period to accommodate the user's right to be forgotten. To fulfill this requirement, the SAP S/4HANA Utilities integration with SAP Marketing Cloud replicates the business partner blocking and deletion events to SAP Marketing Cloud. For follow-on processing and handling of these events on SAP Marketing Cloud, see the *Administration Guide* of SAP Marketing Cloud and search for [Deletion](#).

Deletion of Agreements

When the end date of a utilities contract or a sales contract is reached, the corresponding marketing agreement remains on SAP Marketing Cloud. To maintain data integrity on SAP Marketing Cloud, it is the responsibility of the utility to clean the data on SAP Marketing Cloud, by deleting the agreement and agreement terms that are representing utilities contracts and sales contracts that have reached their end date.

13.13.3.2.7.3 Communication Channel Security

The SAP S/4HANA Utilities integration with SAP Marketing Cloud sends information to SAP Cloud Platform Integration for processing. Then, SAP Cloud Platform Integration sends the processed information to SAP Marketing Cloud.

The following table shows the communication paths used by the SAP S/4HANA Utilities integration with SAP Marketing Cloud, the protocols used for the connection, the types of data transferred, and the data that require special protection:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP Cloud Platform Integration	SOAP	Utilities technical master data and business master data	Business master data and personally identifiable information
SAP Marketing Cloud	OData	Utilities technical master data and business master data	Business master data and personally identifiable information

SOAP connections are protected with Web services security. Secure Sockets Layer (SSL) protocol protects OData HTTP communications.

13.13.3.2.7.4 Authorizations

The SAP S/4HANA Utilities integration with SAP Marketing Cloud uses the authorization concept provided by the SAP NetWeaver Application Server for ABAP (SAP NetWeaver AS for ABAP) component. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS for ABAP Security Guide also apply to the SAP S/4HANA Utilities integration with SAP Marketing Cloud.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. To maintain roles, use transaction `PF09` to launch the Profile Generator on SAP NetWeaver AS for ABAP.

Data Replication Framework Authorizations

In the SAP S/4HANA Utilities integration with SAP Marketing Cloud, the *Creating Outbound Messages* (`DRF_ADM`) authorization object is checked to determine whether the user is authorized to use the `DRFOUT` transaction to trigger data replication.

Service Role and User for SAP Business Workflow

The `SAP_WFRT` user with the *SAP Business Workflow: Service User* (`SAP_BC_BMT_WFM_SERV_USER`) role is delivered with the SAP S/4HANA system. This user is required and responsible for executing the SAP Business

Workflow functions. In the context of the SAP Marketing Cloud solution, this user calls the function modules that are bound to certain Business Object Repository (BOR) events.

13.13.3.2.7.5 Security for Additional Application

Certificate-Based Authentication with SAP Cloud Platform Integration

In the SAP S/4HANA Utilities integration with SAP Marketing Cloud, SAP S/4HANA Utilities communicates with SAP Cloud Platform Integration services by way of SOAP Web services (transaction `SOAMANAGER`). The communication channel between SAP S/4HANA Utilities and SAP Cloud Platform Integration is secured by HTTPS SSL encryption.

To establish secure communications between the SAP S/4HANA Utilities system and SAP Cloud Platform Integration, you must obtain the server certificate from SAP Cloud Platform Integration and then use the Trust Manager (transaction `STRUST`) to import it into the SAP S/4HANA Utilities system.

SAP S/4HANA Utilities Integration with SAP Marketing Cloud

The SAP S/4HANA Utilities integration with SAP Marketing Cloud should be used in conjunction with the *SAP S/4HANA Integration with SAP Marketing Cloud* integration package. This package is used to execute the replication of business partner data and product data from an SAP S/4HANA system to an SAP Marketing Cloud system. For more information about this integration package, see SAP API Business Hub and search for [SAP S/4HANA Integration with SAP Marketing Cloud](#).

13.13.3.2.8 Utilities Product Integration Layer

Authorizations

The Utilities Product Integration Layer (UPIP) uses the authorization concept provided by the SAP NetWeaver Application Server for ABAP (SAP NetWeaver AS for ABAP) component and SAP HANA business data platform. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS for ABAP Security Guide and SAP HANA apply to the UPIP. The SAP authorization concept is based on assigning authorizations to users based on roles.

13.13.3.2.9 S/4HANA Utilities for Customer Management

The SAP S/4HANA Utilities for Customer Management package supports business-to-consumer (B2C) contract management for residential customers. For residential customers, processes such as selling energy

products, changing budget billing plans, entering meter reading results, starting market communication, correcting bills, and changing master data are offered.

Deletion of Personal Data

In SAP S/4HANA Utilities for Customer Management there is a special contract type to process customer management processes: the **Utilities Sales Contract**. This contract stores personal data related information within a reference to an IS-U contract.

For deletion process based on ILM there can be used the ILM object CRMS4_IUCH.

If you want to add company specific settings, you can create your own report and use this one as a template. For more information, see the [Data Protection and Privacy \[page 31\]](#) section.

Information Retrieval

Based on the ILM object CRMS4_IUCH there can be used the shipped model (same name: CRMS4_IUCH) for the Information Retrieval Framework (IRF) to provide relevant personal related data currently existing in the system.

Read Access Logging

Read Access Logging for SAP S/4HANA Utilities for Customer Management. You can configure which read-access information to log and under which conditions. SAP delivers sample configurations for applications. In order to use these configurations, save the ZAIP attachments from the SAP Note [2369386](#). Extract these ZIP files and import the RAL configurations using the import function for configurations in transactionSRALMANAGER.

13.13.4 Financial Services

13.13.4.1 Banking

13.13.4.1.1 SAP Business Partner for Financial Services (FS-BP)

The security policy with *SAP Business Partner for Financial Services* (FS-BP) is very similar to the security policy with the central *SAP Business Partner* (SAP BP).

13.13.4.1.1 Authorizations

You create roles in *Customizing* for *SAP Banking* under ► *SAP Business Partner for Financial Services* ► *General Settings* ► *Business Partner* ► *Basic Settings* ► *Authorization Management* ►.

The authorization objects are the responsibility of the *SAP Business Partner. SAP Financial Customer Information Management* (FS-BP) is only responsible for the following authorization objects:

- **T_BP_DEAL** (*Standing Instructions/Transactions*)
You can use this authorization object to control the company code-dependent authorizations for displaying/creating/changing standing instructions.
There are standing instructions for:
 - Payment details
 - Derived flows
 - Correspondence
 - Transaction authorizations
- **B_BUPA_SLV** (*Selection Variant for Total Commitment*)
A selection variant includes various settings for the total commitment (such as which business partner roles and relationships can be used for the selection, or whether detailed information can be displayed).

If you activate the SACF scenario **FSBP_RATINGS** (*FS-BP: Scenario for Ratings and Credit Standing Data*) in the *Workbench for Switchable Authorization Check Scenarios* (transaction **SACF**), the following FS-BP authorization objects are also available:

- **B_BUPA_RAT** (*Business Partner: Ratings*)
You can use this authorization object to check whether a user has the authorization to create, change, display, or delete rating procedures. For each rating procedure, you can differentiate between an authorization for a permitted period or an authorization for any period. The prerequisite for this is that you have made the settings for the periods in *Customizing* for *SAP Banking* under ► *SAP Business Partner for Financial Services* ► *Settings for Financial Services* ► *General Settings* ► *Ratings/Credit Standing* ► *Ratings* ► *Set Rating Procedures and Ratings* ►.
- **B_BUPA_CRS** (*Business Partner: Credit Standing Data*)
You can use this authorization object to check whether a user has the authorization to display and change credit standing data.

13.13.4.1.1.2 Network and Communication Security

In the case of *Total Commitment*, SAP ERP communicates with other SAP systems (such as Account Management (FS-AM)). Communication with non-SAP systems is also possible.

Communication takes place using Remote Function Call (RFC).

13.13.4.1.1.2.1 Communication Destinations

Depending on the scenario, an RFC user is required for communication via Remote Function Call (RFC). This user requires the appropriate authorizations for the target system (such as FS-CML or FS-AM).

13.13.4.1.1.3 Data Protection

The data protection concept with SAP Business Partner for Financial Services (FS-BP) is very similar to the data protection concept with the central SAP Business Partner (SAP BP).

Integration with Agent Framework (FS-FND-AF)

SAP Business Partner for Financial Services can be used in conjunction with the Agent Framework to provide other participating applications with all changes made to business partner master data. The Agent Framework uses the Change Notification Service (CA-GTF-TS-CNS) and adds to it.

If you made the necessary settings in Customizing, the CNS generates so-called change pointers for each change made to a business partner. These change pointers can then be processed by the Agent Framework which sends the updated information to the participating applications. In addition to the change pointers, the system generates an image of the export object. These images are stored in table `FSBP_CNS_IMAGE` and contain personal data of the corresponding business partner. For data privacy reasons, you have to delete the processed change pointers regularly. You should therefore schedule a regular job to call one of the two deletion reports `CNS_CP_DELETE` or `CNS_CP_DELETE_MULT`.

More Information

For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 and go to

- [▶ Cross Components ▶ Data Protection ▶](#)

13.13.4.1.1.4 Data Storage Security

The authorization object `B_CCARD` controls access to the credit card information that is stored in the business partner. This control falls under the area of responsibility of the central *SAP Business Partner*.

You can use authorization groups (authorization object `B_BUPA_GRP`) to protect employee data.

If you activate the SACF scenario `FSBP_RATINGS` (*FS-BP: Scenario for Ratings and Credit Standing Data*) in the *Workbench for Switchable Authorization Check Scenarios* (transaction `SACF`), the following FS-BP authorization objects are also available:

- B_BUPA_RAT (*Business Partner: Ratings*)
- B_BUPA_CRS (*Business Partner: Credit Standing Data*)

13.13.4.1.2 Bank Customer Accounts (BCA)

13.13.4.1.2.1 Authorizations

The following standard roles are available in *Bank Customer Accounts (BCA)*, for example:

Role	Description
SAP_ISB_ACCOUNTS_ADMIN_AG	SAP Banking BCA: Administrator in Account Management
SAP_ISB_ACCOUNTS_ASSISTANT_AG	SAP Banking BCA: Assistant in Account Management
SAP_ISB_ACCOUNTS_STAFF_AG	SAP Banking BCA: Clerical Staff in Account Management

i Note

These standard roles are only samples and not suitable for operative usage.

Standard Authorization Objects

You can find the authorization objects and the related documentation in the system using transaction SU21 under the object class *IS_B Industry-Specific Solutions - Bank*.

For more information on authorization management and the authorization objects in *Bank Customer Accounts*, see the product assistance documentation, under [Enterprise Business Applications > Finance > SAP Banking > Bank Customer Accounts \(BCA\) > General Subjects > Authorization Administration > Authorization Objects](#).

Bank Customer Accounts (BCA) also contains the following business transaction events on the subject of authorizations:

Business Transaction Event	Description
SAMPLE_INTERFACE_00011040	AUTH1 account
SAMPLE_INTERFACE_00011700	Authorization checks in the information system

Business Transaction Event	Description
SAMPLE_INTERFACE_00011701	Authorization check in the information system (RFC)
SAMPLE_INTERFACE_00010950	Check management
SAMPLE_INTERFACE_00010210	Payment item dialog
SAMPLE_INTERFACE_00010410	Payment order dialog
SAMPLE_INTERFACE_00010411	Standing order dialog

13.13.4.1.2.2 Network and Communication Security

The table below shows the communication channels between systems used by *Bank Customer Accounts (BCA)*:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client with SAP GUI for Windows to application server	DIAG	All application data	Password, personal data
Application server to application server	RFC	All application data	Personal data (e.g. account balances)
Application server to application server	SOAP	All application data	Personal data (e.g. account balances)

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

→ Recommendation

We recommend that you use secure protocols (SSL, SNC) whenever possible.

For more information, see *Transport Layer Security* and *Transport Security for Web Services* in the ABAP Platform Security Guide.

Since *Bank Customer Accounts (BCA)* is based on SAP NetWeaver technology, for more information about network security see the *SAP NetWeaver Security Guide* at *Network and Communication Security*.

If you offer services on the Internet, you need to protect your network infrastructure with at least a firewall. You can increase the security of your system (or group of systems) by creating the groups in different network segments, each of which is protected from unauthorized access by a firewall.

⚠ Caution

Remember that unauthorized access can also come from inside if an intruder has already taken control of one of your systems.

Ports

BCA runs on SAP NetWeaver and uses ports from the AS ABAP or AS Java.

For more information, see *Ports of SAP NetWeaver Application Server for ABAP* and *AS JAVA Ports* in the *SAP NetWeaver Security Guide*.

13.13.4.1.2.3 Deletion of Personal Data in IS-B-BCA

Use

The *Bank Customer Accounts (IS-B-BCA)* component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
BKK	For more information, see SAP Note 2023415 ►.	BKK_BUPA_EVENT_EOP_CHECK ILM object FIBA_BUPA

Application	Detailed Description	Provided Deletion Functionality
BKK	For more information, see Archiving or Destroying Bank Customer Accounts Data, and SAP Note 2023417 .	ILM objects: <ul style="list-style-type: none"> • BKKPRENOTE • FIBA_ACCNT • FIBA_BKST • FIBA_CFBAL • FIBA_EFTEX • FIBA_EFTIN • FIBA_ENRCH • FIBA_EVLIM • FIBA_GL • FIBA_GLBAL • FIBA_HIERA • FIBA_HOLD • FIBA_INCAL • FIBA_ITEM • FIBA_ORDER • FIBA_PECAL • FIBA_PXPO • FIBA_STORD • FIBA_TERM • FIBA_TOTAL

Available Check

Implemented Solution: End of Purpose Check

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

13.13.4.1.2.4 Specific Read Access Log Configurations

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions. SAP delivers sample configurations for applications.

The scenario *Payment Document Display/Change/Create* (Tx WZR(1/2/3)) in *Settlement Management* (LO-AB) logs data in order to record any access to banking data related to a customer or a vendor. You can find the configurations as described in the [Read Access Logging \[page 33\]](#) chapter.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Configuration	Fields Logged	Business Context
LOAB_BANK	KOMWBRD-BANKL	Bank Keys
LOAB_BANK	KOMWBRD-BANKN	Bank account number
LOAB_BANK	KOMWBRD-BANKS	Bank country key
LOAB_BANK	KOMWBRD-BKONT	Bank country key
LOAB_BANK	KOMWBRD-BKREF	Reference specifications for bank details
LOAB_BANK	KOMWBRD-DTAMS	Instruction key for data medium exchange
LOAB_BANK	KOMWBRD-DTAWs	Indicator for Data Medium Exchange

13.13.4.1.2.5 Change Log

Personal data is subject to frequent changes. Therefore, for review purposes or as a result of legal regulations, it may be necessary to track the changes made to this data. When these changes are logged, you should be able to check which employee made which change, the date and time, the previous value, and the current value, depending on the configuration. It is also possible to analyze errors in this way. In *Bank Customer Accounts (BCA)* this is implemented via change document functionality.

For more information about *Change Documents*, choose the relevant SAP NetWeaver version and open the following documentation:

Under *Application Help*, go to *SAP NetWeaver Library*: [▶ Function-Oriented View](#) [▶ Application Server](#) [▶ Application Server ABAP](#) [▶ Other Services](#) [▶ Services for Application Developers](#) [▶ Change Documents](#) [▶](#)

13.13.4.1.2.6 Dual Control

To increase the security standard you should activate the principle of dual control.

The following is a list of the relevant objects and the corresponding activity in the Customizing of *Current Account System: Bank Customer Accounts (BCA)*, where you can set the indicator for the dual control.

i Note

The principle of dual control is **not** activated in the standard system.

Object	Customizing Activity
Account	Dual Control for Master Data
Account Balancing	Currency Changeover at Account Balancing and Principle of Dual Control
Account Closure	Master Data > Account > Account Closure > Release > Assign > ... >
Account Hierarchies	Activate Release Relevance for Account Hierarchies
Conditions	Enter Basic Settings for Conditions
Forward Order	Account Management > Release > Release Forward Orders > Assign > ... >
	Maintain Amount Limit/Principle of Dual Control for Payment Order
Hold Amount Limit	Maintain Hold Amount Limit/Principle of Dual Control
Limits	Maintain Principle of Dual Control for Limits
Notice on Amount	Dual Control for Notice Management
Payment Order	Account Management > Release > Release Payment Orders > Assign > ... >
	Maintain Amount Limit/Principle of Dual Control for Payment Order
Payment Item	Account Management > Release > Release Payment Items > Assign > ... >
	Maintain Amount Limit/Principle of Dual Control for Payment Item
Prenote	Account Management > Maintain Prenotes > Release > Assign > ... >
Standing Order	Account Management > Release > Release Standing Orders With Fixed Amount > Assign > ... >
	Account Management > Release > Release Standing Orders With Variable Amount > Assign > ... >

Object	Customizing Activity
	Maintain Amount Limit/Principle of Dual Control for Standing Order

13.13.4.1.3 Loans Management (FS-CML)

13.13.4.1.3.1 Authorizations

Authorization management for mortgage loans is based on the existing authorization concept in [Loans Management\(FS-CML\)](#).

The authorization check is performed according to the principle of inclusion, that is to say, if a user has authorization to activate a business transaction, he or she also has authorization to delete it. The authorization for making a posting includes the authorization for making a cancellation.

If other functions are called from a business transaction, the relevant authorization check is performed in this business transaction before the other function is accessed. This avoids any termination of the functions that are being called.


To set up your authorization management for mortgage loans, you can use the following roles included in the delivery scope:

Role	Description	Scope
Loans Officer	SAP_CML_LOANS_OFFICER	<ul style="list-style-type: none"> • Create, change, display, delete business partner • Collateral value calculation, credit standing calculation and decision-making • Maintain objects and securities • Create contracts, or transfer from application or offer • Enter disbursements • Process correspondence • Release loan (colleague or superior) • Process business operations (such as charges, individual posting, pay-off)

Role	Description	Scope
Credit Analyst	SAP_CML_CREDIT_ANALYST	<ul style="list-style-type: none"> • Create, change, display, delete business partner • Maintain loan enquiries, applications and offers • Calculate credit standing • Decision-making • Maintain limits • Calculate the collateral value • Maintain objects and securities
Rollover Officer	SAP_CML_ROLLOVER_OFFICER	<ul style="list-style-type: none"> • Loan rollover (individual and mass) • Process correspondence • Management of rollover file • Maintain condition tables
Staff Accountant for Loans	SAP_CML_STAFF_ACCOUNTANT	<ul style="list-style-type: none"> • Post transactions • Clearing • Create payments • Post and monitor incoming payments • Process waivers and write-offs • Cancellation • Accrual/deferral • Valuation • Generating accounting reports
Manager of Loans Department	SAP_CML_DEPARTM_MANAGER	<ul style="list-style-type: none"> • Release • Maintain condition tables • Change limits • Risk analysis • Monitor file (rollover or process management) • Monitor portfolio and portfolio trend using reports; reports and queries
Product Administrator	SAP_CML_PRODUCT_ADMIN	<ul style="list-style-type: none"> • Update reference interest rates • Maintain condition tables • Maintain new business tables

Role	Description	Scope
Technical Administrator	SAP_CML_TECHNICAL_ADMIN	<ul style="list-style-type: none"> • Perform mass runs (such as mass print run), set status of plan to completed, post planned records • Currency Conversion • Update reference interest rates and currency rates • Reorganization and data archiving • Define queries, drilldown reporting forms and reports • Maintain performance parameters • Analyze change pointers • Define export interfaces

You can assign these roles to the users in your company. Do not make any changes to the original roles, as these changes would be overwritten by the standard settings when the system is upgraded.

If you want to make adjustments, copy these roles. To do so, in the SAP Easy Access menu, choose [► Tools](#) > [Administration](#) > [User Administration](#) > [Role Administration](#) > [Roles](#) . Here you can group together authorizations for consumer loans into your own defined roles, and assign these to users in your departments, for example. In the first step you maintain the role menu. You can structure this yourself by adding and, if necessary, renaming files, transactions, and reports. In addition to manually grouping together the relevant transactions, you can also transfer these from the SAP menu or another role. You then maintain the authorizations for your role. The system proposes certain authorizations and their characteristics. You can also add more objects. Then you need to generate the authorization profile. Finally, you maintain the users who are to have the authorizations contained in the role. You can also use elements from organizational management, such as position in the organization. The advantage here is that you do not have to maintain the user assignment individually in each role if a person changes jobs. You can also use this function in release.

13.13.4.1.3.2 Network and Communication Security

Loans Management (FS-CML) does not communicate with other systems.

The only exception is the loan origination process. In this process, CRM serves as the entry system, and FS-CML as the back-end system. Communication takes place by means of XI.

13.13.4.1.3.3 Data Storage Security

The security of sensitive data in *Loans Management* (such as loan contracts, consumer loans, collateral values, credit standing calculations, collateral) is guaranteed by the general authorization concept of *Loans Management (FS-CML)*.

It is possible to display business partner data from *Loans Management*. You can use the authorization concept of central *SAP Business Partner* to protect this data.

For more information about authorizations and security of data storage, see <http://help.sap.com> under *SAP Business Partner Security*.

Using Logical Path and Filenames to Protect Access to the File System

The *Loans Management (FS CML)* application saves data in files in the file system. Therefore, you must provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal).

You can do this by specifying logical paths and file names in the system that map to the physical paths and file names. The system validates this mapping at runtime and if access is requested to a directory that does not match a defined mapping, then the system issues an error message.

The following lists the logical file names and paths used by *Loans Management (FS CML)* and the programs for which these file names and paths apply:

Logical File Names Used in This Application

The following logical file names have been created to enable the validation of physical file names:

- CML_PAYMENT_US
- Program using this logical file name:
- RFVD_AUTODRAFT_PROCESS
- RFVD_PAY_STOP
- Parameters used in this context: None
- CML_CREDIT_BUREAU
- Program using this logical file name:
- RFVD_CBR_PROCESS
- Parameters used in this context: None
- CML_MIGRATION_OBJECTS_LOGFILE_IN
- Program using this logical file name:
- RFVOBJ01
- Parameters used in this context: None
- CML_MIGRATION_OBJECTS_LOGFILE_OUT
- Program using this logical file name:
- RFVOBJ01
- RFVOBJ01_CREATE_STRUCTURE
- Parameters used in this context: None
- CML_MIGRATION_OBJECTS_PHYSFILE_IN
- Program using this logical file name:
- RFVOBJ01
- Parameters used in this context: None
- CML_MIGRATION_OBJECTS_PHYSFILE_OUT
- Program using this logical file name:
- RFVOBJ01

- RFVBJ01_CREATE_STRUCTURE
- Parameters used in this context: None
- CML_MIGRATION_COLLATERALS_LOGFILE_IN
- Program using this logical file name:
- RFVSIC01
- Parameters used in this context: None
- CML_MIGRATION_COLLATERALS_LOGFILE_OUT
- Program using this logical file name:
- RFVSIC01
- RFVSIC01_CREATE_STRUCTURE
- Parameters used in this context: None
- CML_MIGRATION_COLLATERALS_PHYSFILE_IN
- Program using this logical file name:
- RFVSIC01
- Parameters used in this context: None
- CML_MIGRATION_COLLATERALS_PHYSFILE_OUT
- Program using this logical file name:
- RFVSIC01
- RFVSIC01_CREATE_STRUCTURE
- Parameters used in this context: None

Logical File Paths Used in This Application

- The logical file names CML_PAYMENT_US and CML_CREDIT_BUREAU use the logical file path CML_ROOT.
- The logical file names CML_MIGRATION_OBJECTS_LOGFILE_IN, CML_MIGRATION_OBJECTS_LOGFILE_OUT, CML_MIGRATION_OBJECTS_PHYSFILE_IN, CML_MIGRATION_OBJECTS_PHYSFILE_OUT, CML_MIGRATION_COLLATERALS_LOGFILE_IN, CML_MIGRATION_COLLATERALS_LOGFILE_OUT, CML_MIGRATION_COLLATERALS_PHYSFILE_IN and CML_MIGRATION_COLLATERALS_PHYSFILE_OUT use the logical file path CML_MIGRATION

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

13.13.4.1.3.4 Deletion of Personal Data in FS-CML

Use

The Consumer Mortgage Loans (FS-CML) component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance

for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance*
 ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
CMLCONTRCT	Loan Master Data	Archiving object CMLCONTRCT ILM object CMLCONTRCT
CMLMODCALC	Model Calculation	Archiving object CMLMODCALC ILM object CMLMODCALC
CMLCRSTND	Credit Standing Calculation	Destruction object CML_CRSTAND-CALC_DESTRUCTION ILM object CML_CRSTANDCALC_DESTRUCTION
CMLINTPAR	Interested Party	Destruction object CML_INTEREST-PARTY_DESTRUCTION ILM object CML_INTERESTPARTY_DESTRUCTION
CMLCOLLATE	Collaterals	Destruction object CMLCOLLATE ILM object CMLCOLLATE
CMLCOLOBJ	Collateral Objects	Destruction object CMLCOLOBJ ILM object CMLCOLOBJ

Relevant Application Objects and Available EoP functionality

Application Object	Implemented Solution (End of Purpose Check)	Further Information
CMLCONTRCT	Loan Master Data	FLBP_CONTR_EVENT_EOP_CHECK
CMLMODCALC	Model Calculation	FLBP_MODEL-CALC_EVENT_EOP_CHECK
CMLCRSTND	Credit Standing Calculation	FLBP_CR_STND_EVENT_EOP_CHECK

Application Object	Implemented Solution (End of Purpose Check)	Further Information
CMLINTPAR	Interested Party	FLBP_INT_PAR_EVENT_EOP_CHECKN
CMLCOLLATE	Collaterals	FLBP_COLLTRL_EVENT_EOP_CHECK
CMLCOLOBJ	Collateral Objects	FLBP_COLLOBJ_EVENT_EOP_CHECK

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of `business partner master data` in `Customizing for Cross-Application Components` under `Data Protection`.

13.13.4.1.3.5 Specific Read Access Log Configurations

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions. SAP delivers sample configurations for applications.

During read accesses to the master data and transaction data of master loan contracts, the master loan contract number that the user uses for the access is logged.

During read accesses to the loan contracts for a business partner, the business partner number is logged. Furthermore, the IDs of all accounts and master loan contracts that the user could see as a result of this access are logged.

You can find the configurations as described in the [Read Access Logging \[page 33\]](#) chapter.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Interface Name	Fields Logged	Log Domain	Business Context
BankAccountContractProcessingManageLoanContractIn	VDARL-RANL VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
BankAccountContractProcessingQueryLoanContractIn	VDARL-CONTRACT_IBAN	BANKACCT_STANDARDID	IBAN

Interface Name	Fields Logged	Log Domain	Business Context
LoanDisbursementRequestERPByBasicDataQueryResponse_In	VDAUSZ-BANKL	BANK_ROUTINGID	Bank Key
LoanPendingPaymentWaiverRequestERPByBasicDataQueryResponse_In	VDGPO-BVTYP	BUSINESSPARTNERBANK DETAILS_ID	Business Partner Bank ID
	VDARL-HKTID	BANKACCT_ID	Account Number
	VDARL-SLAENDER	BANK_COUNTRYCODE	Bank Country Code
	VDARL-RDARNEHM	PARTYID	Business Partner ID
BankAccountContractProcessingQueryLoanContractBorrowerPartyChangeRequestIn	VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
	VDARL-RANL		
BankAccountContractProcessingManageLoanContractBorrowerPartyChangeRequestIn	VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
	VDARL-RANL		
	VDARL-RDARNEHM	PARTYID	Business Partner ID
BankAccountContractProcessingQueryLoanContractBorrowerPartyChangeRequestIn	VDGPO-BVTYP	BUSINESSPARTNERBANK DETAILS_ID	Business Partner Bank ID
	VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
	VDARL-RANL		
BankAccountContractProcessingManageLoanContractInterestOnArrearsRequestIn	VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
	VDARL-RANL		
	VDARL-RDARNEHM	PARTYID	Business Partner ID
	VDGPO-BVTYP	BUSINESSPARTNERBANK DETAILS_ID	Business Partner Bank ID
BankAccountContractProcessingQueryLoanContractInterestOnArrearsRequestIn	VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
	VDARL-RANL		
	VDARL-RDARNEHM	PARTYID	Business Partner ID
	VDAUSZ-BANKL	BANK_ROUTINGID	Bank Key
BankAccountContractProcessingQueryLoanContractCapitalTransferRequestIn	VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
	VDARL-RANL		
BankAccountContractProcessingManageLoanContractInterestOnArrearsRequestIn	VDARL-BUKRS	BANKACCTCONTR_ID	Account Contract Number
	VDARL-RANL		

Interface Name	Fields Logged	Log Domain	Business Context
tractCapitalTransferRequestIn	VDARL-RDARNEHM	PARTYID	Business Partner ID
	VDGPO-BVTYP	BUSINESSPARTNERBANK DETAILS_ID	Business Partner Bank ID
	VDAUSZ-BANKL	BANK_ROUTINGID	Bank Key
	VDARL-SLAENDER	BANK_COUNTRYCODE	Bank Country Code

More Information

For more information about the RAL sample Customizing for FS-CML, see SAP Note [2429604](#).

13.13.4.1.4 Collateral Management (CM)

Purpose

The purpose of this guide is to explain the security-specific features built-in for the SAP *Collateral Management (CM)*.

To understand the security features provided in CM, you must read the Application Server ABAP security guide that describes the basic security aspects and measures for SAP systems.

13.13.4.1.4.1 Authorizations

A multitude of standard roles are shipped with SAP *Collateral Management (CM)* in the SAP ECC 6.0. These roles are of exemplary character. The standard roles must be modified by the Customers based on their requirements.

i Note

The Customers must not use the standard roles in their production systems only with some medications. It is advisable without any modifications. Use the Profile Generator (transaction PFCG) to identify the standard roles and create additional roles.

The following roles are available in CM for banks:

Role	Purpose
SAP_FS_CMS_DISPLAY_ALL	Displaying all the entity objects in <i>CM</i> .

Role	Purpose
SAP_FS_CMS_MAINTAIN_ALL	Maintaining (Create, change and display only) all entity objects.
SAP_FS_CMS_MAINTAIN_ALL_PRC	Executing all the process related activities in addition to maintenance of objects
SAP_FS_CMS_CUST_ALL	Customizing
SAP_FS_CMS_ADMIN	CM administrator role
SAP_FS_CMS_COL_AUDITOR	Maintaining all the entity objects and the access to run all the reports in CM.
SAP_FS_CMS_CREDIT_MANAGER	Displaying collateral objects and collateral agreements.
SAP_FS_CMS_CREDIT_RISK_MANAGER	Maintaining collateral objects and collateral agreements and displaying receivables.
SAP_FS_CMS_LIQUIDATION_OFFICER	Maintaining liquidation measures.

Authorization Objects in CM

Technical name	Name
CMS_PCN_02	Authorization for activities (change request mode)
CMS_PCN_01	Authorization for activities (normal mode)
CMS_OMS1	Authorization for all collateral objects other than real estate (replace CMS_OMS from ECC 6.0 onwards)
CMS_OMS	Authorization for all collateral objects other than real estate (obsolete from ECC 6.0 onwards)
CMS_CAG	Authorization object for collateral agreements
CMS_RE	Authorization object for real estate objects in CM.
CMS_RBL	Authorization object for receivable in CM.

Characteristic Based Authorizations

In the Collateral Management, all the objects must belong to an administration organizational unit. The authorization objects for collateral objects (real estate and other collateral objects) and collateral agreements are based on a combination of the administration organizational unit and the entity type (assigned using a process control key). For receivables, the authorizations are based on the receivable organizational unit, the receivable status and the product. Authorizations for receivables is valid only for the receivables created in the CM or even the local copies of the receivables in external credit systems.

i Note

For example, you can use the attribute administration organization unit to differentiate between employee ,VIP and normal customers objects. You can also create objects in these organizational units as characteristics, which can then also be used to protect application data.

13.13.4.1.4.2 Network Communication and Security

The table below shows the communication paths used by the SAP *Collateral Management* (*CM*), the protocol used for the connections and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Financial Customer Information System (FS- Business Partner)	RFC	Business partner master data	
SAP Document Management System (DMS)	RFC	Document data	
Loans Management (CML)	RFC	Loan data	
SAP Business Information Warehouse (BIW)	IDoc and RFC	Collateral agreements, collateral objects, charges, collateral agreement – receivable assignment and calculations data	
SAP Bank Analyzer (Basel II)	IDoc and RFC	Collateral agreements, collateral objects, charges, collateral agreement – receivable assignment and calculations data	

The following RFC connections have to be set up for operating the *CM* . You are advised not to create the users belonging to these as dialog users.

- RFC communication with the Tool BW
- RFC communication within the Tool BW
- RFC communication in the context of import methods for the client copy. The relevant authorization objects are:
- S_TABU_DIS; S_RS_ICUBE; S_RS_ADMWB; S_RS_ISOUR; S_BTCH_ADM; S_ADMI_FCD; S_BTCH_JOB; S_RS_ODSO; S_RS_ISET

CM provides the following business application programming interfaces (BAPIs) for allowing external systems to connect to it:

- BAPI_CM_AST_GET_MULTI
- BAPI_CM_CAG_CREATE
- BAPI_CM_CAG_GETDETAIL_MULTI
- BAPI_CM_CAG_GET_BY_RBL
- BAPI_CM_GENLNK_RBL_ON_RBL_01
- BAPI_CM_GENLNK_RBL_ON_RBL_02
- BAPI_CM_SEC_GETDETAIL_MULTI
- BAPI_CM_RE_GETDETAIL_MULTI
- BAPI_CM_RIG_GETDETAIL_MULTI
- BAPI_CM_MOV_GETDETAIL_MULTI

B APIs are standard SAP interfaces and are important in the technical integration and in exchange of business data between SAP components and between the SAP and non-SAP components. B APIs enable you to integrate these components. They are therefore an important part of developing integration scenarios where multiple components are connected to each other, either on a local network or on the internet.

B APIs allow integration at the business level and not at the technical level. This provides for greater stability of the linkage and independence from the underlying communication technology.

The current requirement for B APIs in *CM* caters mainly to the migration scenarios. Hence these B APIs are not protected by special authorizations. Authorization checks for B APIs can be provided (in the future releases), if there are requirements for them.

CM also provides an extensive enhancement concept that offers user exits in the form of Business Add-Ins (BADIs).

Network Security and Communication Channels

Collateral Management (CM) uses the same communication channels that are described in the SAP NetWeaver AS security guide. No further customer-specific communication channels are provided. Hence the aspects and actions described in the SAP NetWeaver AS security guide (such as use of SAPRouter in combination with Firewall, use of Secure Network Communication (SNC), Communication Front-End-Application Server, connection to the database) also apply for *CM*.

13.13.4.1.5 Reserve for Bad Debt (FS-RBD)

Please Note: Monitor System Storage before file import and restrict access authority for RBD file upload.

13.13.4.1.5.1 Authorizations

The authorization concept used by *Reserve for Bad Debt (RBD)* is the same as the SAP authorization concept.

The authorization checks in RBD differentiate between the following dimensions:

- Activity
You use the activity to control what a user is permitted to do.
- Organization
At the level of the RBD-specific objects *RBD Area* or *Organizational Unit*, you specify which data the user is permitted to display or edit in accordance with the activity.

Standard Profiles

Preconfigured standard roles are not shipped with RBD. The following standard profiles are shipped with the SAP system:

Standard Profiles

Role	Description
S_A.SYSTEM	Access authorizations for the basis system only
S_A.ADMIN	Access authorizations for administration of the operational SAP system, but without access authorization for the following areas: <ul style="list-style-type: none"> • ABAP/4 Development Workbench • Maintenance of super users • Maintenance of standard profiles beginning with "S_A"
S_A.DEVELOP	Access authorizations for users who work with ABAP/4 Development Workbench
S_A.CUSTOMIZ	Access authorizations for basis settings in the Customizing system
S_A.USER	Access authorizations for end users (without access authorization for SAP work areas)

Authorization Objects

The following authorization objects are shipped with *Reserve for Bad Debt (RBD)*.

RBD Authorization Objects

Object	Description	Authorization Field <i>Activity</i>	Authorization Field <i>RBD Area</i>	Authorization Field <i>Organizational Unit</i>
RBD_ARCH	RBD: Archiving	03(<i>Display</i>)	Relevant	Not relevant

Object	Description	Authorization Field <i>Activity</i>	Authorization Field <i>RBD Area</i>	Authorization Field <i>Organizational Unit</i>
RBD_CUST	RBD: Customizing	16(<i>Execute</i>)	Not relevant	Not relevant
RBD_EDIT	RBD: Dialog & Batch	01(<i>Add or Create</i>) 02(<i>Change</i>) 03(<i>Display</i>) 05(<i>Lock</i>) 10(<i>Post</i>) 66(<i>Update</i>) 85(<i>Reverse</i>) 86(<i>Transfer Post</i>) 91(<i>Reactivate</i>) 95(<i>Unlock</i>) H1(<i>Deactivate</i>)	According to Customizing (table / IBS / CRB_RBD_P)	According to Customizing (table / IBS / CRB_ORGEIN)
RBD_REPO	RBD: Reporting	Not relevant	According to Customizing (table / IBS / CRB_RBD_P)	According to Customizing (table / IBS / CRB_ORGEIN)

Object	Description	Authorization Field <i>Activity</i>	Authorization Field <i>RBD Area</i>	Authorization Field <i>Organizational Unit</i>
/IBX/EDIT	IPX: Dialog & Batch	02(<i>Change</i>) 03(<i>Display</i>) 06(<i>Delete</i>) 10(<i>Post</i>) 21(<i>Transfer Valuation</i>) 23(<i>Maintain</i>) 41(<i>Delete on Database</i>) 43(<i>Release</i>) 46(<i>Aggregate Valuation</i>) 60(<i>Import</i>) 69(<i>Delete Valuation</i>) 71(<i>Analyze</i>) 78(<i>Assign</i>) 85(<i>Reverse</i>) 93(<i>Calculate</i>) 94(<i>Override</i>) c8 (<i>Confirm Change</i>)	According to Customizing (table / IBS / CRB_RBD_P)	Not relevant

⚠ Caution

For the *RBD Area* and *Organizational Unit* authorization fields, you can use the wildcard symbol “*”. If you use the wildcard symbol, access authorization is not checked for the relevant authorization field.

♣ Example

Description in relation to these authorization objects:

- The assignment of authorization object RBD_CUST with *activity* 16 authorizes the user to use the function *RBD: Duplicate Customizing Account Determination* (/ IBS / MRB_CUST_KTOFI).
- The assignment of authorization object RBD_EDIT with *activity* 01 and *RBD area* 0001 enables a user to display the data for an RBD account in RBD area 0001.
- The assignment of authorization object RBD_EDIT with *activity* 02, *RBD area* 0002, and *organizational unit* London enables a user to change data for an RBD account in RBD area 0002 that is assigned to the organizational unit “London”.

However, if the user is not assigned any other access authorizations, he or she cannot change an RBD account from RBD area 0002 that is assigned to the organizational unit “Tokio”.

- The assignment of authorization object RBD_EDIT with *activities* 02 and 10, and RBD area 0003 enables a user to create and post planned records for an RBD account in RBD area 0003. However, a prerequisite for this is that the principle of multiple control for posting planned records (risk provision proposals) has **not** been activated in Customizing for RBD.
- The assignment of authorization object RBD_REPO with *RBD area* "*" and *organizational unit* "*" allows a user to display the RBD data for all RBD areas and all organizational units, using the reports of the RBD information system.

Use of RBD Authorization Objects

RBD Area Menu, Account Management Folder

Transaction	Object (Activity)	RBD Area + Organizational Unit
Create RBD Account / IBS/ RB_KTO_INS	RBD_EDIT (01)	Relevant + Relevant
Change RBD Account / IBS/ RB_KTO_UPD	RBD_EDIT (02, 05, 10, 85, 95, H1)	Relevant + Relevant
Display RBD Account / IBS/ RB_KTO_DIS	RBD_EDIT (03) RBD_ARCH(03)	Relevant + Relevant Relevant + Not Relevant
Reactivate RBD account / IBS/ RB_KTO_REACT	RBD_EDIT (91)	Relevant + Relevant
Balance Sheet Transfer RBD / IBS/ RB_RECLAS	RBD_EDIT (not relevant)	Not Relevant + Not Relevant
ECF: Balance Sheet Transfer / IBS/ RB_ECF_RECLAS	RBD_EDIT (86)	Relevant + Not Relevant
ECF: Contract Reallocation / IBS/ RB_REALLOC	RBD_EDIT (86) RBD_REPO (not relevant)	Relevant + Not Relevant Relevant + Not Relevant
ECF: Manual Contract Manage- ment / IBS/RB_MANCON	RBD_EDIT (01, 02, 03)	Relevant + Not Relevant

RBD Area Menu, Information System Folder

Transaction	Object (Activity)	RBD Area + Organizational Unit
Worklist - Processor / IBS/ RB_WORKLIST and / IBS/ RB_WORKLIST_SEL	RBD_REPO (not relevant) RBD_EDIT (not relevant)	Relevant + Relevant Not Relevant + Not Relevant

Transaction	Object (Activity)	RBD Area + Organizational Unit
Monitoring - Planned Record Change / IBS/RB_MAN_PLAN_CHG	RBD_REPO (not relevant) RBD_EDIT (not relevant)	Not Relevant + Relevant Not Relevant + Relevant
Decision Template for Past Analysis / IBS/RB_PROPRES_HGB	RBD_REPO (not relevant) S_GUI (61)	Not Relevant + Not Relevant Not Relevant + Not Relevant
Decision Template for Future Analysis / IBS/RB_PROPRES_IAS	RBD_REPO (not relevant) S_GUI (61)	Not Relevant + Not Relevant Not Relevant + Not Relevant
Decision Template for ECF Procedure / IBS/RB_PROPRES_ECF	RBD_REPO (not relevant) S_GUI (61)	Not Relevant + Not Relevant Not Relevant + Not Relevant
Reporting Function / IBS/RB_REPORTING	RBD_REPO (not relevant)	Not Relevant + Not Relevant
Development List / IBS/RB_DEVL	RBD_REPO (not relevant)	Relevant + Relevant
Development List per Source System Contract / IBS/RB_DEVL_SINGLE	RBD_REPO (not relevant)	Relevant + Relevant
Individual Document Table - Source System / IBS/MRB_VS_SALDO	Not relevant	Not Relevant + Not Relevant
Posting Log / IBS/RB_LOG_POST	RBD_EDIT (03) S_APPL_LOG (03)	Relevant + Not Relevant
<ul style="list-style-type: none"> • Drilldown Reporting with References / IBS/RB_REF • IRP: Filling Report ECF Gate / IBS/RB_ECF_FILL • IVA: List of Notes for FS-CML / IBS/RB_HINT • IVA: List of Notes for Multiple Source Systems / IBS/RB_HINTM 	RBD_REPO (not relevant)	Relevant + Not Relevant

RBD Area Menu, Flat-Rate Value Adjustment Procedure Folder

Transaction	Object (Activity)	RBD Area + Organizational Unit
FVA: Fill RBD Gate for FS-CML / IBS/RB_FILL_GATE	Not relevant	Not Relevant + Not Relevant
FVA: Enrich RBD Gate / IBS/RB_GATE_MODIFY	RBD_REPO (not relevant)	Relevant + Not Relevant
FVA: Update Run / IBS/RB_PWV_UPD	RBD_EDIT (10)	Relevant + Not Relevant

Transaction	Object (Activity)	RBD Area + Organizational Unit
FVA: Update Run (PPF) / IBS/ RB_PWV_UPD_PPF	RBD_EDIT (10)	Relevant + Not Relevant
RBD Area Menu, Periodic Processing Folder		
Transaction	Object (Activity)	RBD Area + Organizational Unit
IVA: Update Run - Past Analysis / IBS/ RB_EWB_UPD	RBD_EDIT (10)	Relevant + Relevant
<ul style="list-style-type: none"> IVA: Filling Report Future Analysis / IBS/RB_IAS_FILL IVA: Update Run - Future Analysis / IBS/RB_IAS_UPD IVA: Update Run - Future Analysis (PPF) / IBS/RB_IAS_UPD_PPF IVA: Unwinding Run Future Analysis / IBS/RB_IAS_UPD_UNW 	RBD_EDIT (02)	Relevant + Relevant
<ul style="list-style-type: none"> IVA: Posting Run - Future Analysis / IBS/RB_IAS_POST IVA: Posting Run - Future Analysis (PPF) / IBS/RB_IAS_POST_PPF IVA: Unwinding Posting Run Future Analysis / IBS/RB_IAS_POST_UNW 	RBD_EDIT (10)	Relevant + Relevant
<ul style="list-style-type: none"> IRP: Filling Report ECF Gate / IBS/ RB_ECF_FILL 	RBD_EDIT (02)	Not Relevant + Not Relevant
<ul style="list-style-type: none"> IRP: Deletion Report ECF Gate / IBS/RB_ECF_CLEAR 	Not relevant	Not Relevant + Not Relevant
<ul style="list-style-type: none"> IRP: Update Run ECF / IBS/ RB_ECF_UPDATE IRP: Update Run ECF (PPF) / IBS/ RB_ECF_UPD_PPF IRP: Unwinding Run ECF / IBS/ RB_ECF_UPD_UNW IRP: Unwinding Run ECF (PPF) / IBS/RB_ECF_UNW_PPF 	RBD_EDIT (02, 10)	Relevant + Not Relevant
IRP: Creation Process ECF / IBS/ RB_ECF_A_CREATE	RBD_EDIT (02)	Relevant + Not Relevant

RBD Area Menu, Administration Folder

Transaction	Object (Activity)	RBD Area + Organizational Unit
RBD: Assign Administrator / IBS/ RB_ASSIGN_CO	RBD_EDIT (02)	Not Relevant + Not Relevant
RBD: Automatic Account Crea- tion / IBS/RB_ACC_CREATION	RBD_REPO (not relevant)	Relevant + Not Relevant
IVA: Initialization Run for Future Analy- sis / IBS/RB_IAS_UPD_INIT	RBD_EDIT (02)	Relevant + Relevant
IRP: Initial Run ECF / IBS/ RB_ECF_UPD_INIT	RBD_EDIT (02, 10)	Relevant + Not Relevant
IRP: Initialization ECF (PPF) / IBS/ RB_ECF_INIT_PPF	RBD_EDIT (02, 10)	Relevant + Not Relevant
Archive: RBD Account Data (Gen- eral) / IBS/RB_CSARA_ACC	S_ARCHIVE	Not Relevant + Not Relevant
Archive: RBD Flow Data ECF / IBS/ RB_CSARA_ECO	S_ARCHIVE	Not Relevant + Not Relevant
Archive: RBD Flow Past / IBS/ RB_CSARA_HCO	S_ARCHIVE	Not Relevant + Not Relevant
Remove Obsolete Postings (Past) / IBS/RB_HCO_DEL_POST	RBD_EDIT (02)	Relevant + Relevant
Man. Contr.: Data Cleansing / IBS/ RB_MANCON_DEL	RBD_EDIT (02)	Relevant + Relevant
Deletion Report for FVA Interface / IBS/ RB_GATE_CLEAR	RBD_EDIT (02)	Relevant + Relevant

RBD Area Menu, Impairment Processing Extension - Environment Folder

Transaction	Object (Activity)	RBD Area
Upload Files to Application Server / IBX/FILE_UPLOAD	/IBX/EDIT (60)	Not relevant
Import CSV Files / IBX/CSV_IMPORT	/IBX/EDIT (60)	Not relevant
Maintain Import Data / IBX/IMP_CHNG	/IBX/EDIT (43, 60)	Not relevant
Main Dialog / IBX/MAIN	/IBX/EDIT (02, 03, 10, 23, 94)	Not relevant
Restrict Data Selection / IBX/ SELECTION	Not relevant	Not relevant

Transaction	Object (Activity)	RBD Area
Adjustment of Initial Comparative Data / IBX/CH_IN_RAT	/ IBX/EDIT (C8)	Not relevant
Maintain Initial PDs / IBX/MPD	/ IBX/EDIT (C8)	Not relevant
RBD Area Menu, Impairment Processing Extension - Processes Folder		
Transaction	Object (Activity)	RBD Area
Start Migration / IBX/MIGRATION	/ IBX/EDIT (10, 78, 93)	Not relevant
Fill Import Interface Using CSV Files / IBX/IMPORT	/ IBX/EDIT (60) In addition to the technical authorization, the system storage must be monitored in order to prevent the databases from being overflowed.	Not relevant
Import CML Files / IBX/CML_IMPORT	/ IBX/EDIT (60, 93)	Not relevant
Build CF-Based Time Slices / IBX/CR_SLICE_FRM_CF	/ IBX/EDIT (93)	Not relevant
Refine Imported Data / IBX/IMP_REFINE	/ IBX/EDIT (60, 93)	Not relevant
Delete Import Data / IBX/IMP_DELETE	/ IBX/EDIT (06)	Not relevant
Start Import Data Check / IBX/IMP_CHECK	/ IBX/EDIT (60, 78)	Not relevant
Start LPD Recalculation / IBX/RECALC_LPD	/ IBX/EDIT (93)	Not relevant
Start Impairment Categorization / IBX/IC_ASSIGN	/ IBX/EDIT (78)	Not relevant
Start Impairment Calculation / IBX/CALCULATION	/ IBX/EDIT (93)	Not relevant
Delete Open Valuations / IBX/VALUA_DELETE	/ IBX/EDIT (69)	Not relevant
Compress Open Valuations / IBX/VALUA_COMPRESS	/ IBX/EDIT (46)	Not relevant
Transfer Simulated Valuations / IBX/VALUA_TRANSFER	/ IBX/EDIT (21)	Not relevant
Reverse Valuations / IBX/REVERT	/ IBX/EDIT (85)	Not relevant

Transaction	Object (Activity)	RBD Area
Display Logs /IBX/COCKPIT	Not relevant	Not relevant
RBD Area Menu, Impairment Processing Extension - Archiving Folder		
Transaction	Object (Activity)	RBD Area
Delete Records /IBX/ DEL_FLOW_RECORD	/IBX/EDIT (93)	Not relevant
Delete Technical Process Run Informa- tion /IBX/DEL_RUN_INFO	Not relevant	Not relevant
Display Archived Data /IBX/ ARCHIVE_SHOW	Not relevant	Not relevant

Definition of Customer-Specific Roles

The following information is required for the definition of customer-specific roles:

- SAP logon names of all employees who are to work with RBD
- Relevant transactions that are to be executed in the respective role
- Relevant activities that are to be executed within the relevant transactions
- *RBD areas* and *organizational units* affected

To avoid having to define a separate role for each employee, we recommend that you form groups of employees that are permitted to execute the same functions. You can then assign a defined role to all of the employees in the group.

13.13.4.1.5.2 Network and Communication Security

Depending on the risk provision method used and analysis horizon, the *Reserve for Bad Debt* (FS-RBD) application communicates with the following systems:

- SAP Loans Management for Banking, Suite Edition (FS-CML)
- SAP Deposits Management for Banking, Suite Edition (IS-B-BCA)
- SAP Deposits Management for Banking (FS-AM)
- SAP Collateral Management for Banking, Suite Edition (FS-CMS)
- SAP General Ledger Accounting (FI-GL)

Communication takes place using Remote Function Call (RFC). Please use separate users / passwords for RFC and Web services. Also do not use technical users because of better tracability.

13.13.4.1.5.2.1 Communication Destinations

For Remote Function Call (RFC) connections to *SAP Deposits Management for Banking* (FS-AM), technical users are required.

These technical users require read authorization, for example, to read balances and account master data. Please use separate users / passwords for RFC and Web services. Also do not use technical users because of a better tracability.

13.13.4.1.5.3 Deletion of Personal Data in FS-RBD

Use

The *Reserve for Bad Debts* (FS-RBD) component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
/IBX/CONTR	Contract Header Data	Archiving object /IBX/CONTR ILM object IBX_CONTR
/IBX/VALUA	IPX Valuation	Archiving object /IBX/VALUA ILM object IBX_VALUA
/IBS/RBECO	RBD Transaction Data ECF	Archiving object /IBS/RBECO ILM object RBCON_ECF
/IBS/RBHCO	RBD Transaction Data Past Horizon	Archiving object /IBS/RBHCO ILM object RBCON_HGB
/IBS/RBKTO	RBD Account Data	Archiving object /IBS/RBKTO ILM object RBKTO_ECF

Relevant Application Objects and Available EoP functionality

Application Object	Implemented Solution (End of Purpose Check)	Further Information
/IBX/CONTR	EOP check of contract header data based on contract end date	/IBX/CONTR_BUPA_EOP_CHECK
/IBX/VALUA	EOP check of contract header data based on contract end date	/IBX/CONTR_BUPA_EOP_CHECK
/IBS/RBECO	EOP check of contract header data based on contract end date	/IBS/RB_CONTR_BUPA_EOP_CHECK
/IBS/RBHCO	EOP check of contract header data based on contract end date	/IBS/RB_CONTR_BUPA_EOP_CHECK
/IBS/RBKTO	EOP check of contract header data based on contract end date	/IBS/RB_CONTR_BUPA_EOP_CHECK

You configure the settings related to the blocking and deletion of `business partner master data` in Customizing for Cross-Application Components under `Data Protection`.

13.13.4.1.5.4 Specific Read Access Log Configurations

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions. SAP delivers sample configurations for applications.

The RBD Reporting Interface `/IBS/RB_IS_REPORTING RFC` logs fields with sensitive customer data in the specified log domains.

You can configure your individual log domains, which contain individual fields with sensitive customer data, using the Read Access Logging Guide.

You can find the configurations as described in the following chapter. [Read Access Logging \[page 33\]](#)

In the following example configurations, fields are logged in combination with additional fields, in the following business contexts:

Interface Name	Fields Logged	Log Domain	Business Context
/IBS/RB_IS_REPORTING RFC	/IBS/TRB_KTO-RBDID /IBS/TRB_KTO-RBDNR	RBD_ACCID	RBD account number

Interface Name	Fields Logged	Log Domain	Business Context
/IBS/RB_IS_REPORT- ING_RFC	/IBS/TRB_KTO-REFNR	RBD_ACCREF	RBD account reference
/IBS/RB_IS_REPORT- ING_RFC	/IBS/TRB_KVV-PARTV	RBD_PARTV	Partner Reference Source System
/IBS/RB_IS_REPORT- ING_RFC	/IBS/TRB_KVV-VERTV	RBD_VERTV	Contract Number Source System
/IBS/RB_IS_REPORT- ING_RFC	/IBS/TRB_KVV-FINRV	RBD_FINRV	Finance Project Number Source System
/IBS/RB_IS_REPORT- ING_RFC	/IBS/TRB_ECF_HD- RBDID /IBS/TRB_ECF_HD- RBDNR	RBD_ACCID	RBD account number
/IBS/RB_IS_REPORT- ING_RFC	/IBS/TRB_KVV-VERTV /IBS/TRB_ECH_HD- RBDNR	RBD_VERTV	Contract Number Source System
/IBS/RB_IS_REPORT- ING_RFC	/IBS/TRB_ECH_HD- VERTV	RBD_VERTV	Contract Number Source System

More Information

For more information about the RAL sample Customizing for FS-RBD, see SAP Note [2519373](#).

13.13.4.1.5.5 Trace and Log Files

Trace or log files are created during processing. These can contain security-relevant information – such as master data, balances, and flow data from source system contracts.

13.13.4.2 Insurance

13.13.4.2.1 Claims Management

With Claims Management for Insurance, you can manage the entire claims process, from first notification of loss to claims adjustment and financial reporting.

13.13.4.2.1.1 Data Storage Security



Using Logical Path and File Names to Protect Access to the File System

SAP Claims Management save data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following list shows the logical file names and paths used by SAP Claims Management and for which programs these file names and paths apply:

Logical File Names Used in SAP Claims Management

The following logical file names have been created in order to enable the validation of physical file names:

- ICLVEH
 - Program using this logical file name and parameters used in this context: ICL_VEHCATALOG_UPLOAD
 - Customizing path: [SAP Insurance](#) > [Claims Management](#) > [Claim](#) > [Business Settings](#) > [Damaged Objects/Diagnoses](#) > [Damaged Objects/Injured Persons](#) > [Import Catalog for Insured Objects](#) 
- ICLDIAG
 - Program using this logical file name and parameters used in this context: ICL_DIAG_UPLOAD
 - Customizing path: [SAP Insurance](#) > [Claims Management](#) > [Claim](#) > [Business Settings](#) > [Damaged Objects/Diagnoses](#) > [Damaged Objects/Injured Persons](#) > [Diagnoses](#) > [Import Diagnosis Groups and Diagnoses](#) 
- ICLSUPPL
 - Program using this logical file name and parameters used in this context:
ICL_ICLCLAIMDATA_UPLOAD
- ICLDI
 - Program using this logical file name and parameters used in this context: ICL_DATA_UP_DOWNLOAD

Activating the Validation of Logical Path and File Names

These logical paths and file names, as well as any subdirectories, are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent)

and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

13.13.4.2.1.2 Data Protection

13.13.4.2.1.2.1 Read Access Logging

In Read Access Logging, you can configure which read-access information to log and under which conditions. In the following table, you can find the configurations (shipped with SAP Claims Management), the fields are logged, and the relevant business context:

Configuration	Fields Logged	Business Context
ICL_SSN	<ul style="list-style-type: none"> Tax Number Category (field TAXTYPE in for instance table ICLC_ICL_BP_MINI_SCREEN-) Business Partner Tax Number (TAXNUM) 	<p>SAP Claims Management logs tax data.</p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px;"> <p>i Note</p> <p>In the Mini Business Partner the tax number is only logged if the user has selected the tax number category US1.</p> </div>
ICL_BANK	<ul style="list-style-type: none"> Bank details ID (BKEXT) Bank country key (BANKS) Bank Key (BANKL) Bank account number (BANKN) IBAN (IBAN) 	SAP Claims Management logs bank account data.

Configuration	Fields Logged	Business Context
ICL_HEALTH	<p>The fields in the following categories are logged:</p> <ul style="list-style-type: none"> • Claim item groupings and the relevant items with subclaim type, coverage, coverage type, benefit type, benefits catalog • Diagnosis • Procedures • Tooth notation and eyeglass prescription • Level of care • Suspension of care • Insured persons and claimant • Facts capture • Payments 	SAP Claims Management logs health data.

For Read Access Logging of health data, you have to activate specific views in Customizing for *SAP Insurance* under [► Claims Management ► Claim ► Technical Settings ► Data Protection ► Read Access Logging ► Activate Specific Views for Read Access Logging](#).

13.13.4.2.1.2.2 Deletion of Personal Data

SAP Claims Management might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 [► Product Assistance ► Cross Components ► Data Protection](#).

Relevant Application Objects and Available Deletion Functionality

Application Object	Provided Deletion Functionality
Archiving of Claims (Archiving Object ICLCLAIM)	ILM Object ICLCLAIM (see SAP Note 1976123)
Archiving of Claim Bundles (Archiving Object ICLECCEVT)	ILM Object ICLECCEVT (see SAP Note 1976123)

Application Object	Provided Deletion Functionality
Archiving of Subclaims (Archiving Object ICLSUBCL)	ILM Object ICLSUBCL

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management in Customizing for *Cross-Application Components* under ► *Data Protection* ► *Authorization Management* ►. For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for *Cross-Application Components* under ► *Data Protection* ► *Blocking and Unblocking* ► *Business Partner* ►.

You configure the settings related to the blocking and deletion of customer master data in Customizing for *SAP Insurance* under ► *Claims Management* ► *Claim* ► *Technical Settings* ► *Archiving* ►.

13.13.4.2.1.2.3 Change Log

In order to log personal data in FS-CM, you can use the following standard function of FS-CM:

- Log of changes in a claim and in a claim bundle
When you are processing a claim or a claim bundle, you can view a structured overview showing the changes in the relevant claim or claim bundle. To call up the structured change overview, choose ► *Tools* ► *Claim Changes (Overview)* ► in claim processing, or ► *Tools* ► *Bundle Changes (Overview)* ► in claim bundle processing. In the next dialog screen you see the overview tree with the changes that have been made.
For more information, see Application Help of SAP Claims Management under ► *Claim* ► *Administration of the Claims Management System* ► *Display of Changes in Claim and Claim Bundle* ►.

i Note

Changes of business partner data will be logged in the business partner system since business partner data are not stored in FS-CM.

13.13.4.2.1.2.4 Information Retrieval

Claims Management uses the Information Retrieval Framework (IRF) to retrieve information about the business partner data that is stored in claims. For more information, see SAP Note [2690400](#).

13.13.4.2.1.2.5 User Consent

It is the responsibility of insurance companies themselves to obtain the consent of all of their business partners with regard to the use of their personal data.

13.13.4.2.2 Policy Management

With Policy Management, you can manage insurance contracts. You can map the whole life cycle of a contract, starting from the creation of an application, through policy issuance and ongoing contract maintenance, right up to the termination of the contract.

13.13.4.2.2.1 Authorizations

Authorization Concept

If the ABAP Platform functions are not sufficient, you can use the Business Add-In (BAI) /PM0 / ABP_TECHCHKTA_BADI (in enhancement spot /PM0/ABT_TECHCHKTA_ES) to define rules for authorizing characteristics, such as the postal code, replacement business, and checks for amounts and dual control.

Authorization Roles

Policy Management provides the following role types:

- **Template Roles**
Template roles are templates that can be copied and adjusted in customer implementation projects.
- **Demo Roles**
Demo roles are examples based on template roles and authorization values of sample content. You should only use them for demo or test purposes.

Naming Convention for FS-PM Roles

The role name must reflect the component and the process. Consequently the naming convention is SAP_FSPM_<role flag>_<role type>_<role_description>, with the following meanings:

- SAP = Standard prefix
- FSPM = Component
- <role flag> = Role flag with possible values C for Composite roles and S for Single roles
- <role type> = Role type with possible values TMPL for template roles and DEMO for demo roles
- <role description> = In composite roles, it is a position description (for example, POLHANDLER for policy handlers). In single roles, it is a description of a task (for example, CREATE_POLICY).

In the *Auto* line of business every set of applications (Bonus-Malus, Insurer Information System, etc.) has its own authorization object with a set of permitted activities. The naming convention is /MVA/(A)FSPM_AUTO_<role_description> with the following meaning:

- /MVA/ = Standard prefix
- (A)FSPM_AUTO = (A) Standard Role and FSPM_AUTO for line of business *Motor Vehicle*
- <role_description> = For *Motor Vehicle* managements (for example BM = Bonus-Malus Management) or for special purpose for example DISPLAY (designed to display *Motor Vehicle* specific data only)

Authorization Classes

Policy Management provides the following authorization classes:

- P MOB (FS-PM Basis)
This class contains all cross-line of business authorization objects.
- P MOL (FS-PM Life)
This class contains the authorization objects that are needed only in the *Life* line of business.
- P MOR (FS-PM Workplace)
This class contains the authorization objects for accessing the PBT (Policy-Based Technology) and PBT-related transactions.
- P MOO (FS-PM: Authorizations in Orchestration Layer)
This class contains the authorization object for the automatic premium loan financing (APLF).
- /PMG (FS-PM: Group Insurance Authorization Object Class)
This class contains the authorization object for the master policy business process. The authorization object can be configured for the following lines of business:
 - BS: *Basis*
 - LL: *Life*
 - LP: *P&C* (Liability and Personal Accident Insurance)

Switchable Authorizations Check Framework (SACF)

The Switchable Authorizations Check Framework (SACF) provides additional authorization checks for the following FS-PM scenarios:

- /PM0/INDEX_01 (Index Component)
- /PM0/CORRESPOND_01 (Correspondence)
- /PM0/FPP_01 (Framework for Parallel Processing)
- /PM0/NOTIFICATION_01 (Notifications)
- /PM0/INFO_CONT_01 (Integration FS-CD)
- /PM0/MODELCALC_01 (Model Calculation)
- /PM0/CLAIMS_01 (Integration FS-CM)
- /PM0/EXT_DATES_01 (Related Dates)
- /PM0/MIGRATION_01 (Migration)
- /PM0/PREM_01 (Premium Access)
- /PM0/BP_01 (Integration BP)

For more information, see the documentation for each scenario in the system.

13.13.4.2.2.2 Communication Destinations

Overview

Policy Management provides functions for data exchange with other application components. These application components can be found either in separate systems or in the same system. To enable you to access these application components, an RFM (Remote Function Module) destination must be created for the relevant system. This RFM destination establishes a connection between Policy Management and the external system.

Note the following with regard to communication destinations:

- Connection
 - If the application component is in the same system, the destination is `NONE`.
 - If the application component is in a separate system, you must create a user-defined RFM destination for each external system that interacts with Policy Management, and you must also ensure that the external systems use the correct RFM destination. You define which application component should use which RFM destination in Customizing for *SAP Insurance* under [► Policy Management ► Integration ► Process Primary Settings for Interfaces to External Systems ►](#). Access to the external system can be screen-based (online) or non-screen-based (offline). It is possible that both of these access types will be executed by different users with different authorizations. You can therefore enter two destinations for each application component in the Customizing activity [Process Primary Settings for Interfaces to External Systems](#) (one RFM destination for online access and

one for offline access). You can assign different users with different authorizations for accessing the external system to these RFM destinations.

- The RFM destination configured in transaction SM59 determines which user is used to access the external system. For each RFM destination, you can enter the user to be used to access the external system. You either enter a user name or specify the current user.
If you use the current user to access the external system, the system displays a log-on dialog box where the user must enter a password to log on to the external system. You can bypass this dialog box by establishing a trusted/trusting connection between the two systems. This means that if there is an RFM between a trusted and trusting system, a password is no longer sent when you log on to the trusting system.

Caution

Note that Policy Management users require special authorization to access external application components. To ensure that only authorized users can access the data on external systems, SAP recommends that you create a trusted relationship between Policy Management and the external system and that you always use the current user to access data.

Connection Destinations

Destination	Delivered	Type
RFM destination for product runtime	No	RFM
RFM destination for Business Partner for Financial Services (FS-BP)	No	RFM
RFM destination for Collections and Disbursements (FS-CD)	No	RFM
RFM destination for Financials (FI)	No	RFM
RFM destination for Incentive and Commission Management (FS-ICM)	No	RFM
RFM destination for Portfolio Assignment (PFO)	No	RFM
RFM destination for Organizational Management (OM)	No	RFM

13.13.4.2.2.3 Data Protection and Privacy

13.13.4.2.2.3.1 Read Access Logging

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions. Policy Management delivers the following sample configurations:

- Configuration for bank details
- Configuration for payment cards
- Configuration for health data
- Configuration for policy number

For more information, see SAP Note [2630769](#).

i Note

Regarding the Fiori app *Policy Inquiry*:

Since the Fiori app *Policy Inquiry* is not directly RAL-enabled you must activate RAL indirectly via the corresponding OData service `UI_POLICYINQUIRY`.

13.13.4.2.2.3.2 Deletion of Personal Data

Blocking and Archiving

Note the following with regard to blocking and archiving in Policy Management (FS-PM):

- The archiving function is used for the blocking of data. Archiving and blocking of business objects takes place at the same time (= end of residence time). Each archiving object corresponds to an ILM object.
- Archived data can only be displayed in the *Inquiry* business process and cannot be changed. Archived data is protected by authorization check and only available in read-only mode for authorized users.
- For performance reasons, you can define different residence periods for different data groups (cash flow documents, inactive contract versions, fund orders, etc).
- Since insurance contracts often have a long contract duration, SAP recommends keeping the updated (newest) contract data in the operational system, while archiving out-dated object data. The last contract version can only be archived when the contract status is *Inactive* and the residence time for this version is outdated.
- You can define rules determining residence periods and ILM configurations in Customizing for *SAP Insurance* under **► Policy Management ► General Settings ► Archiving** or *Data Protection*.

Data Deletion

Note the following with regard to data deletion in FS-PM:

- Data deletion is managed on the basis of ILM objects in the ILM system.
- FS-PM provides preconfigured retention rules defined in ILM for FS-PM ILM objects.
- Archived data belonging to a contract is deleted with the contract when the retention period of the contract is over.
- Data groups that do not belong to a contract have their own retention-date determination rules.

Information transfer to SAP NetWeaver Business Warehouse (SAP NetWeaver BW)

When an object is archived (and deleted) in a back-end system, the standard behavior is that SAP NetWeaver Business Warehouse (SAP NetWeaver BW) is informed that the object can also be deleted there. FS-PM deviates from this standard behavior, however, in that certain objects, such as a life insurance policy, may need to be archived but not deleted. In the case of a life insurance policy with a term of 30 years, for example, it may be necessary for the versions of the first 20 years to be deleted, whereas the versions of the last ten years are still required. For this reason, FS-PM has created four implementations in the BAdI `BADI_IRM_NOTIFICATION` that ensure that only those objects are reported to SAP NetWeaver BW that are actually deleted in FS-PM.

The following implementations are provided with the BAdI `BADI_IRM_NOTIFICATION`:

- `BADI_IRM_NOTIFICATION_PM0_ABD`
- `BADI_IRM_NOTIFICATION_PM0_ABG`
- `BADI_IRM_NOTIFICATION_PM0_ABO`
- `BADI_IRM_NOTIFICATION_PM0_ABP`

End of Purpose (EoP) Check

For detailed information about the EoP check in Policy Management, search for **Business Partner End of Purpose (EoP) - Checks in Policy Management for Insurance** in the documentation of [SAP S/4HANA](#).

Further Notes

- Deletion of Personal Data During Fund-Relevant Benefit Processing (Cleaning of Table `/PM0/ABDUPPCMPS`)
If you also create provisional non-cash flow documents of the *Fund Shares* category during fund-relevant benefit processing, you must ensure the following:
 - These non-cash flow documents are reversed in your process
 - The entries for personal data are deleted in the associated input tables, such as `/PM0/ABDUPPCMPS` (*Contains Person to Indicate as Deceased*)

The deletion of data that is no longer required is guaranteed in the standard integration with Claims Management. However, if you have customer-specific implementations, you must ensure that this data is deleted. The function modules /PM0/ALT_CM_CANCEL_ORDERS and /PM0/ABY_DELETE_DISPO_DATA are provided for this purpose.

13.13.4.2.2.3.3 Change Log

To log personal data, you can use the following standard functions of Policy Management:

- Log of changes in contract journal
- Scrolling in journal
- Changes to a policy displayed in the policy summary
- Changes to a contract displayed in the contract summary

⚠ Caution

Changes to business partner data are logged in the business partner component since business partner data is not stored in Policy Management.

13.13.4.2.2.3.4 Information Retrieval

Policy Management uses the Information Retrieval Framework (IRF) to retrieve information about the **business partner** data that is stored in policies, contracts, and applications. For more information, see SAP Note [2678890](#).

In the following table, you can find a list of all standard ILM objects (and the corresponding responsibilities in the IRF) which provide business partner data:

ILM Object	Description of ILM Object	Responsibility (IRF)
PM0_ABC	FS-PM Archive Correspondence	PM0_ABC
PM0_ABD	FS-PM Archive Coinsurance	PM0_ABD
PM0_ABG	FS-PM Archive Master Policy	PM0_ABG and PMG_ABDGGEN
PM0_ABN_C	FS-PM Archive Accounting Component Cash Flow Documents	PM0_ABN_C
PM0_ABO	FS-PM Archive Object Management	PM0_ABO
PM0_ABP_CONTRACT	ILM Object for In-Force Business Man- agement (Contract)	PM0_ABP_CONTRACT

ILM Object	Description of ILM Object	Responsibility (IRF)
PM0_ABPDC	FS-PM Archive Data Container See also separate note at the end of this chapter.	PM0_APDC
PM0_ABS	FS-PM Archive Transfer Object	PM0_ABS
PM0_ABT	FS-PM Archive Accounting Component Info Container	PM0_ABT
PM0_ALPRO	FS-PM Archive Model Calculation	PM0_ALPRO
PMG_ABGMA	FS-PM Archive Master Policy Application	PMG_ABGMA
MVA_AML	FS-PM Auto: Archive Malus File	MVA_AML
MVA_ARS	FS-PM Auto: Archive Registration (Austria)	MVA_ARS
MVA_ARSD	FS-PM Auto: Archive Registration (Germany)	MVA_ARSD
MVA_AVAS	FS-PM Auto: Archive IIS	MVA_AVAS
MVA_AVWB	FS-PM Auto: Archive CIC	MVA_AVWB
MVA_ACE	FS-PM Auto Archive Central Call	MVA_ACE

The following standard ILM objects do not provide business partner IDs:

- PM0_ABN_A (FS-PM Archive Accounting Component Account Balances)
- PM0_ABN_N (FS-PM Archive Accounting Component Non Cash Flow Documents)
- PM0_ABN_R (FS-PM Archive Accounting Component RI Documents)
- PM0_ALVAL (FS-PM Archive Guarantee Values)
- PM0_CTX (FS-PM Archive Process Context)
- MVA_ACE (FS-PM Auto Archive Central Call)

These standard ILM objects provide information about policies, contracts, applications, and licenses, but no information as to which business partner this data belongs. Consequently the IRF does not support business partner evaluation for these ILM objects directly.

Please note the following on these ILM objects (that do not provide business partner IDs directly):

- You can retrieve all relevant information about these ILM objects by using ILM object PM0_ABP_CONTRACT and then starting the *Inquiry* process.
- If you add a business partner ID to one of these ILM objects, you must create a new data model for this ILM object in the IRF.
- For more information about the MVA_ACE ILM object, see SAP Note [2683283](#).

i Note

In table `/PM0/ABDCSUBJCTX`, business partners maybe stored in the XML field. Therefore, SAP provides the function module `/PM0/ABX_DTINF_BP_ABDCSUBJCTX` that handles the occurrences of `PARTNER_ID` and `PARTN2_ID` (see code lines with `Create find condition for field XML` comment in function module `/PM0/ABX_DTINF_BP_ABDCSUBJCTX`).

If you add further or other partner IDs to table `/PM0/ABDCSUBJCTX`, you must create a function module similar to `/PM0/ABX_DTINF_BP_ABDCSUBJCTX`. Ensure that `Create find condition for field XML` is implemented in the same way as in function module `/PM0/ABX_DTINF_BP_ABDCSUBJCTX`.

Note to ILM Object PM0_ABPCD - Adding Partner IDs to Table `/PM0/ABDCSUBJCTX`

In table `/PM0/ABDCSUBJCTX`, business partners maybe stored in the XML field. Therefore, SAP provides the function module `/PM0/ABX_IRF_SUBJCTX_DCC_GUID` which uses method `SELECT_ABDCSUBJCTX` of class `/PM0/CL_ABX_IRF_SERVICES` that handles the occurrences of `PARTNER_ID` and `PARTN2_ID` (see code lines with `Create find condition for field XML` comment in method `SELECT_ABDCSUBJCTX`).

If you add further or other partner IDs to table `/PM0/ABX_IRF_SUBJCTX_DCC_GUID`, you must create a function module similar to `/PM0/ABX_DTINF_BP_ABDCSUBJCTX`. Ensure that `Create find condition for field XML` is implemented in the same way as in method `SELECT_ABDCSUBJCTX`.

In your BAdI-Implementation, you have to do the following:

- Remove the link of FS-PM standard (from `BUT000-PARTNER` to `/PM0/ABDCSUBJCTX-XML` via function module `/PM0/ABX_IRF_SUBJCTX_DCC_GUID`).
- Add your function module for this link (from `BUT000-PARTNER` to `/PM0/ABDCSUBJCTX-XML` via function module `<Customer Function Module>`).

13.13.4.2.2.3.5 User Consent

It is the responsibility of insurance companies themselves to obtain the consent of all of their business partners with regard to the use of their personal data.

13.13.4.2.2.4 Connected Product Engine

Policy Management uses a product engine to check the actuarial aspects of the policy and to perform calculations. You can guarantee the security of the product engine system by using suitable user authorizations at operational level. You can rule out the influence of the product engine runtime and the used content by restricting access to the product engine (using BAdI `/PM0/ABP_AUTH_BADI`).

⚠ Caution

The product engine should always be located in the inner security zone.

The product engine does not save any in-force business data (stateless). It calculates and returns new application data from the application data supplied by Policy Management. Therefore, the product engine does not change the in-force business data directly. This situation, along with the journal management and history management functions provided by Policy Management, ensures to a large extent that the application data cannot be corrupted by the product engine.

13.13.4.2.3 Insurance Product Engine msg.PMQ

With the insurance product engine msg.PMQ, you can define and calculate insurance products. msg.PMQ consists of the following:

- **PMQ.Designer**
During the product development, a multi-layered security concept for the protection of the product data against unauthorized access is effective.
Product data are copied for processing into the local file system of the computer on which PMQ.Designer is installed. It should be ensured administratively by operating system means that exclusively the user that has copied those data may access them. On the supported systems, e.g. that is often already achieved by storing the data inside the home directory of the user. Beyond that for protection against hardware theft it is recommended to encrypt the volume on which the product data are stored.
During the local processing of product data, the user may modify all product data files, either by PMQ.Designer means or by external tools (e.g. text editors). For that purpose PMQ.Designer does not have an own user and permissions management. By integration with a version control system, however that functionality is provided implicitly.
For central storage and for distributed processing of product data, it is mandatory to connect PMQ.Designer with a version control system. On the level of the version control system, security mechanisms are effective that prevent unauthorized retrieval and transfer back respectively modification of the product data. All modern version control systems offer a user management for that purpose and allow the fine-grained granting of read and write permissions on the product data for individual users or user groups. The granting of user permissions ensues administratively by the means of the respectively used version control system. It is recommended to define all permitted users and their permissions at least on the top level of every repository of the version control system. It is not recommended to permit anonymous access to the product data, neither for read operations.
The communication between PMQ.Designer and a version control system usually takes place via web-based protocols (HTTP). It is recommended only to use secured connections for this purpose. If other protocols are used, an adequate encryption should be used.
- **MSGPMCON**
The msg.PM connection (MSGPMCON) is the link between msg.PMQ and Insurance Policy Management (FS-PM) as part of SAP S/4HANA.
- **TOMATOSJ**
TOMATOSJ has to be secured on operational level against unauthorized accesses.
On the one hand, installation and administration of TOMATOSJ XSA instances should be permitted for authorized user groups only. This has to be ensured administratively by mechanisms of the XSA platform. Furthermore, the access to all file system directories that are configured for TOMATOSJ, should be

restricted to authorized user groups by operating system means. This is especially valid for the directory in which the product data are stored.

Particularly to highlight is that TOMATOSJ should only be executed in an especially protected network area (high-security area).

The communication with TOMATOSJ for calculation requests takes place via web-based services (REST services). For that purpose exclusively secured connections are recommended. A web interface or other accesses (e.g. for administration) are not provided. Because of that on the level of the services no user group-specific accesses are neither necessary nor provided.

TOMATOSJ does not change nor save data of Policy Management (FS-PM). As a result of calculation requests only new respectively derived data are being created and returned to FS-PM. The further processing of the result data falls to FS-PM.

For more information, see the attachments in SAP Note [2635866](#).

13.13.4.2.4 SAP Statutory Reporting for Insurance

13.13.4.2.4.1 Deletion of Personal Data in FS-SR

Use

The *Statutory Reporting* (FS-SR) might process data (personal data) that is subject to the data protection laws applicable in specific countries. The business partners in the statutory reports can only be legal entities (in German: juristische Personen), not natural persons. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data in the applications providing the data, for example, in *Loans Management* (FS-CML). For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►. In FS-SR, business partner data can only be deleted manually, using deletion reports.

Relevant Application Objects and Available Deletion Functionality

Application Object	Detailed Description	Provided Deletion Functionality
Ledger Data Table	For more information, see SAP Note 2304306 .	<ul style="list-style-type: none">Transaction ISSR_NB2Transaction ISSR_MIG5
Stored List		Transaction ISSR_OUT_ALV
Business Partner Change List		Transaction ISSR_DEL_CNS_GPCH

13.13.5 Public Services

13.13.5.1 Defense & Security

13.13.5.1.1 Defense & Security

13.13.5.1.1.1 Roles and Authorization

This chapter describes the use of roles and authorizations in the industry solution SAP S/4HANA Defense & Security. Defense & Security uses the standard authorization concepts provided by SAP S/4HANA.

SAP delivers standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles. In Defense & Security, PFCG delta roles are used to access content in the application. To complete the end-user role, these roles must be used along with other roles delivered by SAP. Example roles are included in the table below. These roles are designed to support your Defense & Security business processes.

13.13.5.1.1.1.1 Roles

The frontend and backend roles that are delivered by Defense & Security are shown below. You can use these roles as templates for your own roles.

Defense Frontend Roles

Role Name	Role Description
SAP_BR_ORG_PLANNER	Organizational Planner - Force Element
SAP_BR_CAP_PLANNER	Organizational Planner - Capabilities
SAP_BR_FEMAINT_PLANNER	Maintenance Planner - Force Element
SAP_BR_FEMAT_PLANNER	Material Planner - Authorized Materials
SAP_BR_MD_AUTHMAT	Master Data Specialist - Authorized Material Data
SAP_BR_ORG_PLANNER_PERS	Organizational Planner - Personnel
SAP_BR_MAINT_TECH_OFFICER	Technical Officer - Armed Forces

Reused Roles

Role Name	Role Description	Comment
SAP_BR_PRODMASTER_SPECIALIST	Master Data Specialist -Product Data	This role can be useful for the material planner.
SAP_BR_PROJECTMANAGER	Project Manager	This role is necessary when using EPPM project integration in Capabilities.

13.13.5.1.1.1.2 Defense Authorization Objects

This chapter lists the authorization objects used and the data control languages for the defense-specific objects.

In Defense & Security, we have created some new authorization objects and reused the authorization objects that come from the associated frameworks, to ensure that the integration with the D&S business processes is consistent.

Force Element

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_ASSGMT obsolete	Authority object used for assignments.	DFS_SRCTYP	Source Object Type
		DFS_TGTTYP	Assignment Type
		DFS_STAT	System Status
		ACTVT	Activity
DFS_FE_SNT	To control authorizations for the force element and reference force element's sensitivity information.	SENSTVYKEY	Sensitivity of the force element/ reference force element
		ACTVT	Activities for the sensitivity field
DFS_FE_SPR	To control activities associated with the force element's priority information.	ACTVT	Activities for the priority field on the sensitivity tab
DFS_ASSGMTS	Authority object for status handling in the assignment framework.	DFS_SRCTYP	Source Object Type
		DFS_TGTTYP	Assignment Type
		DFS_VRGNG	Business Transaction
		ACTVT	Activity

Authorization Object	Purpose	Attributes	Field Description
DFS_ASSGMS	Authority object used for the assignment source type	DFS_SRCTYP	
		DFS_SRCOTY	Source Type
DFS_ASSGM1	Authority object used for assignments including the profile.	DFS_SRCTYP	Source Object Type
		DFS_TGTTYP	Assignment Type
		DFS_STAT	System Status
		ACTVT	Activity
		PROFL	Authorization Profile
DFS_FE_CON	Authorization Object for PLOG_CON enablement	ACTVT	Activity

Reused authorization objects

PLOG	Personnel Planning
PLOG_CON	Personnel Planning with Context
C_ARPL_WRK	CIM: Work Center - Plant

Flexible Material Planning Object

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_FMPO_A	Authorization objects used to assign accompanying parts.	ACTVT	Activity
		ASGNMT_IND	Flexible Material Planning Object: Assignment Indicator
		MATKL	Material Group
DFS_FMPO_C	Authorization objects used to create the FMPO.	ACTVT	Activity
		RIC_ID	Reportable Item Code - Numerical ID
		ISTAT	Planning Status
		RICCODE	Reportable Item Code
DFS_FMPO_M	FMPO authorization objects used to assign models.	ACTVT	Activity
		MATKL	Material Group
		EXTWG	External Material Group
DFS_FMPO_H	Maintain the FMPO hierarchy.	ACTVT	Activity

Reused authorization objects

M_MATE_MAN	Material Master: Data at Client Level
M_MATE_MAR	Material Master: Material Types
M_MATE_MAT	Material Master: Materials
M_MATE_NEU	Material Master: Create
M_MATE_STA	Material Master: Maintenance Statuses
M_MATE_WGR	Material Master: Material Groups
P_ORGIN	HR: Master Data

Defense Logistics

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_ALL_PL	Authorization objects used to create and maintain the allowance plan.	ACTVT	Activity
DFS_ALL_PR	Authorization objects used to create and maintain the allowance request.	ACTVT	Activity
DFS_ALP_S	Authority object for status handling in the allowance plan.	ACTVT	Activity
		DFS_VRGNG	Business Transaction

Modeling Canvas

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_MODEL	Authorization objects used to create and maintain models.	ACTVT	Activity
DFS_MODELS	Authority object for status handling in the model.	ACTVT	Activity
		DFS_VRGNG	Business Transaction

Defense Maintenance

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_PLTFRM	Authorization objects used to create and maintain the platform.	ACTVT	Activity

Capability Planning and Mission Essential Task List

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_CAP_CO	Authorization object used to create and maintain the different capability types (capability node, capability hierarchy node and capability root).	DFS_COTYPE	Capability Type
		ACTVT	Activity
		DFS_STAT	System Status
DFS_CAP_CS	Authorization object used to create and maintain the capability statements.	ACTVT	Activity
		DFS_CSTYPE	Capability Statement Type
		DFS_CSCAT	Defense: Capability Statement Category
DFS_CAPMET	Authorization object used to create the mission essential task list.	ACTVT	Activity
		DFS_MTTYPE	Mission Essential Task Type
		DFS_STAT	System Status

Scenario

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_SCN	Authorization objects used to create and maintain scenarios.	ACTVT	Activity
		DFS_SCNTYP	Scenario Type
DFS_SCN_S	Authority object for status handling in the scenario.	ACTVT	Activity
		DFS_VRGNG	Business Transaction

Reused authorization objects

P_ORGIN	Human Resources
C_PROJ_KOK	Controlling area for project definition
C_PROJ_PRC	Profit center for project definition
C_PRPS_KOK	Controlling area for project definition
C_PRPS_PRC	Profit center authorization for WBS elements

Authorized Personnel

Defense-specific authorization objects

Not available

Reused authorization objects

PLOG	Personal Planning
------	-------------------

Organizational Measure

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_ORGM	Authorization objects used to create and maintain organizational measures	ACTVT	Activity
		DFS_ORGMT	Measure Type

Reused authorization objects

S_SCDO_OBJ	Change Documents for the Change Document Object
S_SCMG_CAS	Case Management: Case

Personal and Functional Equipment (PFEM)

All existing PFEM relevant authorization objects works as it is. Additionally force element and flexible material planning object relevant authorization objects are needed for enhanced PFEM functionality.

Structural Authorization

Defense-specific authorization objects

Authorization Object	Purpose	Attributes	Field Description
DFS_STRAUT	Authorization object for structural authorization enablements.	ACTVT	Activity

13.13.5.1.1.1.2.1 Default Authorization Value Settings

The product master configuration of the default authorization values is shown below. This is mainly required to conform to industry-specific requirements and to enable the S/4 HANA Defense & Security-specific authorization objects to apply to the product master app.

The default value for the authorization object DFS_FE_SNT for MD_C_PRODUCT_MAINTAIN is yes, without any other values.

The default value for the authorization object DFS_STRAUT for both MD_C_PRODUCT_MAINTAIN_SRV and MD_PRODUCT_OP_SRV is yes, without any other values.

13.13.5.1.1.1.3 Defense Cross-Topics

On the basis of customer feedback, Defense & Security has introduced an additional authorization function, which is described in the following.

13.13.5.1.1.1.3.1 Sensitivity

Defense & Security provides a *Sensitivity* field, which customers can use to assign a specific sensitivity value to force elements. This can for example be used to define special force units. As a result, this field can then be used to prevent certain users accessing these units.

To categorize the sensitivity of a unit, we have added the following field to the existing infotype.

HRP1950 infotype

Table Name	Field Name	Data Element	Domain
HRP1950	SENSITIVITY_KEY	DFS_SENSITIVITY_KEY	DFS_SENSITIVITY_KEY

View Name	Table Name	Global Field Name for CDS view	Domain	Text Table
DFS_FE_SENSTV_V	DFS_FE_SENSTVTY	FrcElmntOrgSenstv-Key	DFS_SENSITIVITY_TEXT	DFS_FE_SENSTVT_T

Some of the sample values are shown below

MANDT	SENSITIVITY_KEY	SENSITIVITY_TEXT
903	01	Very High
903	02	High
903	03	Medium
903	04	Low

13.13.5.1.1.1.3.2 Structural Authorization

The SAP S/4HANA programming model supports the creation of Fiori-based apps using core data services (CDS) for data modeling and access, the OData protocol for service exposure, and the business object processing framework for transactional processing. Since CDS is a core mechanism for data retrieval from the backend, the relevant data control language (DCL) is required to restrict data according to authorizations for each user.

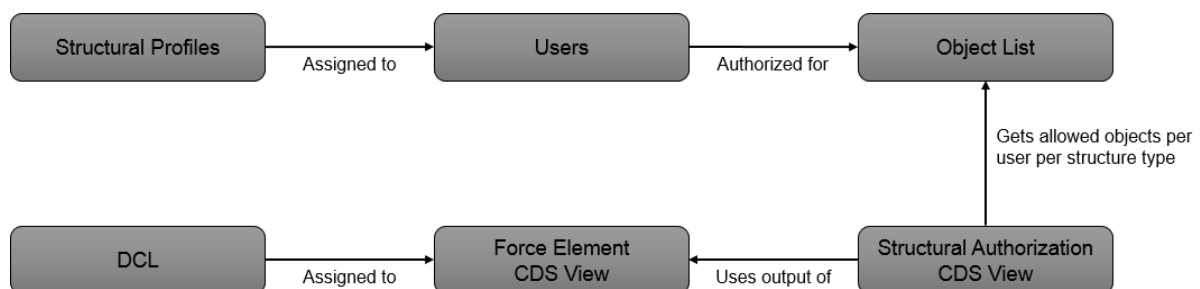
The picture below shows how structural authorizations are used in Defense & Security in conjunction with the S/4 programming model.

In addition to force elements, all assignments that are assigned to a force element are also enabled for structural authorization. This means that if user does not have authority for a force element, the assignments are also not visible (for example in other apps).

Users require change authority for force elements to change an assignment if the structural authorization is active.

In the case of force element to force element assignments (such as sup, sup by, maint, maint by), the user requires the authority for both the source and the target force elements to be able to edit.

An FMPO is also enabled for the structural authorization if an assignment from the FMPO to the force element exists. If the user does not have authority for the force element, the FMPO CRUD app does not display this FMPO. The user requires change authority for the assigned force element to be able to change the FMPO.



The existing configuration and artefacts, such as the structural profiles, transactions, such as OOSP/OOSB and other current report programs, such as RHAUTH01 are completely reused and integrated with the CDS views and DCLs to achieve the structural authorization.

The steps below are performed to achieve structural authorization:

1. Profiles for structural authorizations are created in the OOSP transaction. You must specify the details of the planning version, object ID, object type, evaluation path, status vector and processing type required.

Auth.profile	No.	Pla...	Type	Object I	Maint.	Eval.path	Status vec	Depth	Sign
	1	01	0		✓	DFPS_DEF	12345	2	
	2	01	0		✓	DFPS_DIS	12345	2	
	3	01	0		✓	B002	12345	2	

2. These profiles created are assigned to users in the OOSB transaction with a validity start date and end date as shown in the screenshot below that contains example values. The Exclude flag is now observed when executing the program (step 3). All force elements are deleted from the structural authorization table.

User name	Auth.profile	Start	End date	Exclusion	Display Objects
		22.03.2019	31.12.2032	<input type="checkbox"/>	
		31.12.2050	31.12.2099	<input type="checkbox"/>	
		25.03.2019	25.03.2099	<input type="checkbox"/>	
		25.03.2019	25.03.2099	<input type="checkbox"/>	
		01.01.1900	31.12.9999	<input type="checkbox"/>	

3. Execute the program DFS_FE_STRUC_AUTHZN manually if any changes are made in the OOSB or OOSP transaction. This displays the authorized objects IDs assigned to each user.

With the 2020 release, the structural authorization can also be applied to non-force element objects. The position, flexible material planning object (FMPO) and product master are currently supported.

13.13.5.1.1.1.3.3 Context-Based Structural Authorization

Context-based structural authorization is based on the structural authorization concept. For more information about the structural authorization concept, see [Structural Authorization \[page 870\]](#). Users and force elements can be assigned to respective profiles, but access is only granted if there is a match. If a user wants to perform different types of activities (such as display, edit, delete) on different force elements, they require context-based structural authorization. It is modeled using the personnel planning with context procedure used in Human Resources.

V_DFS_FE_PDCON

This view is used to activate context-based structural authorization for Defense & Security. You must select the indicator for it in transaction SM30. You must also enable the dummy authorization object DFS_FE_CON.

13.13.5.1.1.1.4 Reference to Reused Functions

This chapter lists the functions that have been integrated with Defense & Security or are reused by it. It provides you with information about the security-related aspects of these additional components.

Enterprise Portfolio and Project Management

Enterprise Portfolio and Project Management is integrated with the defense-specific capability business object. For more security-relevant information, see the chapter [Enterprise Portfolio and Project Management \[page 529\]](#).

Attachments

SAP Defense & Security allows the user to upload files as attachment, for example for the force element and capabilities business objects. Since attachments can potentially contain viruses, these viruses could enter your system when you upload the attachments. To reduce this risk as much as possible, we recommend you use an external virus scanner and restrict the MIME types for the attachments.

For more security-relevant information, see the chapter [Virus Scanning \[page 24\]](#).

Access to Attachments Using Microsoft Internet Explorer

You are using Microsoft Internet Explorer and want to display attachments in the browser. To do this, Microsoft Internet Explorer checks the content of the attachment to determine the file type and display the attachment correctly (MIME type sniffing). In the worst case, it is therefore possible that harmful files with an undesired file type are displayed in the browser or might cause other damage. To avoid this potential threat to security, deselect MIME type sniffing in the security settings for Microsoft Internet Explorer.

Classification

The classification Reuse UI component is integrated with the defense-specific force element, capabilities and mission essential tasks business objects. For more security-relevant information, see the chapter [Integrated Product Development for Discrete Industries \[page 560\]](#).

Status

Status management is implemented using SAP general status management for the flexible material planning object, capabilities and mission essential tasks business objects. The status framework allows you to define

your own status values. The authority objects B_USERSTAT and B_USERST_T can be used to handle the authority of the user and system status.

13.13.5.1.1.1.5 Reference to Data Control Language

Defense customers normally use a wide range of ECC / S/4HANA functions. At the same time, these customers often require more specialized authorization checks. To allow for this in a CDS-enabled environment, please check the data control language (DCL) customer extensibility functionality that is now available.

13.13.5.1.1.2 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries.

13.13.5.1.1.2.1 Deletion of Personal Data

The Defense & Security solution might process personal data that is subject to the data protection laws that apply in specific countries as described in SAP Note [1825544](#).

Destruction of personal data is supported in the capability, flexible material planning object (FMPO), scenario and platform code, since they store the personal number in their business objects. The goal is to provide an option for the customer to track access to the personal number in the capability, FMPO, scenario and platform code and to provide a program that will help them remove the assignment of the personal number from these objects.

Capability

The destruction objects in the capability are mentioned as follows.

Application	Detailed Description	Provided Deletion Functionality
Capability	Destruction object = DFS_CAP_OWNER (for active persistency)	<p>The corresponding ILM object is DFS_CO_CAPABILITY.</p> <p>The corresponding data deletion program is DFS_CAP_OWNER_DES.</p> <p>The program requires a capability object ID as input.</p> <p>The program reads the configuration to identify whether the capability object ID mentioned on the selection screen has an expired person (owner) contract end date, and whether the corresponding retention period is over.</p> <p>If both of these conditions are met, the personal ID attached to such a capability code is deleted.</p> <p>The contract end date for the person is taken from the table PA0000; field 'BEGDA'. Example: Start date of the retirement record with the field 'STAT2' is not equal to '1' (Inactive) or '3' (Active).</p>
Capability	Destruction object = DFS_CAP_OWNER_DRAFT (for draft persistency)	<p>The corresponding ILM object is DFS_CO_CAPABILITY_D.</p> <p>The corresponding data deletion program is DFS_CAP_OWNER_DRAFT_DES.</p> <p>The program requires a capability object ID as input.</p> <p>The program reads the configuration to identify whether the capability object ID mentioned on the selection screen has an expired person (owner) contract end date, and whether the corresponding retention period is over.</p> <p>If both of these conditions are met, the personal ID attached to such a capability code is deleted.</p> <p>The contract end date for the person is taken from the table PA0000; field 'BEGDA'. Example: Start date of the retirement record with the field 'STAT2' is not equal to '1' (Inactive) or '3' (Active).</p>

Flexible Material Planning Object

Application	Detailed Description	Provided Deletion Functionality
FMPO	Destruction object = DFS_FMPO_VARNT_DES (for active persistency)	<p>The corresponding ILM object is DFS_FMPO_VARNT_DES.</p> <p>The corresponding data deletion program is DFS_FMPO_VARNT_DES.</p> <p>The program reads the configuration to identify whether the FMPO status is obsolete and the corresponding retention period is over based on the last changed date.</p> <p>If both of these conditions are met, the personal ID attached to such an FMPO variant is deleted.</p> <p>The last changed date for the FMPO variant is taken from the table DFS_FMPO_VARNT; field FLXMTPLOBJVARLASTCHANGEDDTETME.</p>
FMPO	Destruction object = DFS_FMPO_VARNT_D_DES (for draft persistency)	<p>The corresponding ILM object is DFS_FMPO_VARNT_D_DES.</p> <p>The corresponding data deletion program is DFS_FMPO_VARNT_D_DES.</p> <p>The program reads the configuration to identify whether the status is obsolete and the corresponding retention period is over based on the last changed date.</p> <p>If both of these conditions are met, the personal ID attached to such an FMPO variant is deleted.</p> <p>The last changed date for the FMPO variant is taken from the table DFS_FMPO_VARNT_D; field FLXMTPLOBJVARLASTCHANGEDDTETME.</p>

Scenario

The destruction object in the scenario is mentioned as follows.

Application	Detailed Description	Provided Deletion Functionality
Scenario	Destruction object = DFS_SCEN_OWNER_DES	<p>The corresponding ILM object is DFS_SCENARIO.</p> <p>The corresponding data deletion program is DFS_SCEN_OWNER_DES.</p> <p>The program requires a scenario ID as input.</p> <p>The program reads the configuration to identify whether the scenario ID mentioned on the selection screen has an expired person (owner) contract end date, and whether the corresponding retention period is over.</p> <p>If both conditions are met, the personal ID attached to such a scenario is cleared from the record.</p> <p>The contract end date for the person is taken from the table PA0000; field 'BEGDA'. Example: Start date of the retirement record with the field 'STAT2' is not equal to '1' (Inactive) or '3' (Active).</p>

Platform Code

The destruction object in the platform code is mentioned as follows.

Application	Detailed Description	Provided Deletion Functionality
Manage Platform Code	Destruction object = DFS_MAINT_OWNER (for active persistence)	<p>The corresponding ILM object is DFS_MAINT_PLTFRM_DES.</p> <p>The corresponding data deletion program is DFS_MAINT_OWNER_DES.</p> <p>The program requires a platform object ID as input.</p> <p>The program reads the configuration to identify whether the platform object ID mentioned on the selection screen has an expired person (owner) contract date, and whether the corresponding retention period is over.</p> <p>If both of these conditions are met, the personal ID attached to such a platform code is deleted.</p> <p>The contract end date for the person is taken from the table PA0000; field 'BEGDA'. Example: Start date of the retirement record with the field 'STAT2' is not equal to '1' (Inactive) or '3' (Active).</p>

13.13.5.1.1.2.2 Read-Access Logging

Read access to personal data is partially based on legislation and can be logged. The RAL component can be used to monitor and log read-access to data, and provide information, such as which business users accessed personal data and when they did so.

Read-access logging is supported in all defense objects. Find the details below.

In the following configurations given as an example, fields are logged in combination with additional fields in the following business contexts:

Configuration	Fields Logged	Business Context
DFS_CAP_CAPBLTOBJECT_SRV	DFSCAPBLTOBJTYPE DFSCAPABILITYOBJECTID DFSCAPBLTOBJOWNER DFSCAPBLTOBJTYPE PROJECT STATUSCODE EMPLOYEEENAME EMPLOYEEPERSONNELNUMBER	Logging of the BP/EMPLOYEE domain in the capability object.
DFS_FMPO_FLXMTPLOBJ_SRV	FLXMTPLOBJVAROWNEROBJECTID FLXMTPLOBJVARRESPPLNROBJEC-TID	Logging of the BP/EMPLOYEE domain in the FMPO.

Configuration	Fields Logged	Business Context
UI_DFS_SCENARIO	DFSCAPABILITYOBJECTID DFSCAPBLTOBJNAME DFSCAPBLTOBJSHORTNAME DFSDIRECTIVEDESCRIPTION DFSDIRECTIVEID DFSOBJECTNAME DFSSCENARIOALTVESTDAMOUNTINTC DFSSCENARIOALTVID DFSSCENARIOALTVNAME DFSSCENARIOALTVSHORTNAME DFSSCENARIOALTVTASKID DFSSCENARIOALTVTASKNAME DFSSCENARIOALTVTRANSCRCY DFSSCENARIODESC DFSSCENARIOID DFSSCENARIOISHORTNAME DFSSCENARIOSTATUS DFSSCENARIOSTATUSOBJECTID DFSSCENARIOIOTYPE DFSSCENARIOVALIDITYENDDATE DFSSCENARIOVALIDITYSTARTDATE FORCEELEMENTORGID FRCELMNTORGNAM PROJECT PROJECTNAME	Logging of the DEFENSE/ IS_DFS_SENSITIVE domain in the scenario.
UI_DFS_SCENARIO	EMPLOYEEENAME DFSSCENARIOOWNER	Logging of the SAP/EMPLOYEE domain in the scenario.

Configuration	Fields Logged	Business Context
DFS_POS_DEFENSEPOSITION_SRV	PERSONNELNUMBER DFSPOSITIONVALDTYSTARTDATE DFSPOSITIONVALDTYENDDATE DFSPOSITIONRELATEDOBJECTID DFSPOSITIONOPEXERCISEID DFSPOSITIONROTATIONKEY DFSOBJECTSUBTYPE	Logging of the BP/EMPLOYEE domain in the defense position.
UI_C_DFS_MAINT_PLATFORM	DFSMAINTPLATFORMID DFSMAINTPLATFORMLONGNAME DFSMAINTPLATFORMDESCRIPTION DFSMAINTPLATFORMSTATUSTEXT PARTNERFUNCTIONNAME DFSMAINTPLATFORMSHORTNAME DFSMAINTPLATFORMOWNERNAME DFSMAINTBUSINESSOBJECTNAME DFSASSGMTVALDTYSTRDATE DFSMAINTPARENTPLATFORMID DFSMAINTBUSINESSOBJECTTYPE DFSMAINTPLATFORMTYPE DFSMAINTPLATFORMOWNERID DFSMAINTBUSINESSOBJECTID DFSMAINTPLATFORMTYPETEXT DFSASSGMTVALDTYENDDATE DFSMAINTPARTNERFUNCTION	Logging of the BP/EMPLOYEE domain in the defense maintenance platform.

The new log domain *IS_DFS_SENSITIVE* is also created, which can be used by customers to log the fields that they classify as 'sensitive' across all defense objects.

SAP delivers sample configurations for applications. To use these configurations, save the ZIP attachments from the SAP Note [2805607](#) for release OP 1909 and SAP Note [2948600](#) for release OP 2020. Extract these ZIP files and import the RAL configurations using the import function for configurations in the transaction SRALMANAGER.

13.13.5.1.1.3 Change Logs

Users do not see the change log views in the default delivery of Defense & Security due to data protection reasons.

All defense objects use change logs as a default. However, you cannot see an integrated view of the change logs in the Fiori apps for Defense, and must instead retrieve and view these change logs externally. Customers must ensure that sufficient authorization and access restrictions (for example those that apply to viewing personal data changes) are in place if such a provision is available for users.

The change document objects created are shown below.

Change Document	Business Context
DFS_CO_CHGDOC	Change logging for the capability object
DFS_MET_CHGDOC	Change logging for METL
DFS_STAT_CHGDOC	Change logging for the capability statement
DFS_ASSGMT	Change logging for the DFS assignment
DFS_SCN_CHGDOC	Change logging for the defense scenario
DFS_MODEL	Change logging for the defense modeling canvas
DFS_FE_MEASURES	Change logging for manage measures
DFS_PLC_CHGDOC	Change logging for the platform code
DFS_ALLWNC	Change logging for the defense allowance
DFS_FMPO_CHGDOC	Change logging for FMPO

The existing HR change document objects are used for force element and reference force element objects, since the backend APIs are reused in the Fiori app transactions.

13.13.5.1.2 Explosives Management

Role and Authorization Concept

Frontend Role

Standard Roles for Explosives Management

Role	Name
SAP_BR_WAREHOUSE_CLERK_EXP	Warehouse Clerk

Backend Role

Authorization Objects for Explosives Management

Authorization Object	Name
/SCWM/LG	EWM Storage Bin
EHFND_DTS	EHS: Data Series
B_BUPA_RLT	Business Partner: BP Roles
S_SERVICE	Check at Start of External Services
S_START	Start Authorization Check for TADIR Objects
EHFND_CHM	EHS: Chemical
EHFND_CTRL	Controls
EHFND_DCTR	EHS: Default Controls
EHFND_LOC	Location
EHFND_VEN	EHS: Vendor
EHSS_AGT	EHS: Risk Assessment Agent
EHSS_JOB	EHS: Job Authorization Object
EXM_CMPCHK	Authorization for Compliance Check Object Types
EXM_LOC	Authorization Object for Location Types
P_ORGIN	HR: Master Data
P_PERNR	HR: Master Data - Personnel Number Check
/SCWM/CHG	EWM Batch
C_KLAH_BKL	Authorization for Classification
C_LIME_HU	LIME Handling Unit
C_LIME_LOC	LIME Location
C_LIME_SI	LIME Stock Item
C_TCLA_BKA	Authorization for Class Types
C_TCLS_BER	Authorization for Org. Areas in Classification System
C_TCLS_MNT	Authorization for Characteristics of Org. Area
K_CCA	CO-CCA: Gen. Authorization Object for Cost Center Accounting

Authorization Object	Name
K_CSXS	CO-CCA: Cost Center Master
M_MATE_CHG	Material Master: Batches/Trading Units
PLOG	Personnel Planning
S_TABU_DIS	Table Maintenance (using standard tools such as SM30)
S_TABU_NAM	Table Access by Generic Standard Tools

To access the Manage Explosive Storage Locations application, you must create a backend role with the following WebDynpro applications:

Name	Description
DFPS_EXPL_LHR_OIF	Manage Location Structure
DFPS_EXPL_LOC_UI_ENTRY	Explosive Storage Location UI Entry
DFPS_EXPL_STR_FACILITY	Explosive Storage Location
EHFND_LOC_BULKCHG_GAF	Change Attributes
EHFND_UI_DEF_CTR_OVP	Default Controls

Data Protection

Deletion of Personal Data

The Manage Explosive Storage Locations application is based on the Manage Locations application of the Environment, Health, and Safety. For more information, see [Deletion of Personal Data \[page 65\]](#)

The Manage Explosive Storage Locations application reuses the following archiving object from the Manage Locations application:

Application Objects	Provided Deletion Functionality
Assignment of Person to Locations	Archiving object EHFND_LOCP

For more information, see the section Application Objects and Available Deletion Functionality in Health and Safety Management in [Deletion of Personal Data \[page 65\]](#).

13.13.5.2 Higher Education and Research

13.13.5.2.1 Authorizations

The SAP ECC Industry Extension Higher Education & Research component uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the ABAP Platform Security Guides also apply to the SAP ECC Industry Extension Higher Education & Research component. The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) when using ABAP technology and the User Management Engine's user administration console when using Java.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used by SAP Student Lifecycle Management (SLCM).

Role	Description
Composite Roles	
SAP_CM_ADM_COORDINATOR	Admission coordinator
SAP_CM_ADM_OFFICER	Admission officer
SAP_CM_ASM_COORDINATOR	Assessment coordinator
SAP_CM_ASM_OFFICER	Assessment officer
SAP_CM_STREC_COORDINATOR	Student records coordinator
SAP_CM_STREC_OFFICER	Student records officer
Single Roles	
SAP_CM_ACCOUNT_DATA_UPDATE	Technical user for automatic update of student account data after changes to account-relevant student master data
SAP_CM_ADMIN_ACAD_STRUCTURE	Administrator for the academic structure (internal single role)
SAP_CM_ADMOFF_STUDYDATA	Activities for the admission coordinator
SAP_CM_ADMREGDATA_DISP	Display study data
SAP_CM_ALL	

Role	Description
SAP_CM_ASMCO_ADDACT	Additional activities for the assessment coordinator
SAP_CM_ASMDATA_DISP	Display progression and grades
SAP_CM_ASMOFF_ACT	Activities for the assessment officer
SAP_CM_STMASTERDATA_DISP	Display student master data
SAP_CM_STMASTERDATA_MAINT	Edit student master data
SAP_CM_STRCO_ADDACT	Additional activities for the student records coordinator
SAP_CM_ASMDATA_DISP	Display progression and grades
SAP_CM_ASMOFF_ACT	Activities for the assessment officer
SAP_CM_STMASTERDATA_DISP	Display student master data
SAP_CM_STMASTERDATA_MAINT	Edit student master data
SAP_CM_STRCO_ADDACT	Additional activities for the student records coordinator
SAP_CM_STROFF_ACT	Activities for the student records coordinator
SAP_CM_MODULEBOOK	Module booking (only up to release CM 4.72)
SAP_CM_REGIST	Activities for registration (only up to release CM 4.72)
SAP_CM_STUDENTMASTER	Student master data processing (only up to release CM 4.72)

All of the above roles are automatically generated by the system.

i Note

SAP_IQ_CAMPUS and SAP_CM_ALL are critical roles because they contain a comprehensive authorization for all Student Lifecycle Management functions. The following roles are obsolete as of the SAP ECC Industry Extension Higher Education & Research 6.0 release:

- SAP_IQ_CAMPUS
- SAP_CM_MODULEBOOK
- SAP_CM_REGIST
- SAP_CM_STUDENTMASTER

Standard PFCG Roles in SAP Student Lifecycle Management

If a user does not want to use the portal role, you can choose the PFCG role option. The SLCM application provides the following PFCG roles:

Name of PFCG Role	Relevance to NWBC	Relevance to Portal Role
SAP_SR_ACADEMIC_ADVISOR_5	NWBC role for advisor	Equivalent to the portal role <code>Academic Advisor</code>
SAP_SR_UNIVERSITY_INSTRUCTOR_5	NWBC role for university instructor	No equivalent portal role available
SAP_SR_STUDENT_5	NWBC role for student	Equivalent portal role <code>Student</code>

Once you configured these roles you can access the applications attached to the role using SAP NetWeaver Business Client. You can use these as entry points to the different applications that can be accessed by the academic advisor, the instructor or the student.

Standard Authorization Objects

If a user does not want to use the portal role, you can choose the PFCG role option. The SLCM application provides the following PFCG roles:

Authorization Object	Description
P_CM_AUDCT	Student Lifecycle Management: requirement catalogs
P_CM_AUDIT	Audits
P_CM_AUDPR	Requirement profile
P_CM_CORR	Correspondence
P_CM_FCDOC	Student accounting document
P_CM_PROC	Activity
P_CM_UCAS	Authorization Object Student Lifecycle Management UCAS (only for Great Britain)
P_CM_UCASR	Authorization Object Student Lifecycle Management UCAS for Reports (only for Great Britain)
P_CM_NLPAY	NL Payment Details Authorization Object
P_CM_NLVER	NL Verification Authorization Object

Basic Authorizations in SAP Student Lifecycle Management

There are three important authorization objects within SLCM to simplify authorization assignment: :

- S_TCODE
S_TCODE checks whether a user is allowed to start a given transaction. Every time the user starts a menu command or a transaction code using the command line, the roles assigned to the user are checked to see whether the user has the authority to execute this transaction.
- PLOG
PLOG checks whether a user is allowed to read, write or insert specific HR Infotypes.
- P_CM_PROC
P_CM_PROC checks whether a user has the authority for a specific Student Lifecycle Management process.

Structural Authorizations in SAP Student Lifecycle Management

Structural authorizations enable you to define the set of objects the user is authorized to process. You determine these objects using evaluation paths. For example, you can define whether the user receives a display authorization or a maintenance authorization for these objects.

- Evaluation Paths
An evaluation path is an instruction for the system that determines which object types and relationships are to be included in an evaluation of the organizational plan. It describes the chain of relationships that exist between objects in a hierarchical structure. The report takes into account only the objects that lie along the specified evaluation path.
- Organizational Structure
One or more relationships are then used as paths to evaluate structural information in your organizational plan (relating to the organizational or reporting structures) or matrix organization. The sequence of the relationships included in the evaluation path is decisive in how the results of the evaluation are displayed.

i Note

As functions of other applications areas, for example, Training and Event Management, Notification Processing or Student Accounting are integrated into SLCM, users also need authorizations for these areas.

i Note

SLCM contains a number of single roles, which you can combine with the roles of other application areas to create composite roles. You can either assign a composite role or individual roles to users.

Authorizations in Business Rule Framework plus (BRFplus)

To handle the BRFplus security, the standard authorizations are available in the BRFplus framework.

For information about the authorization concept of BRFplus, go to https://help.sap.com/s4hana_op_2020, enter *Services for Application Developers* into the search bar, press , open the search result with that title, and navigate to ► [Business Rule Framework plus \(BRFplus\)](#) ► [Concepts](#) ► [Authorizations](#) ►

13.13.5.2.2 Deletion of Personal Data

Use

The student administration of the `Student Lifecycle Management` application might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note 1825544. The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. The Student Lifecycle Management (SLCM) solution uses SAP ILM to support the blocking and deletion of personal data as described in the following sections. SAP delivers an end of purpose check (EoP) for the students registered in the SLCM application. SAP delivers an end-of-purpose check (EOP) for the blocking of business partner data if the SLCM application has a student linked to a business partner. All applications register either an end of purpose check (EoP) in the Customizing settings for the blocking and deletion of the business partner data or a where-used check (WUC). n.

You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► [Product Assistance](#) ► [Cross Components](#) ► [Data Protection](#) ►.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. . This check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases:

- Phase one: The relevant data is actively used.
- Phase two: The relevant data is actively available in the system.
- Phase three: The relevant data needs to be retained for other reasons.

For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities. Blocking of data can impact system behavior in the following ways:

- Display: The system does not display blocked data.
- Change: It is not possible to change a business object that contains blocked data.
- Create: It is not possible to create a business object that contains blocked data.
- Copy/Follow-Up: It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- Search: It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data. For information about the configuration settings required to enable this three-phase based end of purpose check, see the Process Flow and Configuration: Simplified Blocking and Deletion.

End of Purpose Check (EoP) in SLCM

The end-of-purpose check for SLCM is a simple check to ensure data integrity in the event of potential blocking. It checks whether there is any dependent data for a business partner that is a student in the SLCM application and returns one of the following statuses:

- If the business partner is not a student the system returns status as '1' (No business with business partner).
- If the business partner exists as a student in the SLCM system, then the system checks for the SORT (Start of retention time), and depending on the date, returns the status '2' (business is ongoing) or '3' (business is complete).

The system does not block the business partner related to the student if the status is '3', business is ongoing .

Relevant Application Objects and Available Deletion Functionality

Archiving Object	Description
HRIQ_ACADW	IS-HER-CM: Academic work - Admissions registrations
HRIQ_AD	IS-HER-CM: Admission decision framework
HRIQ_EXTTR	IS-HER-CM: Student external transcripts
HRIQ_FEE	IS-HER-CM: Fee calculation document
HRIQ_MODBK	IS-HER-CM: Module booking
HRIQ_PROC	IS-HER-CM: Activity document
HRIQ_STAT	IS-HER-CM: Statistical reporting
HRIQ_STGRT	IS-HER-CM: Student grants
HRIQ_STMD	Archiving Object for Student master data
HRIQ_STYDT	IS-HER-CM: Study data
HRIQ_ATTDN	Attendance data

Archiving Object	Description
GFD_ARCH1	Archiving for Admission Portal (Form Runtime) and MyRequest applications

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
PSCM	Student Lifecycle Management: Public Sector Campus Management	HRIQ_ATTDN: Data Destruction in Student Lifecycle Management
PSCM	Student Lifecycle Management: Public Sector Campus Management	HRIQ_SPCD: Data Destruction for Student Special Category data

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
PSCM	EoP implemented	EoP checks if the business for the student and related business partner is complete or ongoing.

Process Flow

1. Before archiving data, you must first define residence time and retention periods in SAP Information Lifecycle Management (ILM).
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
3. You do the following:
 - Run transaction IRMPOL and enter the required retention policies for the central business partner (ILM object: CA_BUPA).
 - Run transaction BUPA_PRE_EOP to enable the end of purpose check function for the central business partner.
 - Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and vendor master in SAP S/4HANA (ILM objects: HRIQ_STMD).
 - Run transaction CVP_PRE_EOP to enable the end of purpose check function for the customer master and vendor master in SAP S/4HANA .
4. Business users can request unblocking of blocked data for customers, vendors and central business partners by using the transaction BUP_REQ_UNBLK.

5. If you have the necessary authorizations, you can unblock data by running the transaction `BUFA_PRE_EOP` and `CVP_UNBLOCK_MD`.
6. You delete data by using the transaction `ILM_DESTRUCTION` for the ILM objects of SLCM.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for `Cross-Application Components` under `Data Protection`.

- Define the settings for authorization management under [► Data Protection ► Authorization Management ▾](#). For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for `Cross-Application Components` under [► Data Protection ► Blocking and Unblocking ► Business Partner ▾](#)

13.13.5.2.3 Data Storage Security

Data Storage

The data for the application are saved in the database tables. Only the data for academic structure can come from a file system, the security aspects of which is described in the next section. There is structural authorization and role based authorization to control access to these data. For more information, see Authorizations.

Using Logical Path and File Names to Protect Access to the File System

The `SAP Student Lifecycle Management` applications save data in files in the file system. Therefore, provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by the `Student Lifecycle Management` application and for which programs these file names and paths apply:

Logical File Names Used

The following logical file names have been created in order to enable the validation of physical file names:

- `ISHER_WEBCATALOGXML`

- Programs using this logical file name and parameters used in this context:
 - RHIQ_XML_ACADSTRUC (XML Files of Academic Structure)

Logical Path Names Used

The logical file names listed above all use the logical file path ISHER_WEBCATALOG.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see about data storage security, see the respective chapter in the ABAP Platform Security Guide.

13.13.5.2.4 Read Access Logging (Industry Applications)

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions.

Read access to personal data is partially based on legislation, and it is subject to logging functionality. The Read Access Logging (RAL) component can be used to monitor and log read access to data and provide information such as which business users accessed personal data (for example, fields related to bank account data), and when they did so. In RAL, you can configure which read-access information to log and under which conditions. SAP delivers sample configurations for applications. For more information, see the application-specific chapters of the Security Guide.

You can display the configurations in the system by performing the following steps:

1. In transaction SRALMANAGER, on the *Administration* tab page, choose *Configuration*.
2. Choose the desired channel, for example, WebDynpro.
3. Choose Search.
The system displays the available configurations for the selected channel.
4. Choose Display Configuration for detailed information on the configuration. For specific channels, related recordings can also be displayed.

Prerequisites

Before you can use the delivered RAL configurations, the following prerequisites are met:

- You are using:
 - SAP NetWeaver 7.1 SPO
 - AS ABAP 7.51
 - Kernel 7.45 SP21 and above
 - SAP_UI 7.51 (UI5 1.40)
- The RAL configurations have been activated.
- You have enabled RAL in each system client.

More Information

For general information on Read Access Logging, go to https://help.sap.com/s4hana_op_2020, open the product assistance, and navigate to ► [Cross Components](#) ► [Data Protection](#) ► [Security Safeguards Regarding Data Protection](#) ► [Read Access Logging \(RAL\)](#) ►.

13.13.5.2.5 Read Access Logging for Admission Portal

Use

Read access to personal data is partially based on legislation, and it is subject to logging functionality. The Read Access Logging (RAL) component can be used to monitor and log read access to data and provide information such as which business users accessed personal data (for example, fields related to bank account data), and when they did so.

In RAL, you can configure which read-access information to log and under which conditions.

SAP delivers sample configurations for applications. For more information, see the application-specific chapters of the Security Guide

You can display the configurations in the system by performing the following steps:

1. In transaction SRALMANAGER, on the [Administration](#) tab page, choose [Configuration](#).
2. Choose the desired channel, for example, OData service.
3. Choose [Search](#).
The system displays the available configurations for the selected channel.
4. Choose [Display Configuration](#) for detailed information on the configuration. For specific channels, related recordings can also be displayed.

i Note

For a list of the delivered log domains, see the product assistance at SAP Help Portal under https://help.sap.com/s4hana_op_2020 ► [Product Documentation](#) ► [Security Guide](#) ► [SAP S/4HANA Industries](#) ► [Higher Education and Research](#) ► [Data Protection](#) ►

Prerequisites

Before you can use the delivered RAL configurations, the following prerequisites are met:

- You are using:
 - SAP NetWeaver 751 SP0
 - AS ABAP 7.51
 - Kernel 7.45 SP21 and above
 - SAP_UI 7.51 (UI5 1.40)
- The RAL configurations have been activated.
- You have enabled RAL in each system client.

More Information

For general information on Read Access Logging, go to https://help.sap.com/s4hana_op_2020, open the product assistance, and navigate to ► [Cross Components](#) ► [Data Protection](#) ► [Security Safeguards Regarding Data Protection](#) ► [Read Access Logging \(RAL\)](#) ►.

For up-to-date information on the delivered RAL configurations, see SAPNote [2347271](#)🔗.

13.13.5.2.6 Specific Read Access Log Configurations

In Read Access Logging (RAL), you can configure which read-access information to log and the conditions. SAP delivers sample configurations for applications. In order to use these configurations, save the ZIP attachments from the following SAP Notes:

[2375056](#)🔗 - Read Access Logging content for application Student Life Cycle Management (SLCM)

Extract these ZIP files, and import the RAL configurations using the Import function for configurations using transaction SRALMANAGER. The Student Lifecycle management (SLCM) Application ,IS-HER-CM , Student master data (PIQSTM) logs data in order to save the Students master data and also personal data . You can

find the configurations as described in the Read Access Logging chapter. In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Configuration	Fields Logged	Business Context
SLCM_REC_RAL_STMD	Student Number Ethnic Origin / Religion Student Disability / Challenge / Health Student Social Status	The Student Social and Health and Ethnic data is stored as master data in SAP SLCM Application. This data is used in calculation of Grants and Fee depending on the various parameters. The Same transaction is used to store multiple academic data and in few of the tabs these personal data is shown .

13.13.5.2.7 Specific Read Access Log Configurations for Admission Portal

In Read Access Logging (RAL), you can configure which read-access information to log and the conditions. SAP delivers sample configurations for applications. In order to use these configurations, save the ZIP attachments from the following SAP Notes:

[2601072](#) - Read Access Logging content for application Student Life Cycle Management (SLCM)

Extract these ZIP files, and import the RAL configurations using the Import function for configurations using transaction SRALMANAGER.

The Admission Portal logs data in order to capture the data from the admission application forms (form runtime) and my request applications. You can find the configurations as described in the Read Access Logging chapter.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Configuration	Fields Logged	Business Context
GFD_CONFIG_SRV	GFD_FormSubmission:CONTENT	To capture the standard fields data which comes in JSON format
GFD_CONFIG_SRV	GFD_FormSubmission:CUSTOM_CONTENT	To capture the custom content fields data which also comes in JSON format

13.13.5.2.8 Consent Administration

Student Lifecycle Management captures the consent management questions in the preliminary questionnaire. The information entered in the fields of the questionnaire is only stored when the user has opted **Yes** for consent management question. When the user clicks **Apply**, the BAdI `BADI_GFD_FORM_REDIRECT` checks this logic

and saves the data. In case the user selects *No* for the consent management question an error message must be created by you to return without saving the data.

→ Recommendation

You can implement the BAdI `BADI_GFD_ERROR_INFO` for further processing like *Saving* or *Declining*.

In My Request application, you must handle this saving or rejecting of data in the error handling BAdI `BADI_GFD_ERROR_INFO`.

Following are some of the important consent management questions:

Attribute Name	Data Type	Length	Description	Mandatory	Important
JURISDICTION	CHAR	3	Jurisdiction	X	
VALID_FROM	DEC	21,7	Consent's Valid From Point in Time	X	
VALID_TO	DEC	21,7	Consent's Valid To Point in Time	X	
EXPIRING_DATE	DEC	21,7	Expiring Date		
GRANTED_AT	DEC	21,7	Granted At		X
GRANTED_BY	CHAR	128	Granted By User		X
WITHDRAWN_AT	DEC	21,7	Point in time Consent is withdrawn		X
WITHDRAWN_BY	CHAR	128	User who withdraw the Consent		X
LANGUAGE	LANG	1	Language	X	
CNSNT_QSTN_TXT	STRING	-	Consent Text	X	
PURPOSE_NAME	CHAR	30	Purpose Name	X	
PURPOSE_DESCRIPTION	CHAR	80	Purpose Description		
PURPOSE_SENSITIVE_PERS_DATA	CHAR	1	Purpose Sensitive Data	X	
APPLICATION_NAME	CHAR	30	Application Name		X
APPLICATION_DESCRIPTION	CHAR	80	Application Description		

13.13.5.3 Public Sector

13.13.5.3.1 Public Sector Management

Data Storage

Using Logical Paths and File Names to Protect Access to the File System

Public Sector Management stores data in files in the file system. For this reason, it is important to be able to grant access to the files in the file system explicitly without granting access to other folders or files (also known as folder traversals). You do this in the system by entering logical paths and file names that are assigned to the physical paths and file names. This assignment is validated during runtime, whereby an error message is issued whenever a user tries to access a folder that does not correspond to a stored assignment.

The following lists provide an overview of the logical file names and paths that are used by Public Sector Management and of the programs for which these file names and paths are valid:

Logical File Names Used in Public Sector Management

The logical file name PSM_EXECUTION_DATA_EXPORT has been created to enable the validation of physical file names.

The program RFEXBLK0 uses this logical file name.

Logical Path Names Used in Public Sector Management

The above-mentioned logical file name uses the logical file path PSM_ROOT.

Activating the Validation of Logical Paths and File Names

These logical paths and file names are entered in the system for the corresponding programs. For reasons of downward compatibility, validation is deactivated by default during runtime. To activate validation during runtime, define the physical path using transactions FILE (across all clients) and SFO1 (client-specific). To determine which paths are used by your system, you can activate the relevant settings in the Security Audit Log.

13.13.5.3.1.1 Funds Management

Standard roles for Funds Management (PSM-FM)

Role	Name
SAP_IS_PS_CENTRAL_FUNCTION	Funds Management Central Function
SAP_IS_PS_PO_CONSUMPTION	Postings: Consume Funds
SAP_IS_PS_MD_STRUCTURE	Master Data Funds Management: Maintain Structure

Role	Name
SAP_IS_PS_BCS_AVC_TOOLS	Availability Control - Tools
SAP_IS_PS_BCS_BUD_TOOLS	Budgeting - Tools
SAP_IS_PS_PO_RECONCILE	Reconciling Data with Feeder Applications
SAP_IS_PS_BCS_BUD_MAINTENANCE	Maintain Budget Data
SAP_IS_PS_BCS_BUD_PLANNING	Plan Budget Data
SAP_IS_PS_BCS_DISPLAY	Display Budget Values (BCS)
SAP_IS_PS_BCS_STATUS_MAINTAIN	Budgeting – Assign Status
SAP_IS_PS_BCS_STRUCT_DEF	Maintain Budget Structure
SAP_IS_PS_BCS_STRUCT_TOOLS	Budget Structure - Tools
SAP_IS_PS_CASH_DESK	Payment at Cash Desk
SAP_IS_PS_CF_CHECK	Check Budget Closing
SAP_IS_PS_CF_OI_EXECUTE	Carry Forward Consumable Budget
SAP_IS_PS_CF_OI_PREPARE	Prepare Carryforward of Consumable Budget
SAP_IS_PS_MD_DISPLAY	Funds Management Master Data: Display Functions
SAP_IS_PS_MD_ZUOB	Funds Management Master Data: Assignment to CO Structures
SAP_IS_PS_PO_COMMITMENTS	Postings: Commit Funds
SAP_IS_PS_PO_CONSUMPTION_DISP	Postings: Consumed Funds Display
SAP_IS_PS_PO_FOR	Postings: Forecast of Revenue
SAP_IS_PS_PO_TRANSFERS	Postings: Transfer Consumable Budget
SAP_FI_GL_REORG_MANAGER	Reorganization Manager
SAP_FI_GL_REORG_OBJLIST_OWNER	Object List Owner

Authorization objects for Funds Management (PSM-FM)

Authorization Object	Name
F_FICB_FKR	Cash Budget Management/Funds Management FM Area
F_FICB_VER	Cash Budget Management/Funds Management Version
F_FICA_FOG	Funds Management: Authorization Group of Fund
F_FICA_FSG	Funds Management: Authorization Group for Funds Center
F_FICA_SEG	Funds Management: Authorization Group for All Funds Centers
F_FICA_SIG	Funds Management: Authorization Group Internal Funds Centers
F_FICA_FPG	Funds Management: Authorization Group for Commitment Item
F_FICA_TRG	Funds Management: Authorization Groups of FM Acct Assignment
F_FMMD_FAR	Funds Management: Functional Area (Authorization Group)
F_FMMD_MES	Funds Management: Funded Program (Authorization Group)
F_FMMD_BPG	F_FMMD_BPG
F_FMMD_FPG	Funds Management: Funded Program Sets
F_FICA_FNG	Funds Management: Fund Groups
F_FICA_FAG	Funds Management: Function Groups
F_FICA_CIG	Funds Management: Commitment Item Group
F_FICA_FCG	Funds Management: Funds Center Groups
F_FMCA_SHE	Clarification Worklist (FMSHERLOCK)

See also the documentation for Funds Management on the *SAP Help Portal* at help.sap.com > *S/4 HANA* > *Accounting* > *Public Sector Management* > *Funds Management* > *Authorizations* .

Authorization objects of the Budget Control System (BCS)

Authorization Object	Name
F_FMBU_ACC	Budgeting: Account Assignment
F_FMBU_STA	Budgeting: Status
F_FMBU_KYF	Budgeting: Key Figure
F_FMBU_DOC	Budgeting: Document Type
F_FMBU_VER	Budgeting: Version and Budget Category

You can use the following BAdI to implement enhancements to the authorization concept:

BAdI	Name
FM_AUTHORITY_CHECK	Enhance Authorization Check in PSM-FM

13.13.5.3.1.1.1 Deletion of Personal Data in Funds Management

Funds management may process data subject to the data protection laws applicable in specific countries as described in SAP Note [1825544](#).

End of Purpose Check

An EoP check determines whether data are relevant for business activities based on the retention period defined for the data.

For information about the configuration settings required to enable this three-phase based EoP check, see [Process Flow and Configuration: Simplified Blocking and Deletion](#).

Relevant Application Objects and Available Deletion Functionality

Funds Management uses SAP ILM to support the deletion of personal data. For more information, see the documentation for [SAP Information Lifecycle Management](#).

Archiving Object	Description
FM_BUDENT	Budget entry documents
FM_BUDHIE	Budget hierarchy documents
FM_BUDSUM	Budget totals
FM_DOC_CO	CO postings
FM_ACTSUM	Commitments and actuals totals
FM_DOC_OI	Commitments and funds transfers
FM_FUNRES	Earmarked funds
FM_DOC_FI	FI postings

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

Run Deletion Programs

We recommend scheduling regular jobs to run the deletion programs using the *Define Background Job*.

13.13.5.3.1.2 Grants Management

Standard roles for Grants Management (PSM-GM)

Function	Name	Function
SAP_FI_GM_GRANT_ANALYST	Grants Management: Grant Analyst	Master data maintenance, execution of reports
SAP_FI_GM_GRANT_MANAGER	Grants Management: Grant Manager	New entry, check, and approval of master data, execution of billing program
SAP_FI_GM_PROGRAM_ANALYST	Grants Management: Program Analyst	Creation of master data, processing of proposals and budget
SAP_FI_GM_PROGRAM_MANAGER	Grants Management: Program Manager	Check and approval of proposals and budget

Function	Name	Function
SAP_FI_GM_PROJECT_MANAGER	Grants Management: Project Manager	Management of grants and budget, execution of reports

Authorization Objects for Grants Management (PSM-GM)

Authorization Object	Name
F_FIGM_BUD	Grants Management: Authority for Budget
F_FIGM_CLS	Grants Management: Authority for Class
F_FIGM_GNG	GM: Grant Groups
F_FIGM_GNT	Grants Management: Authority for Grant
F_FIGM_PRG	Grants Management: Authority for Programs
F_FIGM_SCG	GM: Sponsored Class Groups
F_FIGM_SPG	GM: Sponsored Program Groups

The master data objects and business processes of Grants Management are protected by standard authorization objects.

US Federal Government uses the authorization concepts of the components that it deploys, such as Funds Management and Material Management. See also the documentation for Funds Management on https://help.sap.com/s4hana_op_2020 under **Product Assistance > Enterprise Business Applications > Finance > Public Sector Management > Funds Management > Authorizations**.

You can use the following BAdI to implement enhancements to the authorization concept:

BAdI	Name
GM_AUTHORITY_CHECK	Grants Management: Authorization Check
GM_BILL_AUTHORITY	GM: User Authorization for DP90 in GM
GM_POST_AUTHORITY	Grants Management Coding Block Authority Check

13.13.5.3.1.3 Network and Communication Security

Public Sector Management communicates with:

- *Human Capital Management* (HCM) as part of the scenario *Position Budgeting and Control*
- *Customer Relationship Management* (CRM) as part of the scenario *Grantor Management*

The communication with these internal SAP components takes place per *Remote Function Call* (RFC). See the corresponding sections in the *RFC/ICF Security Guide*.

The US *Federal Government* has both payment and collection outbound interfaces at its disposal for *Treasury Confirmation* and *Intragovernment Payment and Collections* (IPAC). This outbound interface uses payment methods and flat files.

The inbound interface of the *Central Contractor Registration* (CCR) uses **IDocs**.

For registering portal users in the backend system, we recommend that the user is assigned in both the portal and the backend system. In other words, the user ID of a user in the portal and the backend system should match.

13.13.5.3.1.4 More Security Information

Authorization checks only take place in *Public Sector Management* and *Funds Management* when the authorization group of a master data object is entered. To ensure that an adequate check is carried out, SAP recommends that you define the affected fields as required entry fields in the field status control. You define this setting in Customizing for *Public Sector Management*:

- ▶ *Funds Management-Specific Postings* ▶ *Earmarked Funds and Funds Transfers* ▶ *Field Control for Earmarked Funds and Funds Transfers* ▶ *Define Field Status Variant* ▶ *Assign Field Status Variant to Company Code / Define Field Status Groups*
- ▶ *Actual and Commitment Update/Integration* ▶ *Integration* ▶ *Maintain Field Status for Assigning FM Account Assignments* ▶

For more information, see the documentation on *Funds Management* on *SAP Help Portal* at ▶ help.sap.com ▶ *ERP Central Component* ▶ *Accounting* ▶ *Public Sector Management* ▶.

For Grants Management, note the following system settings in Customizing for *Public Sector Management* under ▶ *Funds Management Government* ▶ *Master Data* ▶ *Grant* ▶:

- *GM Grant Control:Field Group for Authorizations*
- *Maintain Grant Authorization Types*
- *Maintain Grant Authorization Groups*

13.13.5.3.2 Public Sector Collection and Disbursement

The following security chapter of SAP Public Sector Collection and Disbursement (PSCD) also applies security information for SAP Tax and Revenue Management (TRM).

13.13.5.3.2.1 Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

The Industry Solution Migration Workbench (ISMW) saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

Logical File Names / Path Names Used

The Migration Workbench uses the logical file name `ISMW_FILE` with the logical file path `ISMW_ROOT` to enable the validation of physical file names.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see about data storage security, see the respective chapter in the ABAP Platform Security Guide.

13.13.5.3.2.2 Authorizations

SAP Public Sector Collection and Disbursement (SAP PSCD) and SAP Tax and Revenue Management (SAP TRM) uses the authorization concept provided by the AS ABAP or AS Java. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP and SAP NetWeaver AS Security Guide Java also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PFCG`) on the AS ABAP and the User Management Engine's user administration console on the AS Java.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_FMCA_CA_ALL	Sample role including all transactions for SAP PSCD
SAP_FMCA_CA_ALL_EHP5_TRM_NWBC	Sample role for the SAP NetWeaver Business Client (NWBC) for SAP TRM

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for SAP PSCD.

Authorization Object	Field	Value	Description
F_PSDO_BEG	BEGRU	01 Document Generation 02 Document Changes 03 Document Display 85 Reversal of Documents and Resetting of a Clearing	PSCD Document: Authorization Group for Contract Object
F_PSDO_VGT	PSOBTYP_PS	01 Document Generation 02 Document Changes 03 Document Display 85 Reversal of Documents and Resetting of a Clearing	PSCD Document: Contract Object Type Authorization
F_PSOB_ATT	AUTHYP_PS	01 Create 02 Change 03 Display * All Activities	PSCD Contract Object: Authorization Types
F_PSOB_BEG	BEGRU	01 Create or Generate 02 Change 03 Display 06 Delete 08 Display Change Documents	PSCD Contract Object: Authorization Group

Authorization Object	Field	Value	Description
F_PSOB_FDG	FLDGR_PS	01 Create or Generate 02 Change 03 Display	PSCD Contract Object: Field Groups
F_PSOB_VGT	PSOBTYP_PS	01 Create or Generate 02 Change 03 Display 06 Delete 08 Display Change Documents 64 Generate	PSCD Contract Object: Object Type Authorization
F_FMCA_WOF	ABGRD	10 Post B5 Display History F1 Approve	PSCD Write Off: Approval for Write-Off Reason
F_FMCA_WOM	ACTVT	For more information, see transaction SU21.	PSCD Write-Off: Authorization for Mass Approval
F_PSFA_SET	F_PSFA_SET	01 Create or Generate 02 Change 03 Display 06 Delete	PSCD Facts: Authorization for Fact Sets
F_PSFA_TYP	F_PSFA_TYP	01 Create or Generate 02 Change 03 Display 06 Delete	PSCD Facts: Authorization for Fact Set Parts
F_PSFA_CAT	BEGRU	01 Create or Generate 02 Change 03 Display 06 Delete	PSCD Facts: Authorization for Fact Type Parts
F_FMCA_IPM	F_FMCA_IPM	F1 Approve	PSCD Installment Plan: Authorization for Mass Approval

Authorization Object	Field	Value	Description
F_KKCOL	ACTVT	01 Create or Generate	PSCD Co-Liability: Authorization for Co-Liabilities
		02 Change	
		03 Display	
		06 Delete	
		16 Execute	
		39 Check	
		AF Prompts	

The following authorization objects are only relevant for customers who use SAP Tax and Revenue Management (TRM) for Public Sector that is based on SAP Public Sector Collection and Disbursement (PSCD).

Authorization Object	Field	Value	Description
F_PSFH_FVW	FMCA_PHASE	01 Create or Generate	TRM Object: Authorization for Form Handling and Form View
		02 Change	
		03 Display	
		06 Delete	
		F1 Approve	
F_PSFH_REV	FMCA_ABTP	01 Create or Generate	TRM Object: Authorization for Form Handling and Revenue Type
		02 Change	
		03 Display	
		06 Delete	
		F1 Approve	
F_PSFH_ACT	ACTVT	01 Create	TRM Object: Authorization for Form Handling
		02 Change	
		03 Read	
F_PSFH_FBT	FBTYP	01 Create or Generate	TRM Object: Authorization for Form Handling and Form Bundle Type
		02 Change	
		03 Display	
		06 Delete	
		F1 Approve	

Authorization Object	Field	Value	Description
F_PSFH_STA	FMCA_FBSTA	01 Create or Generate	TRM Object: Authorization for From Handling and Status
		02 Change	
		03 Display	
		06 Delete	
		F1 Approve	
F_PSFH_AMD	AMD_ACTION	16 Execute	TRM Object: Authorization for Amendment Actions in the Tax Officer Work Center
F_FMCA_RLT	COREL_TYPE	01 Create or Generate	TRM Object: Authorization for Master Data Relationship Category
		02 Change	
		03 Display	
		06 Delete	

13.13.5.3.2.3 Read Access Logging Configurations in TRM Form Bundle KPI Apps

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions.

SAP delivers template configurations for applications.

When using the *Form Bundle KPI* apps, it is possible to log data to describe who had read access, and when that happened.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

Channel	Configuration Description	Fields Logged	Business Context
SAP Gateway (oData/UI5/Fiori)	Sample Configuration for Read Access Logging in TRM Form Bundle KPIs	Form Bundle Number (:EntityType:C_PubSec FormBundleKPIType:PUBL ICSECTORFORMBUNDLE) Taxpayer Business Partner Number (:EntityType:C_PubSec FormBundleKPIType:TAXP AYER) Joint Taxpayer Business Partner Number (:EntityType:C_PubSec FormBundleKPIType:JOIN TTAXPAYER) Business Partner Identifica- tion Number of a Taxpayer (:EntityType:C_PubSec FormBundleKPIType:TAXP AYERIDENTIFICATION) Taxpayer Business Partner Identification Type (:EntityType:C_PubSec FormBundleKPIType:TAXP AYERIDENTIFICATIONTYPE) Business Partner Identifica- tion Number of a Joint Tax- payer (:EntityType:C_PubSec FormBundleKPIType:JOIN TTAXPAYERIDENTIFICATIO N) Joint Taxpayer Business Partner Identification Type (:EntityType:C_PubSec FormBundleKPIType:JOIN TTAXPAYERIDNTYPE)	When accessing <i>Business Partner Identification Number of a Taxpayer</i> , or <i>Business Partner Identification Number of a Joint Taxpayer</i>

13.13.5.3.2.4 Read Access Logging Configurations in the App TRM Form Bundle

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions.

SAP delivers template configurations for applications.

When using the app *Form Bundle*, it is possible to log data to describe who had read access, and when that happened.

In the following configurations, fields are logged in combination with additional fields, in the following business contexts:

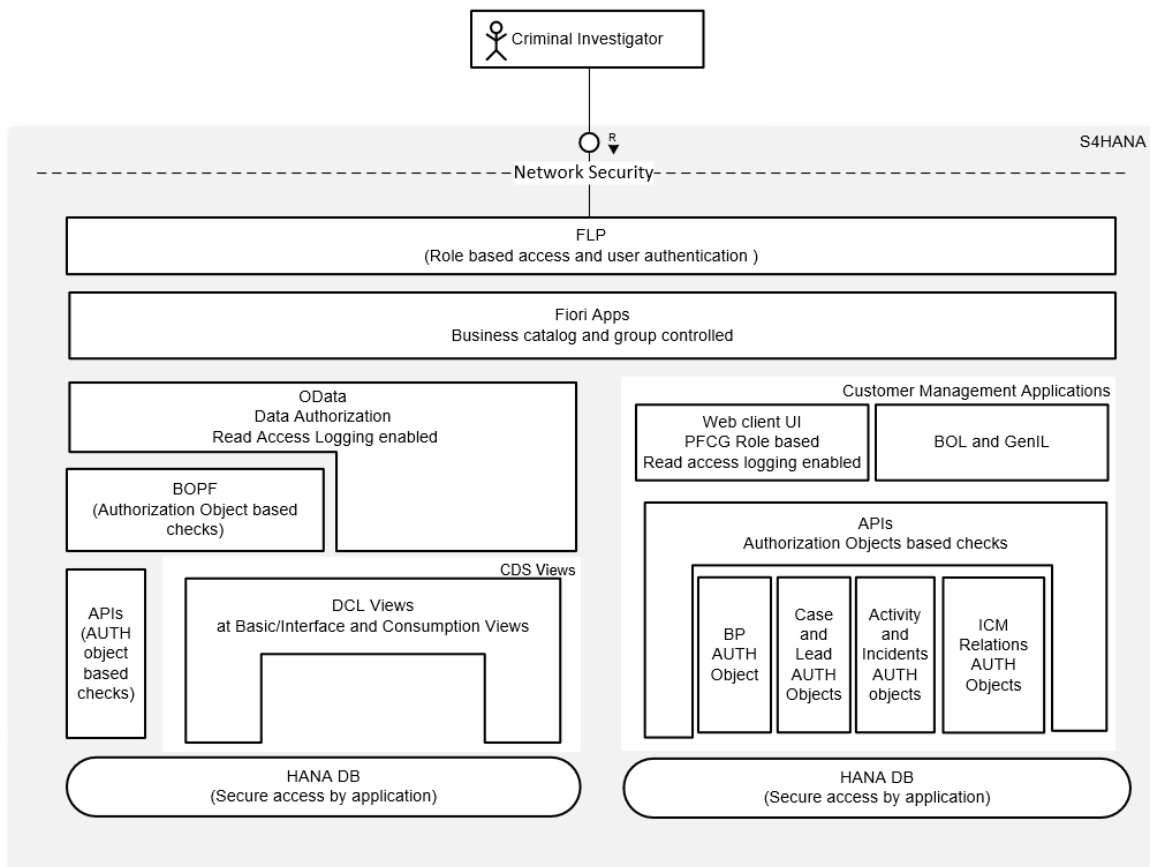
Channel	Configuration Description	Fields Logged	Business Context
SAP Gateway (oData/UI5/Fiori)	Sample Configuration for Read Access Logging in TRM Form Bundle App	<p>Form Bundle Number (:EntityTypes:C_PublicSectorFormBundleTPType:PUBLICSECTORFORMBUNDLE)</p> <p>Technical Identification of the Form Bundle (:EntityTypes:C_PubSecTaxpayerQuickViewType:PUBLICSECTORFORMBUNDLEUUID)</p> <p>Taxpayer Business Partner Number (:EntityTypes:C_PubSecTaxpayerQuickViewType:BUSINESSPARTNER)</p> <p>Taxpayer Business Partner Number (:EntityTypes:C_PublicSectorFormBundleTPType:TAXPAYER)</p> <p>Joint Taxpayer Business Partner Number (:EntityTypes:C_PublicSectorFormBundleTPType:JOINTTAXPAYER)</p> <p>Business Partner Identification Number of a Taxpayer (:EntityTypes:C_PubSecTaxpayerQuickViewType:TAXPAYERIDENTIFICATION)</p> <p>Taxpayer Business Partner Identification Type (:EntityTypes:C_PubSecTaxpayerQuickViewType:TAXPAYERIDENTIFICATIONTYPE)</p> <p>Business Partner Identification Number of a Taxpayer</p>	When accessing <i>Business Partner Identification Number of a Taxpayer</i> , or <i>Business Partner Identification Number of a Joint Taxpayer</i>

Channel	Configuration Description	Fields Logged	Business Context
		(:EntityTypes:C_Public SectorFormBundleTPType :TAXPAYERIDENTIFICATIO N)	
		Taxpayer Business Partner Identification Type (:EntityTypes:C_Public SectorFormBundleTPType :TAXPAYERIDENTIFICATIO NTYPE)	
		Business Partner Identifica- tion Number of a Joint Tax- payer (:EntityTypes:C_Public SectorFormBundleTPType :JOINTTAXPAYERIDENTIFI CATION)	
		Joint Taxpayer Business Partner Identification Type (:EntityTypes:C_Public SectorFormBundleTPType :JOINTTAXPAYERIDNTYPE)	

13.13.5.3.3 Investigative Case Management

The technical system landscape of the SAP Investigative Case Management for SAP S/4HANA is based on the technical system landscape of SAP S/4HANA Service. For more information, see [Service \[page 593\]](#).

Investigative Case Management (ICM) delivers all the functionalities as apps in a SAP Fiori Launchpad. This harmonized approach includes Fiori-based applications (location and object) and Web-client UI-based harmonized applications. As a result, application access goes through different technology security layers and is subjected to numerous authorization checks. The following figure provides an overview of the high level different security checkpoints.



ICM provides CDS based enterprise search models which enables business users to search across different entities.

User Administration and Authentication

Investigative Case Management uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, the SAP NetWeaver Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the [SAP NetWeaver Application Server ABAP Security Guide](#) also apply to the Investigative Case Management application.

In the ICM area, SAP delivers the business role Criminal Investigator. It is designed to be used as a template for defining customer-specific roles. The role supplied already contains numerous functions that you can use to access data and information that you require for your daily work. However, other settings are also required for the UI framework and for authorizations. For more information, search for [User Interface and Roles](#) in Service solution.

User Management Tools

The tools for user and role administration with SAP NetWeaver AS ABAP are the transaction SU01 for User Maintenance transaction and the transaction PFCG for profile generation.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at [ABAP Platform and SAP NetWeaver](#).

Select the release that is relevant for you and then go to [▶ Application Help ▶ Function-Oriented View ▶ Security ▶ Identity Management ▶ User and Role Administration of Application Server ABAP ▶ Administration of Users and Roles ▶](#)

User Types

For Investigative Case Management, it is necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively change their passwords on a regular basis, but users who process background jobs do not.

For Investigative Case Management, there are the following types of users:

- Users with the standard [Criminal Investigation](#) role
These users are subject to the authorization objects outlined in the [Authorizations](#) section below. The authorization model requires that these users be directly associated with the [Criminal Investigation](#) PFCG role both in SAP Fiori frontend and backend systems (using the direct authorization role assignment `SU01` or `PFCG` transactions in backend and business role assignment app in the SAP Fiori frontend system).
- Users with an administrative role
These users are granted universal rights over objects governed by the rules and rights outlined in the [Authorizations](#) section below.

For more information about these user types, see the [User Types](#) section in the [SAP NetWeaver AS ABAP Security Guide](#).

Authorizations

Investigative Case Management uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the [SAP NetWeaver AS Security Guide ABAP](#) also apply to Investigative Case Management.

For more information, see [AS ABAP Authorization Concept](#) in SAP Library for SAP NetWeaver on SAP Help Portal at [ABAP Platform and SAP NetWeaver](#) under [▶ <Choose relevant release> ▶ Security ▶ SAP NetWeaver Security Guide ▶ Security Guides for SAP NetWeaver Functional Units ▶ Security Guides for the Application Server ▶ Security Guides for AS ABAP ▶ SAP NetWeaver Application Server for ABAP Security Guide ▶](#)

Business Function

The following ICM business functions are delivered in *Always ON* state and no further adjustments are needed to activate any features. All the related switches are also available in *Always ON* state.

- CRM_IPS_ICM_3
- CRM_IPS_ICM_1
- CRM_IPS_ICM_4_01
- CRM_IPS_ICM_4_04

Authorization Rules

Investigative Case Management includes the following authorization business rules out-of-the-box:

- Security level rule
The security level rule is used to provide a broad level of authorization. The rule grants access rights to users who have a security level for a given Investigative Case Management application entity type that is higher than or equal to the security level of a given instance of the entity type. The security level assignment is done using the security level static authorization objects discussed in the Standard Static Authorization section above.
- Hidden Rule
The hidden rule is a composite rule. This rule revokes access rights from users who typically have access using the security level rule unless the user is assigned as staff and unit.

The standard authority checks cover static and dynamic authority checks across both ICM specific and reused business object related checks.

i Note

The hidden flag check is in combination with the security level check. When the hidden flag is set, the security level is ignored.

i Note

The default security level of an entity during its creation is *Non-Classified* and default hidden feature is *Non-Hidden*.

Business Roles

Investigative Case Management (ICM) uses the WebClient UI Framework as embedded in the SAP Fiori Launchpad (FLP) called Integration mode. We recommend checking the default Fiori frontend criminal investigator business role (`SAP_BR_INVESTIGATOR`) delivered and copying it as necessary. This role contains preconfigured SAP Fiori Tile Catalogs and Groups. ICM Web UI applications will be accessible using the apps available in the FLP.

i Note

In the integration mode, ICM applications are embedded in a FLP shell instead of the classical WebClient UI Framework L-shape. Hence, there are no backend WebClient UI business roles or navigation bar profiles delivered or loaded in the FLP.

You need to create a backend PFCG role to control the backend authorizations. A default Fiori Launchpad Catalog (`SAP_CRM_BC_INVESTIGATOR`) is delivered with pre-configured function profiles and target ids. This customization plays a key role in generating backend PFCG role. For more information, see IMG Customizing for Service under [UI Framework](#) > [Technical Role Definition](#) > [Define Fiori Launchpad Catalogs](#).

Even though it is technically possible to work with this default criminal investigator business role, we recommend copying this role to create customer-specific business roles.

The following table shows the standard roles that are used and delivered in Investigative Case Management:

Role	Description
SAP_BR_INVESTIGATOR	This is a default Fiori frontend criminal investigator business role. This role contains preconfigured SAP Fiori Tile Catalogs and Groups. ICM Web UI applications are accessible using the apps available in the FLP.

Standard Authorization Objects

The following table contains all relevant services used in the Investigation Case Management. The authorization to start a service must be inserted in the appropriate PFCG role menu.

Service	Type
/IWPGW/TASKPROCESSING	OData Service
CV_ATTACHMENT_SRV	OData Service
C_ICM_LOCATIONTP_CDS_SRV	OData Service
C_ICM_OBJECTTP_CDS_SRV	OData Service
UIU_COMP_BP_EMPL_MAIN_MainWindow_SEARCH	External Service
UIU_COMP_CRM_CALENDAR_MainWindow_OVERVIEW	External Service
UIU_COMP_ICM_BP_MAIN_ICM_BP_MAIN/ MainWindow_SEARCH	External Service
UIU_COMP_CRM_ICM_CMG_MainWindow_SEARCH_CASE	External Service
UIU_COMP_CRM_ICM_ACT_FR_CRM_ICM_ACT_FR/ MainWindow_SEARCH_EMAIL	External Service
UIU_COMP_CRM_ICM_ACT_FR_CRM_ICM_ACT_FR/ MainWindow_SEARCH_INCIDENT	External Service
UIU_COMP_CRM_ICM_CMG_MainWindow_SEARCH_LEAD	External Service
UIU_COMP_CRM_ICM_ACT_FR_CRM_ICM_ACT_FR/ MainWindow_SEARCH_OPERATION	External Service
UIU_COMP_CRM_ICM_ACT_FR_CRM_ICM_ACT_FR/ MainWindow_SEARCH_OPERATION_TMPL	External Service

Service	Type
UIU_COMP_ICM_BPPROF_ICM_BPPROF/ CategoriesWindow_FROMNAVBAR	External Service
UIU_COMP_ICM_EXTERN_MAIN_ICM_EXTERN_MAIN/ MainWindow_EXTERNAL_SRC	External Service
UIU_COMP_ICM_WLI_ICM_WLI/MainWindow_DEFAULT	External Service
UIU_COMP_MDOMM_ORGDATA_MainWindow_SEARCH	External Service
UIU_COMP_WCF_MIXED_LIST_WCF_MIXED_LIST/ MainWindow_DEFAULT	External Service

ICM Authorization Objects

The table below shows the authorization objects that are especially used by Investigative Case Management.

Values for common field ICM_SECLVL can be customized in the IMG under [Service > Industry-Specific Solutions > Public Sector > Investigative Case Management > General Settings > Authorizations > Define Security Levels](#) (with the domain value ICM).

Values for field ICM_RELTYP are defined in the IMG under [Service > Industry-Specific Solutions > Public Sector > Investigative Case Management > General Settings > Relationships > Define Relationship Types](#)

For technical reasons, every user must have authorization for type s900 and s901.

Authorization	Field	Value	Description
CRM_ICMADM	ACTVT	W1 W2	Each value specifies a particular authorization for an activity. W1 grants the authorization to add and remove partners from the <i>Staff & Units</i> assignment block of the Investigative Case Management case entity. W2 grants the right to toggle the hidden flag for all Investigative Case Management case entities.
CRM_ICMCAS	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for a case type. For example, the

Authorization	Field	Value	Description
	ICM_CASTYP	Available case type for ICM	combination ICM_SECLVL = 50 and ICM_CASTYP = ICMC grants the user or owner of the static authorization object instance access to all cases of the type ICM with a security level of 50.
CRM_ICMLEA	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for a lead type. For example, the combination ICM_SECLVL = 50 and ICM_LEATYP = ICML grants the user or owner of the static authorization object instance access to all leads of type ICML with a security level up to 50.
	ICM_LEATYP	Available lead type for ICM	
CRM_ICMOPE	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for an investigative activity type. For example, the combination ICM_SECLVL = 50 and ICM_OPETYP = OPR grants the user or owner of the static authorization object instance access to all investigative activities of activity category OPR with a security level up to 50.
	ICM_OPETYP	Available activity categories for ICM	
CRM_ICMINC	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for an incident type. For example, the combination ICM_SECLVL = 50 and ICM_INCTYP = INC grants the user or owner of the static authorization object instance access to all incidents of activity category INC with a security level up to 50.
	ICM_INCTYP	Available categories for ICM	

Authorization	Field	Value	Description
CRM_ICMLOC	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for locations/ objects. For example, the combination ICM_SECLVL = 50 grants the user or owner of the static authorization object instance access to all locations/objects with a security level up to 50.
CRM_ICMEMA	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for e-mails. For example, the combination ICM_SECLVL = 50 grants the user or owner of the static authorization object instance access to all e-mails with a security level up to 50.
CRM_ICMREL	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for a relationship type. For example, the combination ICM_SECLVL = 50 and ICM_RELTYP = Z001 grants the user or owner of the static authorization object instance access to all relationships of type z001 with a security level up to 50.
	ICM_RELTYP	Available relationship type for ICM	
CRM_ICMBP	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for business partners. For example, the setting ICM_SECLVL = 50 grants the user or owner of the static authorization object instance access all business partners with a security level up to 50.

Authorization	Field	Value	Description
CRM_ICMBPP	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for business partners. For example, the setting ICM_SECLVL = 50 grants a security level of 50 for business partner profiles.
CRM_ICMRLA	ACTVT	Allowed customized ACTVT entries: 1 Create 2 Change 3 Display W3 Edit Expunge Date	This object is used to determine what activities can be performed on a relationship.
CRM_ICMEXP	ACTVT	Allowed customized ACTVT entries: 01 Create or Generate 02 Change 03 Display 06 Delete	This object is used to provide users access to the expunged data.
ICMS4_OBJ	ACTVT	Allowed customized ACTVT entries: 01 Add or Create 02 Change 03 Display 06 Delete 56 Display archive F4 Display in value help	This object is used to provide access to ICM object.

Authorization	Field	Value	Description
ICMS4_LOC	ACTVT	Allowed customized ACTVT entries: 01 Add or Create 02 Change 03 Display 06 Delete 56 Display archive F4 Display in value help	This object is used to provide access to ICM location.

Data Access Related Authorization Objects

Besides ICM specific authorization objects some data access related authorization objects are required and explicitly checked during operations in ICM. To use the complete functionality of ICM these objects must be considered. The table below lists the important authorization objects of this category.

Authorization	Description
B_BUPA_ADR	Business Partner: BP Addresses
B_BUPA_ADR	Business Partner: Authorization Groups
B_BUPA_GRP	Business Partner: Authorization Groups
B_BUPA_RLT	Business Partner: BP Roles
B_BUPR_BZT	Business Partner Relationships: Relationship Categories
B_CCARD	Payment Cards
B_USERSTAT	Status Management: Set/Delete User Status
CRM_BP_ASS	Authorization for Rule Based Assignment
CRM_BPROLE	Business Partner in Service: BP Roles
CRM_CATEGO	Authorization Object for Coherent Categorization
CRM_CO_SE	Authorization Object CRM Order - Bus. Ob. Service Contract
CRM_ORD_LP	Authorization Object CRM Order - Visibility in Org. Model
CRM_ORD_OP	Authorization Object CRM Order - Own Documents

Authorization	Description
CRM_ORD_PR	Authorization Object CRM Order - Business Transaction Type
CRM_TXT_ID	CRM: Text ID
CRMS4_SLSO	Sales Organizational Units of Service Transactions
F_KNA1_APP	Customer: Application Authorization
F_KNA1_BED	Customer: Account Authorization
F_KNA1_GEN	Customer: Central Data
F_KNA1_GRP	Customer: Account Group Authorization
F_LFA1_APP	Vendor: Application Authorization
F_LFA1_BEK	Vendor: Account Authorization
F_LFA1_BUK	Vendor: Authorization for Company Codes
F_LFA1_GEN	Vendor: Central Data
F_LFA1_GRP	Vendor: Account Group Authorization
I_EQTYP	Equipment Category
M_LFMI_EKO	Purchasing Organization in Supplier Master Record
M_MATE_MAR	Material Master: Material Types
M_MATE_MAT	Material Master: Materials
M_MATE_WGR	Material Master: Material Groups
P_ORGIN	HR: Master Data
P_PERNR	HR: Master Data - Personnel Number Check
PLOG	Personnel Planning
PS_RMPSOEH	RMPS: Access Record, Case, Document Special Org. Units
PS_RMPSORG	RMPS: Access Record, Case, Document Org. Assignment of User
PS_RMPSPGE	RMPS TNA: Enhanced Check on Activities
PS_RMPSPSP	RMPS TNA: Status-Dependent Attribute Check
S_SCMG_CAS	Case Management: Case

Authorization	Description
S_SCMG_FLN	Case Management: Authorization by Field
S_SCMG_STA	Case Management: Status
S_SCMG_TXT	Case Management: Text Notes
S_SERVICE	Check at Start of External Services
S_SRMGS_CT	Records Management: Authorizations for Document Content
S_SRMGS_DC	Records Management: Authorization for Documents
S_SRMGS_PR	Records Management: Authorizations for Attributes
S_SRMGS_VV	Records Management: Authorizations for Versions and Variants
S_SRMRECST	Records Management: Record: Authorizations for Record Strctr
S_SRMSY_CL	SAP Records Management : General Authorization Object
S_SRM_STAT	SRM Status Management: General Authorization Object
S_SRM_ST_P	SRM Status Management: Auth. Object for Status Profile
UIU_COMP	CRM UIU Component
V_KNA1_VKO	Customer: Authorization for Sales Organizations

Other Security-Relevant Information

The standard settings in SAP S/4HANA Service allow users to search for all business partners. To limit your searches to persons and organizations in Investigative Case Management from the standard objects, see [Customizing for Service](#) under [Industry-Specific Solutions](#) > [Public Sector](#) > [Investigative Case Management](#) > [Persons and Organizations](#) > [Exclude ICM Persons and Organizations from Account and Contact Search](#).

Data Protection and Privacy

ICM provides specific features and functions to support compliance with the relevant legal requirements and data protection and privacy.

Logging and Monitoring

ICM is mainly used by law-enforcement authorities, therefore logging and monitoring access to sensitive data is required by law in order to fulfil legal compliance. Following are the tools you can consider for fulfilling the logging and monitoring requirements:

- **Read Access Logging**

SAP delivers sample configurations for applications for ICM through SAP Note 2739669.

[Investigative Case Management](#) logs data of ICM person including the person search and results. It also logs data of ICM person that are displayed on the case, lead, activity, incident, object and locations overview pages.

For more information about RAL, see the Product Assistance for SAP S/4HANA on SAP Help Portal at [SAP S/4HANA](#) under [Product Assistance](#) > [Industries](#) > [Public Services](#) > [Public Sector](#) > [Investigative Case Management](#) > [Authorization and Security in ICM](#) > [Data Protection](#) > [Read Access Logging in ICM](#) .

You can access the list of logged fields in the following delivered default configurations:

Configuration	Channel	Business Context
SAP_ICM_PERSON_DETAILS	Web UI	Data access log for the ICM person in Web UI
C_ICM_LOCATIONTP_CDS_SRV	SAP gateway	Data access log for person details in the ICM location entity
C_ICM_OBJECTTP_CDS_SRV	SAP gateway	Data access log for person details in the ICM object entity

- **Work load analysis for ICM**

SAP workload analysis (transaction STAD) plays a vital role during security audits. Auditors often use this transaction to intersect any possible unauthorized system access.

ICM provides a refined flavor of transaction STAD in a wrapper transaction called STAD_ICM. This aims at assisting auditors to provide flexible selection screens. Filter parameters like [User](#), [Transaction](#) and [Report](#) support multiple value filters compared to its predecessor transaction. A default variant DEFAULT_ICM demonstrates auditors to arrive at a positive list of un-authorized access in an ICM system context to readily act upon.

- **ICM Critical Authorizations for User Information System**

SAP User Information System (transaction SUIM) summarizes many different SAP authorization aspects in one place.

For more information, see [User Information System](#) on SAP Help Portal at [User and Role Administration of Application Server ABAP](#) .

User Information System analysis for ICM

To detect critical authorizations assigned to a user via a PFCG role, a variant in the SAP User Information System (transaction SUIM) is created. The variant of the SUIM report "Users or Roles with Combinations of Critical Authorizations" (RSUSR008_009_NEW) contains critical authorization objects which should not be accessible for users in the ICM. Therefore, the SUIM variant allows to scan PFCG roles for the corresponding authorization objects.

As the SUIM variant is based on the SAP standard authorization objects, it must be used as a reference and adjusted for customer specific objects.

Following are the steps to access the SUIM variant in the ABAP system:

1. Use transaction SUIM and execute the following path:

▶ [User Information System](#) ▶ [User](#) ▶ [With Critical Authorizations](#) ▶

2. On the selection screen; choose the option *For Critical Authorizations*, select the variant *SAPICM* and execute again.

For more information on how to use and how to create or adapt SUIM variants for “Users or Roles with Combinations of Critical Authorizations”, see the program documentation (SHIFT F1) which you can find after starting the SUIM function.

- **Auditing in SAP HANA systems**

Auditing at HANA provides you with visibility on who did what in the database (or tried to do what) and when. This allows you, for example, to log and monitor read access to sensitive data.

For more information, see [Auditing Activity in SAP HANA Systems](#) in Security Guide for SAP HANA Platform on SAP Help Portal at [SAP HANA Platform](#).

Information Retrieval

ICM supports information retrieval using SAP NetWeaver component Information Retrieval Framework (IRF). For more technical details, refer to SAP note 2815160.

The following IRF models allow retrieval of ICM entity data with reference to an ICM person.

i Note

The IRF entry point for each of the delivered models is an ICM person ID (business partner ID).

Model Name	ICM Entity Name
CA_BUPA	ICM Person and ICM Relationships
CRMS4_ICML/CRMS4_ICMB	ICM Location/Object and ICM Relationships
CRM_ACT_ON	ICM Activity/Incident and ICM Relationships
SCMG	ICM Case/Lead and ICM Relationships

i Note

Attachments or URLs of the attachments are not part of the above IRF models. Only the metadata of the attachments are available. Administrators can download the attachments by navigating to the corresponding overview pages. The navigation path to download the attachments is as follows:

▶ [Open the app \(Manage Persons and Organizations app for Person entity, Manage Cases app for case entity and so on\)](#) ▶ [Go to the overview page](#) ▶ [Go to Attachments assignment block](#) ▶ [Select the attachments to download](#) ▶ [Choose Download](#) ▶

For more information about system configuration, see [Setting Up the System for the IRF](#) on SAP Help Portal at [Information Retrieval Framework \(IRF\)](#).

i Note

Relationship data between a person and any other entity is read with the precondition that the ICM entity person is a source, in the entity links between relationship types. You must ensure this while setting up entity links for any custom relationship types in the Customizing for Service under [Industry-Specific Solutions Investigative Case Management](#).

For more information about information retrieval, see the product assistance for SAP S/4HANA on SAP Help Portal under ► [Product Assistance](#) ► [Industries](#) ► [Public Services](#) ► [Public Sector](#) ► [Investigative Case Management](#) ► [Authorization and Security in ICM](#) ► [Data Protection](#) ► [Information Retrieval](#) ►.

Archiving, Blocking and Deletion

ICM supports Information Life Cycle (ILM) based archiving, blocking and deletion features for all its entities including relationship data. Additionally, ICM provides specialized features called anonymizing person data and expunging of the relationships to control the lifecycle of data.

i Note

Expunging functionality also deletes person data for outdated expunged relationships.

ICM-related EoP (End of Purpose) checks are made during the BP blocking process. A new application name ICM along with a standard function module CRMS4_ICM_BP_BLOCKING has been registered to perform the check. This prevents ICM data from being accidentally blocked or deleted.

i Note

During blocking (Transaction BUPA_PRE_EOP), the *Check all applications for EoP* parameter must be marked X to enable invoking of the above check.

For more information about archiving ICM entities, blocking and deletion, see the product assistance for SAP S/4HANA on SAP Help Portal under ► [Product Assistance](#) ► [Industries](#) ► [Public Services](#) ► [Public Sector](#) ► [Investigative Case Management](#) ► [Authorization and Security in ICM](#) ► [Data Protection](#) ►.

Archiving of Attachments:

ICM supports Information Life Cycle (ILM) based archiving of documents (DMS based) which are attached to all ICM entities.

The archiving process of SAP Document Management System (DMS) uses the concept of rule inheritance in ILM. The highest retention period of the business object (ICM entity) linked are inherited to the DMS based document. Once the archiving of ICM entity is executed, it also sets the deletion flag for the DMS based documents linked.

13.13.5.3.4 Multichannel Foundation for Utilities and Public Sector (Public Sector)

13.13.5.3.4.1 Internet Communication Framework Security (ICF)

You should only activate the services that are required by the applications running in your system.

The following services must be activated for Multichannel Foundation for Utilities and Public Sector:

- ERP_FMCA_MC (logon user/current user)
- ERP_FMCA_MC_PUBLIC_SRV

ERP_FMCA_MC_PUBLIC_SRV is to be used for the anonymous payment or anonymous form submission scenario and needs to be linked to a predefined "SU01" user.

Use transaction **SICF** to activate these services. If your firewalls use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information about ICF security, see the relevant chapter in the ABAP Platform Security Guide.

13.13.6 Services

13.13.6.1 Engineering, Construction, and Operations

13.13.6.1.1 Equipment and Tools Management

13.13.6.1.1.1 Authorizations

Equipment and Tools Management (ETM) uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

i Note

For more information about how to create roles, see the ABAP Platform Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used:

Authorization Object	Description
J_3GBLART	Authorizations for document types

Authorization Object	Description
J_3GEQART2	CEM – Equipment Types for Document Category 2
J_3GEMPGR2	CEM - Recipient Groups, Document Category 2
J_3GBEWTP2	CEM – Transaction Types, Document Category 2
J_3GACTVT	CEM Allowed Activities
J_3GABRLST	Call CEM Settlement List for Organizational Units
J_3GDISPGR	MRP Group in Equipment
J_3GDDBER	Planning Area in Recipient
J_3G_TCODE	Transaction Code

13.13.6.1.1.2 Deletion of Personal Data

Use

Equipment and Tools Management (ETM) might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 ► *Product Assistance* ► *Cross Components* ► *Data Protection* ►.

Relevant Application Objects and Available Deletion Functionality

Application	Provided Deletion Functionality
Equipment and Tools Management (IS-ADEC-ETM)	Archiving Object /SAPCEM01 /SAPCEM02 /SAPCEM03 /SAPCEM04 /SAPCEM05 /SAPCEM06 /SAPCEM07 ILM Object SAPCEM_01 SAPCEM_02 SAPCEM_07 Reports /SAPCEM/ILM_DELETION_REP_01

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Equipment and Tools Management (IS-ADEC-ETM)	EoP	Checks tables /SAPCEM/BDPO, J_3GBELP

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for [Cross-Application Components→Data Protection](#).

13.13.6.2 Professional Services

13.13.6.3 Commercial Project Inception and Lean Staffing

The following guide covers the information that you require to operate Commercial Project Inception and Lean Staffing securely.

13.13.6.3.1 Introduction

Introduction

i Note

This guide does not replace the administration or operation guides that are available for productive operations.

Target Audience

- Technology consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply likewise to Commercial Project Inception and Lean Staffing. To assist you in securing Commercial Project Inception and Lean Staffing, we provide this Security Guide.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to Commercial Project Inception and Lean Staffing .

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**
This section references to other Security Guides that build the foundation for this Security Guide.
- **Authorizations**
This section provides an overview of the authorization concept that applies to Commercial Project Inception and Lean Staffing .

13.13.6.3.2 Before You Start

It is important that you read and understand the information contained in the [Authorizations \[page 931\]](#) section that is specific to Commercial Project Inception and Lean Staffing. In addition, you should be aware of the information listed in the table below:

Fundamental Security Guides

Scenario, Application or Component Security Guide	Most-Relevant Sections or Specific Restrictions
SAP Netweaver Application Server	ABAP Platform Security Guide - All sections
SAP ECC	SAP ERP Central Component Security Guide - All sections

13.13.6.3.3 User Management and Authentication

[SAP ECC Industry Extension Professional Services](#) uses the user management and authentication mechanisms provided with ABAP Platform, particularly the [Application Server ABAP](#). Consequently, the security recommendations and guidelines for user management and authentication that are described in the [Application Server ABAP Security Guide](#) also apply to [SAP ECC Industry Extension Professional Services](#).

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

User type required for [SAP ECC Industry Extension Professional Services](#) is Dialog user. Dialog users are Individual users used for SAP GUI for Windows.

13.13.6.3.4 Authorizations

Use

The business function *Commercial Project Inception and Lean Staffing* uses the authorization concept provided by the AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to *Commercial Project Inception and Lean Staffing*.

The ABAP Platform authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.

Standard Roles

The table below shows the standard roles that are used by *Commercial Project Inception and Lean Staffing*.

Standard Roles

Role	Description
SAP_SAWE_UNIVERSAL	Maintenance of staff assignments and forecasts
SAP_CATS_LEAN_STAFFING	Maintenance of cross-application time sheet (Web Dynpro application)
SAP_BC_EMPLOYEE	Access to HCM data (for employee search, for example)
SAP_BPR_INT_SALES_REP_14	Maintenance of assignment objects of type "SD order"
SAP_PS_STRUCT	Maintenance of assignment objects of type "project"
SAP_BC_ENDUSER	Non-critical basis authorizations for all users

In addition, users must be assigned to:

- the authorization profile K_ORDER for the maintenance of assignment objects of the type "internal order"
- the authorization profile I_PM_ALL for the maintenance of assignment objects of the type "service order".

i Note

As the authorization profiles K_ORDER and I_PM_ALL comprise all available authorizations for internal orders and service orders respectively, we recommend that you narrow the granted authorization range to suit your specific requirements.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by *Commercial Project Inception and Lean Staffing*.

Standard Authorization Objects

Authorization Object	Field	Value	Description
P_ORGIN and P_PERNR (Authorization check for HR info-types)	INFTY	0002	The employee search in the Lean Staffing application and in the Lean Staffing reporting lists only employees for whose info type 0002 the user has a read authorization.
	SUBTY	<blank>	
	AUTHC	R	
PRS_LS_CUS (new)	ACTVT	02, 03, 06	The system checks this authorization object when staff assignments to customers are made.
V_PRS_LS_H (new)	VKORG	VBAK-VKORG	The system checks this authorization object when staff assignments to SD orders are made. The user must be authorized for the sales area, distribution channel, division, customer group and cost center of the SD order.
	VTWEG	VBAK-VTWEG	
	SPART	VBAK-SPART	
	KDGRP	KNVV-KDGRP	
	KOSTL	VBAK-KOSTL	
	ACTVT	02, 03, 06	
V_PRS_LS_I (new)	PRCTR	VBAP-PRCTR	The system checks this authorization object when staff assignments to SD orders are made. The user must be authorized for the profit center of the SD sales document item.
	ACTVT	02, 03, 06	
C_PRPS_LS (new)	PS_FKOKR	PRPS-FKOKR	The system checks this authorization object when staff assignments to WBS elements are made. The user must be authorized for the controlling area, cost center and profit center of the WBS element.
	PS_FKSTL	PRPS-FKSTL	
	PRCTR	PRPS-PRCTR	
	ACTVT	02, 03, 06	
K_PRS_LS	PRCTR	AUFK-PRCTR	The system checks this authorization object when staff assignments to internal or service orders are made. The user must be authorized for the profit center of the order.
	ACTVT	02, 03, 06	

Authorization Object	Field	Value	Description
PRS_LS_FC	EMP_LEVEL	Level 1, 2 or 3	See description below.
	ACTVT	02, 03, 06	

The authorization for staff assignments is based on the assignment object to which it refers; it is independent of the employee for whom the assignment is made. As shown in the table above, different types of assignment objects (SD order, project and so on) use different fields for this authorization.

The authorization for forecasting is based on the employee whose time is forecast; it is independent of the assignment object for which it is made. There are several levels (EMP_LEVEL) of authorization concerning the employee:

- Level 1: The user is authorized to change and display own forecasts (the forecasts for the employee ID contained in the user's master record).
- Level 2: The user is authorized to change and display forecasts for the members of his or her team (note that level 2 does not necessarily imply level 1). The team is determined on the basis of the employee ID contained in the user's master record, as follows:
 - The HCM organizational model is queried (current relationships according to info type 1001, subtype A008; for details, see method CL_SAWE_API_PROVIDER_FC-> GET_TEAM_OF_EMP). The result of this query is the same for managers and their assistants.
 - You can influence the list of employee IDs returned by this query by adding or removing entries in an implementation of the Business Add-In (BAdI) SAWE_AUTHORITY_CHECK, method TEAM_OF_EMPLOYEE.
 - If neither the HCM organizational model nor the BAdI implementation is used, the team does not contain any employees.
- Level 3: The user is authorized to change and display forecasts for all employees.

The system checks both authorizations (authorization for staff assignments and authorization for forecasting) in the following cases:

- ACTVT = '02' (change): Checked when the Lean Staffing or Forecasting application is executed in the *change mode* (this refers to the UI-based application and to the A2X Enterprise Services).
- ACTVT = '03' (display): Checked when the Lean Staffing or Forecasting application is executed in the *display-only mode*.
- ACTVT = '06' (delete): Checked when the deletion of an assignment object triggers the deletion of its staff assignments and forecasts (without further user interaction).

This is different from the deletion of individual entries in the Lean Staffing and Forecasting applications, because users who are authorized to delete assignment objects (for example, SD order items) may need this authorization, even if they do not have authorization to execute the Lean Staffing or Forecasting application.

The authorizations for reporting are based on the specific user group 'SAWE', which you can maintain using transaction SQ03. Users who are authorized to analyze employee assignments, resource consumption, employee utilization and skill utilization need to be assigned to this user group.

13.13.6.3.5 Data Storage Security

Use

Commercial Project Inception and Lean Staffing stores additional employee-related data besides data stored in the HR Master Data database.

The following additional data can be stored in the respective objects (technical table names in parentheses):

- Employee assignment to projects, customer orders, or internal orders (SAWE_D_SA_HDR and SAWE_D_SA_ITM).
- Employee forecast for the above-mentioned assignments, and also for generic assignments such as training (SAWE_D_TIME_PS and SAWE_D_TIME_PSI).

For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under [▶ Product Assistance](#) [▶ Enterprise Business Applications](#) [▶ Industries](#) [▶ SAP for Professional Services](#) [▶ Lean Staffing](#) [▶ Data Archiving in Lean Staffing](#) [▶](#)

13.13.6.3.6 Deletion of Personal Data

Use

The *Lean Staffing (IS-PRS-LS)* component might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use *SAP Information Lifecycle Management (ILM)* to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 [▶ Product Assistance](#) [▶ Cross Components](#) [▶ Data Protection](#) [▶](#).

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Lean Staffing (IS-PRS-LS)	For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under ▶ Product Assistance ▶ Enterprise Business Applications ▶ Industries ▶ SAP for Professional Services ▶ Lean Staffing ▶ Data Archiving in Lean Staffing ▶	Archiving object SAWE_SA ILM object SAWE_SA Report SAWE_SA_CLEAN_CANDIDATE_LIST

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Lean Staffing (IS-PRS-LS)	End of Purpose (EoP) check	Class registered for the EoP check: CL_WUC_IS_PRS_LS_EOP_CHECK For more information, see SAP note 2390575 .

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of customer and vendor master data in Customizing for *Logistics - General* under **Business Partner** > *Deletion of Customer and Vendor Master Data*.

13.14 Country-Specifics

13.14.1 Deletion of Personal Data in Business Applications

The country-specific applications in the components of the listed business applications might process data (personal data) that is subject to the data protection laws applicable in specific countries. You can use *SAP Information Lifecycle Management* (ILM) to control the blocking and deletion of personal data. For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under **Product Assistance** > *Cross Components* > *Data Protection*.

For information about the available application objects and deletion functionality, see the country-specific function descriptions in the product assistance for SAP S/4HANA on the SAP Help Portal at https://help.sap.com/s4hana_op_2020 under *Product Assistance* by navigating to the specific function you are interested in.

13.14.2 Read Access Logging for Electronic Documents

The Document Compliance Framework provides a RAL (Read Access Logging) channel for Electronic Documents.

The *Electronic Document* channel allows logging to the RAL Manager (transaction SRALMANAGER) in the following cases:

- Preview of eDocuments
- View or export of eDocument files

i Note

- OData API is covered by the existing SAP Gateway (OData) RAL OData channel.
- Submission of eDocuments is out of scope for RAL logging.

The *Electronic Document* channel is identified with the following values:

Values for Electronic Document channel

Field Name	Description
EDOC_TYPE	eDocument Type
FILE_TYPE	eDocument: File Type for Read Access Logging
INTERFACE_STRUCTURE	eDocument: File Structure for Read Access Logging

SAP provides the *Electronic Document* RAL channel as well as the connection to the RAL Manager. The call of the RAL logging is done from the Document Compliance Framework. When creating a RAL configuration, the following list of fields is displayed for the *Electronic Document* channel entity:

- Administrative eDocument data (for example, eDocument type or eDocument process)
- Administrative eDocument file data (for example, eDocument file type or eDocument file name)
- eDocument type-specific fields (for example, for Portugal Invoice: Request ID)
- eDocument file content data:
 - If the file structure is filled, then all the fields from the file structure are available for logging.
 - If no file structure is defined, then all the data of the file can be logged without its structure (for example, a PDF file). The Electronic Document channel provides three fields for domain assignment.

When you access the RAL Manager with the *Electronic Document* channel, the system displays, for a given eDocument type, the file types for which RAL is enabled. You can then select the fields that may include sensitive personal data and for which you want to monitor and log read access.

Related Information

[Read Access Logging \[page 33\]](#)

13.14.3 Specific Read Access Log Configurations

Use

In Read Access Logging (RAL), you can configure which read-access information to log and under which conditions.

SAP delivers sample configurations for applications.

You can find the configurations as described in the [Read Access Logging \[page 33\]](#) chapter.

In the following country-specific configurations, fields are logged in combination with additional fields, in the following business contexts:

China

Channel	Configuration	Fields Logged	Business Context
Web Dynpro	Recording: BOE_BANK_ACCOUNTS _OP	<ul style="list-style-type: none"> • BOE_DRAWER_ACCOUNT • BOE_DRAWEE_ACCOUNT 	Logs read access to the <Drawee Bank Account> and <Drawer Bank Account> fields in bill of exchange documents and reports.
Web Dynpro	Recording: GTI_BANKACCOUNT_W EBDYNPRO	<ul style="list-style-type: none"> • Bank Account • Payer Bank Account Detail • Payer Bank Name 	Logs read access to the fields of Bank Account, Payer Bank Detail and Payer Bank Name for Golden Tax Interface.
Dynpro	Recording: EPIC_ITEM	BANKN	Logs read access to the <Bank Account> field.
SAP Gateway	Service ID: EPIC_BANK_RECONCI LITATION_SRV	<ul style="list-style-type: none"> • BANKN • CREATED_USER 	Logs read access to the <Bank Account> and <Created User> fields.
SAP Gateway	Service ID: EPIC_BANK_RECO_ST ATEMENT_SRV	<ul style="list-style-type: none"> • BANKN • CREATED_USER 	Logs read access to the <Bank Account> and <Created User> fields.

Italy

Channel	Configuration	Fields Logged	Business Context
Dynpro	Recording: BANK_BP_CUPCIG_IT	BANK_CUP_IT-BANKL <i>(Bank Key)</i> BANK_CUP_IT-BANKN <i>(Bank Account)</i>	Logs read access activities for bank key and bank account on business partner, and CUP/CIG bank assignment.

Thailand

Channel	Configuration	Fields Logged	Business Context
Dynpro	BRANCH_CODE_DYNPR O	J_1TPBUPL	Logs read access to the field Branch Code (J_1TPBUPL). Branch code is regarded as sensitive data in customers' master data for Thailand.
Dynpro	TH_VAT_BCODE	\$_LIST_CODE	Logs read access to Thailand branch codes when the VAT report is generated.

14 Business Network Integration

SAP S/4HANA currently supports integration scenarios with the Ariba Network (including Ariba Sourcing via the Ariba Network), and with SAP Fieldglass.

14.1 Security Aspects for Connectivity Types

In all of the connectivity types described below, only the on-premise system opens the connection to the Cloud, thus supporting the highest level of security. A proxy or reverse proxy in the demilitarized zone (DMZ) is not required.

The SAP S/4HANA system communicates with the business networks through the HTTPS protocol, encrypting transmitted data.

Direct Connectivity

For **direct** connectivity, SAP S/4HANA always opens the connection by executing the following actions:

- SAP S/4HANA pushes cXML messages to the business networks (synchronous)
- The Polling Agent in SAP S/4HANA fetches pending messages from the business networks (synchronous)

Mediated Connectivity

For **mediated** connectivity, the SAP S/4HANA system connects through SAP PI. The connection functions as follows:

- SAP S/4HANA pushes cXML messages to SAP PI (asynchronous)
- The *Ariba Network Adapter for SAP NetWeaver* triggers its Polling Agent to fetch pending cXML messages from Ariba Network. The Polling Agent in the PI adapter then pushes the cXML messages to the SAP S/4HANA system (asynchronous).

If SAP S/4HANA communicates with Ariba Network through SAP PI, there are no special security requirements.

i Note

For mediated connectivity, Ariba provides information on how to communicate with Ariba Network in the *Ariba Network Adapter for SAP NetWeaver Setup Guide*. You can contact Ariba for more information.

14.2 Direct Connectivity: SAP S/4HANA as Client

When sending a cXML message to a business network, the sender must authenticate itself:

- SAP Fieldglass supports authentication by client certificate.
- Ariba Network offers authentication with client certificate or with shared secret password. Both authentication methods are also supported by SAP S/4HANA. For more information about the authentication methods on Ariba Network, contact SAP Ariba.

i Note

Communication with the Ariba Network and with SAP Fieldglass is based on HTTPS. For HTTPS SSL encryption, SAP Cryptographic Library is required.

For information about installing the SAP Cryptographic Library, go to https://help.sap.com/s4hana_op_2020, enter *The SAP Cryptographic Library Installation Package* into the search bar, press , and open the search result with that title.

Authentication with Client Certificate (Ariba Network Only)

For authentication with client certificate it is strongly recommended that you use the latest version of the SAP Cryptographic Library (SAPCRYPTOLIB). For more information about latest SAP Cryptographic Library versions, bugs, and fixes see SAP Note [455033](#).

i Note

Only certificates in Personal Security Environment (PSE) format can be imported. Certificates in other formats must first be converted to PSE format. The conversion can be done using the command line tool `SAPGENPSE`. The tool can be installed with SAP Cryptographic Library installation package.

For example, to convert from P12 (Public-Key Cryptography Standards) format to PSE format, enter the following command line:

```
sapgenpse import_p12 -v -r <root certificate> -p <Target PSE file> <Source File>
```

Setting up authentication with client certificate includes the following steps:

1. Get the client certificate from a Certification Authority (CA) that is trusted by Ariba.
2. Import the private key of the certificate into the SAP S/4HANA system by using *Trust Manager* (transaction `STRUST`).
 1. To store the client certificate in SAP S/4HANA, you have to create a new Client Identity in *Trust Manager*. Proceed as follows:
 1. Choose **Environment** > **SSL Client Identities**, enter **ARIBA** as the identity name and **Ariba Network Client** as the description.
 2. Save your entries.
 2. Import the private key of the certificate in Trust Manager. Proceed as follows:
 1. Select the created **ARIBA** SSL Client ID and choose **PSE** > **Import** to import the PSE file.

2. Enter the password for the certificate, if required.
 3. Save your PSE file by choosing ► *PSE* ► *Save as* ► *SSL Client* ►, and enter **ARIBA** as the SSL Client.
 4. Navigate to the *Own Certificate* group box on the *Trust Manager* screen, and double-click the certificate to add it to the certificate list. The certificate is now shown in *Trust Manager* in *Certificate List*.
3. Import the root certificate into the SAP S/4HANA system by using *Trust Manager*. Proceed as follows:
 1. Double-click the SSL Client Identity **ARIBA** that you have created.
 2. Navigate to the *Certificate* group box and choose *Import certificate*. Add the imported certificate to the certificate list by clicking *Add to Certificate List*.
 4. For HTTPS SSL encryption, obtain the server certificate from Ariba. Proceed as follows:
 1. Go to buyer.ariba.com.
 2. Download the certificate using your browser.
For example, if you are using Internet Explorer, choose ► *View* ► *Security Report* ► *View Certificates* ►. On the *Details* tab page, choose *Copy to File* and export it in the Base-64 encoded X.509 format.
 3. Import the server certificate into the SAP S/4HANA system using *Trust Manager*.
 4. Double click the **ARIBA** SSL Client ID that you have created.
 5. Navigate to the *Certificate* group box and choose *Import certificate*. Add the imported certificate to the certificate list by clicking *Add to Certificate List*.
 5. To activate the changes, restart the Internet Communication Manager (ICM) using transaction SMICM and choose ► *Administration* ► *ICM* ► *Restart* ► *Yes* ►.
For more information, go to https://help.sap.com/s4hana_op_2020, enter *Using the ICM Monitor* into the search bar, press , and open the search result with that title.
 6. Configure the Web services in SOA Manager (transaction SOAMANAGER). Find the following consumer proxies:
 - cXMLSynchronousOutboundAdapterMessage_Out (CO_ARBFND_PRX_OADP_OUT)
 - cXMLGetPendingDataRequest_Out (CO_ARBFND_PRX_GPDQ_OUT)
 In the *Details of Consumer Proxy* group box, navigate to the *Configurations* tab page and select the logical port. In the *Configuration of Logical Port* group box, navigate to the *Consumer Security* tab page, choose the *X.509 SSL Client Certificate* radio button, and enter **Ariba** in the *SSL Client PSE of transaction STRUST* field.
 7. For Ariba Network: In the profile of your account on Ariba Network, select the *Certificate* authentication method in the cXML setup and enter the public key of the certificate.

Authentication with User and Password

To set up authentication with a user and a password, proceed as follows:

1. Maintain the user and the password in the *Define Credentials and Endpoints for Ariba Network* Customizing activity or in the *Define Credentials for SAP Fieldglass* Customizing activity, respectively. The password is stored in the secure storage of your SAP S/4HANA system. SAP S/4HANA supports passwords with a maximum length of 36 characters.

Note

According to security requirements, passwords must not be written to logs, protocols, or traces. Therefore, the password is not visible in transactions such as SRT_MONI where the XML message

monitoring and tracing takes place, as business users can also have authorization for the message monitoring transactions. However, when activating an Internet Communication Framework (ICF) recording using transaction SICF, the system logs the password in the corresponding ICF trace. ICF recording is only intended for administrators and requires the S_ADMI_FCD authorization.

Ariba Network integration only: For authentication with shared secret password, the shared secret password has to be provided in the `sender` element of the cXML payload.

2. For HTTPS SSL encryption, obtain the server certificate from the business network. Proceed as follows:
 1. Go to buyer.ariba.com or to fieldglass.net, respectively.
 2. Download the certificate using your browser.

For example, if you are using Internet Explorer, choose **View > Security Report > View Certificates**. On the *Details* tab page, choose *Copy to File* and export the certificate in the Base-64 encoded X.509 format.
 3. Import the server certificate into the SAP S/4HANA system using *Trust Manager*.
 4. Double-click the *SSL Client SSL Client (Anonymous)* node.

Navigate to the *Certificate* group box and choose *Import certificate*. Add the imported certificate to the certificate list by clicking *Add to Certificate List*.
3. To activate the changes, restart the Internet Communication Manager (ICM) using transaction SMICM and choose **Administration > ICM > Restart > Yes >**.
4. In the profile of your account in the Ariba Network, select the *shared secret* authentication method in the cXML setup.

14.3 Direct Connectivity: SAP S/4HANA as Server

No proxy or reverse proxy is required. The asynchronous inbound application service interfaces are called either internally in the SAP S/4HANA system or by SAP PI.

14.4 Roles and Authorizations (Ariba Network)

A technical user is required in the SAP S/4HANA system to process messages coming from the Ariba Network. This user must not have the SAP_ALL authorization. Assign the following roles to this user:

- **SAP_ARBFND_INTEGRATION**
The authorization object ARBFND_ARB is required to execute reports and to process inbound messages. This object can be added by assigning the role SAP_ARBFND_INTEGRATION.
- **Process Purchase Orders** (SAP_MM_PUR_PURCHASEORDER)
This role provides authorization for purchase orders and is required to process incoming messages that update purchase orders.
- **Process Inbound Deliveries** (SAP_LE_INB_DEL_PROCESSING).
This role provides authorization for inbound deliveries and is required to process incoming messages that create inbound deliveries with receiving point.
- **Enter Invoices for Verification in the Background** (SAP_MM_IV_CLERK_BATCH1)

This role provides authorization to post or park incoming invoice documents in the background. Alternatively, you can assign any other role that contains the authorization object M_RECH_WRK.

Users who have to perform supplier-related Customizing activities must have the following authorization objects assigned to their role:

- F_LFA1_GEN with activity "03"
- F_LFA1_GRP with activity "03"
- F_LFA1_BEK with activity "03"

Depending on whether you use direct or mediated connectivity, you also have to assign one of the following roles:

- For **direct** connectivity:
[Web Service Consumer](#) (SAP_BC_WEBSERVICE_CONSUMER)
This role is required for using Web service protocol to communicate in direct connectivity.
- For **mediated** connectivity:
[Exchange Infrastructure: Service User for Application Systems](#) (SAP_XI_APPL_SERV_USER)
This role is required to communicate through XI protocol in mediated connectivity.

To make sure the corresponding profiles are available and active, you must generate the role profiles using transaction PFCG.

14.5 Roles and Authorizations (SAP Fieldglass)

A technical user is required in the SAP S/4HANA system to process messages coming from SAP Fieldglass. This user must not have the SAP_ALL authorization. Instead, you have to do the following:

1. Create a role that contains the authorization object ARBFND_FG, enter your SAP Fieldglass buyer company code in the field FG_BUY_CC, and assign this role to the technical user.
2. Assign the role [Enter Invoices for Verification in the Background](#) (SAP_MM_IV_CLERK_BATCH1) to the technical user. This role provides authorization to post or park incoming invoice documents in the background. Alternatively, you can assign any other role that contains the authorization object M_RECH_WRK.
3. Depending on whether you use direct or mediated connectivity, you also have to assign one of the following roles:
 - For **direct** connectivity:
[Web Service Consumer](#) (SAP_BC_WEBSERVICE_CONSUMER)
This role is required for using Web service protocol to communicate in direct connectivity.
 - For **mediated** connectivity:
[Exchange Infrastructure: Service User for Application Systems](#) (SAP_XI_APPL_SERV_USER)
This role is required to communicate through XI protocol in mediated connectivity.
4. Users who have to perform supplier-related Customizing activities must have the following authorization objects assigned to their role:
 - F_LFA1_GEN with activity "03"
 - F_LFA1_GRP with activity "03"
 - F_LFA1_BEK with activity "03"



To make sure the corresponding profiles are available and active, you must generate the role profiles using transaction PFCG.

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.

© 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.