

PUBLIC
Document Version: 1.1 – 2020-02-10

Security Guide for SAP S/4HANA 1610 FPS01

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Introduction. 8

2 Before You Start. 9

3 SAP S/4HANA System Landscape Information. 10

4 User Administration and Authentication. 12

4.1 User Management. 12

Non-SAP Fiori Technology. 12

SAP Fiori Technology. 14

4.2 User Data Synchronization. 15

4.3 Integration into Single Sign-On Environments. 15

5 Network and Communication Security. 17

5.1 Communication Channel Security. 17

5.2 Network Security. 18

5.3 Communication Destinations. 18

6 ICF and Session Security. 19

7 File System Access Security. 21

8 Virus Scanning. 22

8.1 Virus Scanning in File Uploads. 22

8.2 General Recommendations for Virus Scan Profiles. 23

8.3 Further Protection Against Active Content. 25

9 Additional System Hardening Activities. 26

10 Data Protection. 28

10.1 Read Access Logging. 30

10.2 Deletion of Personal Data. 31

11 SAP S/4HANA Cross Application Infrastructure. 32

11.1 Data Security in SAP ILM. 32

Data Security in SAP ILM System Connections. 32

Users and Authorizations in SAP ILM. 33

Security of Stored Data in SAP ILM. 34

Logs in SAP ILM. 35

11.2 Payment Card Security. 36

Before You Start. 36

Authorizations . . . 37
Data Storage Security . . . 38
Setting Up Encryption Software . . . 39
Making Settings for Payment Card Security . . . 39
Relevant SSF Applications . . . 41
Generating Keys . . . 41
Migration of Payment Card Data Stored in Unencrypted Form . . . 42
Migration of Payment Card Data on SAP Business Partner . . . 42
Migration to SSF Application PAYCRV . . . 43
Migration to Current Key Version . . . 43
Deleting Key Versions . . . 44
Security-Relevant Logs and Tracing . . . 44
Recommended Implementation Steps . . . 44

12 SAP S/4HANA Enterprise Management . . . 46
12.1 Asset Management . . . 46
Maintenance Operations . . . 46
12.2 Finance . . . 47
Financial Accounting . . . 47
Controlling . . . 80
Master Data Framework . . . 113
Joint Venture Accounting . . . 115
Receivables Management . . . 116
12.3 Manufacturing . . . 119
Authorizations in Manufacturing . . . 119
Production Engineering . . . 126
Production Planning . . . 132
Manufacturing Execution for Discrete Industries . . . 140
Quality Management . . . 156
Maintenance Operations . . . 162
12.4 R&D / Engineering . . . 163
Product Safety and Stewardship . . . 163
Product Lifecycle Management . . . 166
12.5 Sales . . . 170
Authorizations in Sales . . . 171
Communication Channel Security . . . 173
Deletion of Personal Data in Sales . . . 174
Country Specifics . . . 176
12.6 Sourcing and Procurement . . . 177
Authorizations . . . 177
Data Storage Security . . . 184
Other Security-Relevant Information . . . 186

Deletion of Personal Data. . . . 189
Ariba Network Integration. . . . 190
Supplier and Category Management. . . . 190
12.7 Supply Chain. . . . 195
Efficient Logistics and Order Fulfillment. . . . 195
Extended Warehouse Management. . . . 204
12.8 Analytics Technology. . . . 214
Process Performance Monitoring. . . . 214
12.9 Enterprise Technology. . . . 217
Central Master Data. . . . 217
Middleware. . . . 222
Specific Read Access Log Configurations. . . . 263
Agent Framework. . . . 264

13 SAP S/4HANA LoB Products for specific Industries. . . . 265
13.1 Automotive. . . . 265
Vehicle processes for Wholesale and Retail. . . . 265
13.2 Banking. . . . 267
SAP Financial Customer Information Management (FS-BP) . . . 267
Bank Customer Accounts (BCA) . . . 269
Loans Management (FS-CML) . . . 273
Collateral Management (CM) . . . 279
Reserve for Bad Debt (FS-RBD) . . . 283
13.3 Higher Education and Research. . . . 291
Authorizations. . . . 291
Deletion of Personal Data. . . . 295
Data Storage Security. . . . 298
Read Access Logging (Industry Applications). . . . 299
13.4 Professional Services. . . . 300
13.5 Commercial Project Inception and Lean Staffing . . . 300
Introduction . . . 301
Before You Start . . . 302
User Management and Authentication . . . 302
Authorizations. . . . 302
Data Storage Security . . . 305
13.6 Public Sector. . . . 306
Finance. . . . 306
Public Sector Collection and Disbursement. . . . 312
Multichannel Foundation for Utilities and Public Sector (Public Sector). . . . 316
13.7 Utilities. . . . 317
Authorizations. . . . 317
Data Storage Security. . . . 322

Enterprise Services Security. . . . 323
Deletion of Personal Data. . . . 323
Multichannel Foundation for Utilities and Public Sector. . . . 326
13.8 Oil and Gas. . . . 330
Authorizations. . . . 330
Internet Communication Framework Security (ICF). . . . 336
Deletion of Personal Data. . . . 337
Read Access Logging. . . . 340
13.9 SAP for Insurance. . . . 340
Authorizations. . . . 341
Data Storage Security. . . . 342
Deletion of Personal Data. . . . 343
Read Access Logging. . . . 344

14 SAP S/4HANA LOB Products. . . . 346
14.1 Asset Management. . . . 346
Maintenance Operations. . . . 346
Environment, Health and Safety. . . . 347
Resource Scheduling. . . . 373
14.2 Commerce. . . . 375
Commerce Management. . . . 375
14.3 Finance. . . . 384
Treasury and Financial Risk Management. . . . 384
Financial Operations. . . . 440
Contract Accounting. . . . 469
Real Estate Management. . . . 473
14.4 Manufacturing. . . . 476
Maintenance Operations. . . . 476
14.5 Enterprise Technology. . . . 477
Geographical Enablement Framework. . . . 477
14.6 Master Data Governance. . . . 479
Authorization Objects and Roles Used by SAP MDG, Consolidation and Mass Processing. . . . 479
Authorization Objects and Roles Used by SAP MDG, Central Governance. . . . 485
Authorization Objects and Roles Used by SAP MDG, Master Data Quality. . . . 497

15 SAP S/4HANA Compatibility Packs. . . . 501
15.1 Finance. . . . 501
Travel Management. . . . 501
15.2 R&D / Engineering. . . . 504
Product Safety and Stewardship. . . . 505
15.3 Human Resources. . . . 531
User Management. . . . 531

Authorizations. 533
Security-Relevant Logging and Tracing. 536
Core HR and Payroll. 537
Talent Management. 614
Time and Attendance Management. 700
15.4 Industries. 718
Engineering, Construction, and Operations. 718
15.5 Service. 721
Warranty Management. 721

16 Business Network Integration. 723
16.1 Security Aspects for Connectivity Types. 723
16.2 Direct Connectivity: SAP S/4HANA as Client. 724
16.3 Direct Connectivity: SAP S/4HANA as Server. 726
16.4 Roles and Authorizations (Ariba Network). 726
16.5 Roles and Authorizations (SAP Fieldglass). 727

Document History

Version	Date	Description
1.0	February 22, 2017	Initial Version
1.1	February 5, 2020	The chapters Data Protection [page 268] (under *SAP Business Partner for Financial Services (FS-BP)*) and Agent Framework [page 264] were added.

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 SAP NetWeaver 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

Important SAP Notes

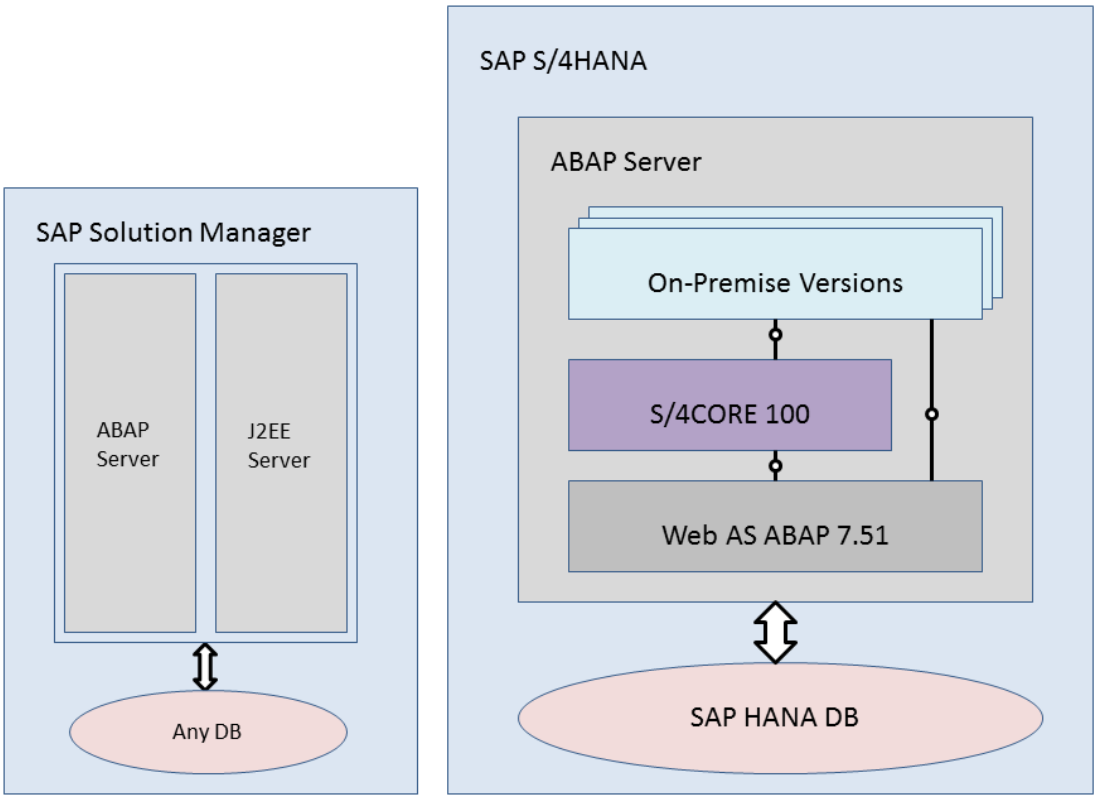
SAP Note 1538539 contains information about saving temporary files when using Adobe Acrobat Reader in SAP applications. SAP Note 138498 contains information on single sign-on solutions. SAP Notes relating to security for the subcomponents of SAP S/4HANA are referenced in the documentation for the individual 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 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 also requires 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.



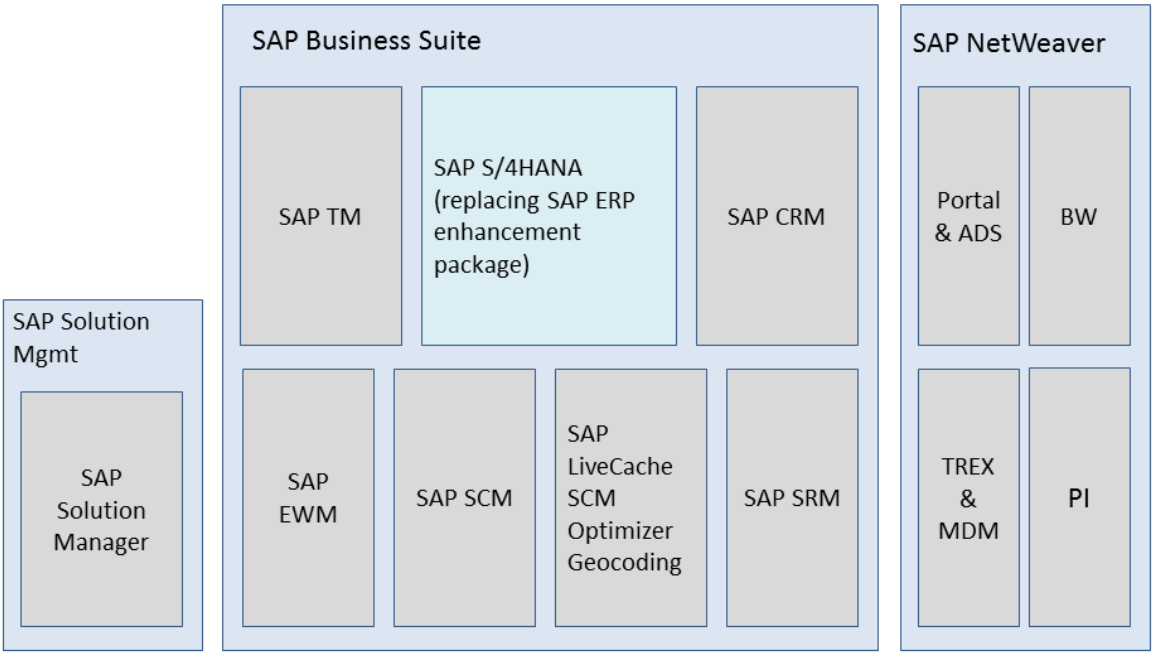
Simple SAP S/4HANA Deployment

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 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 List*.

For more information about the *Simplification List*, see the *Conversion Guide for SAP S/4HANA* at http://help.sap.com/s4hana_op_1610_001 *Product Documentation* .



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

More Information

For more information about SAP Fiori for SAP S/4HANA in a hub deployment, see Landscape Deployment Recommendations for SAP Fiori Front-End Server.

4 User Administration and Authentication

Overview

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

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP S/4HANA 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 S/4HANA.
- User Data Synchronization
  SAP S/4HANA can share user data with other components. This topic describes how the user data is synchronized with these other sources.
- Integration into Single Sign-On Environments

4.1 User Management

4.1.1 Non-SAP Fiori Technology

User management for SAP S/4HANA uses the mechanisms provided with the SAP NetWeaver Application Server for 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. Also, see User and Role Administration of Application Server ABAP at *help.sap.com* *Enterprise Management* *SAP ERP* *SAP ERP 6.0 EHP7* *SAP ERP Security Guide* *SAP ERP Central Component Security Guide* *User Administration and Authentication* *User Administration*.
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, see User Types in the SAP NetWeaver Application Server for ABAP Security Guide.

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
SAP Web Application Server	<sapsid>adm	SAP system administrator	Mandatory	SAP NetWeaver Installation Guide
SAP Web Application Server	SAP Service <sapsid>	SAP system administrator	Mandatory	SAP NetWeaver Installation Guide
SAP Web Application Server	TMSADM	SAP system administrator	Mandatory	SAP NetWeaver Installation Guide
SAP Web Application Server	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	See SAP NetWeaver Security Guide	Optional	SAP NetWeaver 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.

4.1.2 SAP Fiori Technology

For details on the user management and authorization concepts used in SAP Fiori apps, see the *SAP S/4HANA UI Technology Guide* at the SAP Help Portal under http://help.sap.com/s4hana_op_1610_001 ▶ *Product Documentation*.

4.2 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 SAP NetWeaver, you can use all of the mechanisms for user synchronization in SAP NetWeaver here.

For more information, see the *SAP NetWeaver Security Guide* on SAP Help portal at https://help.sap.com/nw75 ▶ *Security Guide*.

4.3 Integration into Single Sign-On Environments

Non-Fiori Technology

SAP S/4HANA supports the single sign-on (SSO) mechanisms provided by SAP NetWeaver Application Server for ABAP technology. Therefore, the security recommendations and guidelines for user management and authentication that are described in the *SAP NetWeaver 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, see *SAP Logon Tickets* in the *Security Guide for SAP NetWeaver Application Server* at https://help.sap.com/nw75 ▶ *Security Guide* ▶ *English* ▶ *Security Guides for the AS ABAP* ▶ *SAP NetWeaver Application Server ABAP Security Guide*.
- 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 see *Client Certificates* in the *Security Guide for SAP NetWeaver Application Server*.
  For more information about available authentication mechanisms, see SAP Library for SAP NetWeaver under *User Authentication and Single Sign-On* at https://help.sap.com/nw75 ▶ *Security Guide*.

For more information about the available authentication mechanisms, see the *User Authentication and Single Sign-On* documentation in the SAP NetWeaver Library.

Fiori Technology

For details on the User Authentication and Single Sign-On concepts used in SAP Fiori apps, see the *SAP S/4HANA UI Technology Guide* at the SAP Help Portal under http://help.sap.com/s4hana_op_1610_001 ▶ *Product Documentation* ◀.

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. 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.

5.1 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 SAP NetWeaver Security Guide.

5.2 Network Security

Network

SAP S/4HANA is based on SAP NetWeaver technology. Therefore, for information about network security, see the respective sections in the SAP NetWeaver Security Guide at https://help.sap.com/nw75 ▶ *Security Guide* ▶ *English* ▶. This includes information on using firewall systems for access control and using network segmentation.

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 diving 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 SAP NetWeaver and uses the ports of AS ABAP. For more information, see the corresponding security guides for SAP NetWeaver under the topics for AS ABAP Ports.

5.3 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

6 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 at http://help.sap.com/s4hana_op_1610_001 under *SAP NetWeaver for SAP S/4HANA* > *Security Guide* > *RFC/ICF Security Guides*.

> **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_cook-ies	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.

7 File System Access Security

More Information

For detailed information about data storage security, see the SAP NetWeaver 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, and DU5.

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 http://help.sap.com/s4hana_op_1610_001, enter one of the following titles into the search bar, press `Enter` 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*

8 Virus Scanning

Basic Concepts

You need to install and run a VSI 2.0-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.

For more information about virus scan profiles and customizing, see the SAP NetWeaver documentation at https://help.sap.com/nw75 ▶ *Application Help* ▶ *Function-Oriented View* ▶ *Security* ▶ *System Security* ▶ *Virus Scan Interface* ▶.

Additional information is available in SAP Notes 786179 and 1494278.

8.1 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 *SAP NetWeaver Security Guide* at https://help.sap.com/nw75 ▶ *Security Guide* ▶ *English* ▶

It is clear that uploaded files need to be scanned for malware. Also, their type needs to be verified against a white list of MIME-types. You can meet both these requirements by installing and running a VSI 2.0-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.

8.2 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 'whitelisting' - 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 whitelist of file types.

Whitelist

Use the 'whitelisting' file type wherever possible.

Consider the following: the whitelist 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 whitelist, you should ensure that the list only contains MIME types from the IANA List .

Template List of File Types

> **i Note**
>
> Your whitelist should be as restrictive as possible. For example, you should delete non-needed types from the template list. A final whitelist 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

8.3 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, see Deleting, Adding, and Enhancing HTTP Header Fields in the SAP NetWeaver documentation at https://help.sap.com/nw75 *Internet Communication Manager (ICM) - SAP NetWeaver* > *Administration of the ICM - SAP NetWeaver* > *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: Example

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.

9 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 a SAP NetWeaver protection to prevent click-jacking attacks. This is a whitelist-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 whitelist.

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 http://help.sap.com/s4hana_op_1610_001, enter *Using a Whitelist for Clickjacking Framing Protection* into the search bar, press `Enter` 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 http://help.sap.com/s4hana_op_1610_001, enter *Unified Connectivity* into the search bar, press `Enter` 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 http://help.sap.com/s4hana_op_1610_001, enter *Customizing Scenario-Based Authorizations* into the search bar, press `Enter` 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`.

10 Data Protection

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 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 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	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.

Term	Definition
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 [page 12].

Authorizations: Authorization concept as described in section User Management [page 12].

Read access logging: as described in section Read Access Logging [page 30].

Transmission control / Communication security: as described in section Network and Communication Security [page 17].

Input control / Change logging

Availability control as described in:

- Section Data Storage Security [page 21]
- SAP Business Continuity documentation in the SAP NetWeaver Application Help under http://help.sap.com/s4hana_op_1610_001 ▶ *SAP NetWeaver for SAP S/4HANA* ▶ *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.

More Information

You can find detailed information on data protection in the SAP Help Portal athttp://help.sap.com/s4hana_op_1610_001 ▶ *Additional Information* ▶ *Product Assistance* ▶ *Cross Components* ▶ *Data Protection*

10.1 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 http://help.sap.com/s4hana_op_1610_001 ▶ *Product Assistance* > *Cross Components* > *Data Protection* .

Prerequisites

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

- You are using:
  - SAP NetWeaver 7.1:SP0
  - AS ABAP 7.51
  - Kernel 7.49
  - SAP_UI 7.51 (UI5 1.40)
- The RAL configurations have been activated.
- You have enabled RAL in each system client.

More information

You can find general information on Read Access Logging in the product assistance for SAP NetWeaver on SAP Help Portal at http://help.sap.com/netweaver.

For up-to-date information on the delivered RAL configurations, see SAPNote 2347271.

For information on delivered log conditions, see the application-specific chapters of the Security Guide.

10.2 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 http://help.sap.com/s4hana_op_1610_001 under *Product Assistance* > *Cross Components* > *Data Protection*.

11 SAP S/4HANA Cross Application Infrastructure

11.1 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.

For more information:

Data Security in SAP NetWeaver ILM System Connections [page 32]

Users and Authorizations in SAP NetWeaver ILM [page 33]

Security of Stored Data in SAP NetWeaver ILM [page 34]

Logs in SAP NetWeaver ILM [page 35]

11.1.1 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*
  - *XML Data Archiving Service (XML DAS)* runs on an AS Java.
    For more information, see: *Configuring XML Data Archiving Service for ILM Stores*

Data Security for System Connections

Communication between systems takes places 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.

11.1.2 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: Connection is the SAP NetWeaver ILM System Landscape [page 32]

Authorizations

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

For more information, see:

Assigning Authorizations for Retention Management Cockpit

Assigning Authorizations for Retention Warehouse Cockpit

Transactions and Authorizations in SAP NetWeaver ILM

11.1.3 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.

For more information, see: *Providing WebDAV Server for ILM Store*

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 Java on which *XML DAS* runs *XML DAS* uses the database pool alias `SAP/BC_XMLA`.

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).

For more information, see:

Generating Checksums Before Archive File Conversion

Generating and Comparing Checksums after ILM Archive File Conversion

11.1.4 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
Storage and Retention Service (SRS)	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`
XML Data Archiving Service (XML DAS)	Log File for XML DAS	AS Java on which XML DAS runs	Can be called in *LogViewer* 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 *LogViewer* File: `defaultTrace.trc` Location: `com.sap.archtech.daservice`
Service-Independent	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)	Can be called in application log Log object: `ILM` Subobjects: • `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)

11.2 Payment Card Security

11.2.1 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 ERP	
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

11.2.2 Authorizations

The functions for secure handling of payment cards use the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS ABAP security guide also apply to the secure handling of payment cards.

The SAP NetWeaver 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 SSFVAPPLIC	01 PAYCRV	Generating a key version

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

11.2.3 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 Tables	Use	Comment
PCA_SECURITY_RAW	Payment Cards and SAP Business Partner	In ERP 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 Tables	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 Tables	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.

11.2.4 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. For executing 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.

11.2.5 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 44] .

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 ERP 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*.

11.2.6 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 ERP 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.

11.2.7 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.

11.2.8 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 42] .

11.2.9 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 ERP 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
BUT0CC	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 BUT0CC.

Database Tables

Database Table	Use
PCA_SECURITY_*	Data of payment card
BUT0CC	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 380].

11.2.10 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.

11.2.11 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.

You run the migration on the SAP Easy Access screen under *Cross-Application Components* > *Security of Payment Card Data* > *Encryption of Payment Cards* > *Execute Conversion* . You can define parallel processing for the migration using the s *ubarea* . 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.

11.2.12 Deleting Key Versions

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.

11.2.13 Security-Relevant Logs 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 39]).

The system updates the log on database table CCSEC_LOG. You can analyze the log on 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.

11.2.14 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 41] .)
2. Make settings for payment card security. (See Making Settings for Payment Card Security [page 39] .)
    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 39] .)
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 42] .)

Variant 2: Security LevelMasked Display, and Encrypted When SavedAlready 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 39] .)
3. Migrate the stored encrypted data to the SSF application PAYCRV. (See Migration to SSF Application PAYCRV [page 43] .)

12 SAP S/4HANA Enterprise Management

12.1 Asset Management

12.1.1 Maintenance Operations

12.1.1.1 Authorizations in Plant Maintenance

Plant Maintenance uses the authorization concept provided by the SAP 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Roles for Plant Maintenance

Role	Description
SAP_COCKPIT_EAMS_MAINT_WORKER2	*Maintenance Worker 2* This role contains all the functions that a maintenance worker requires to carry out their work effectively and safely. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.
SAP_COCKPIT_EAMS_GENERIC_FUNC2	*Generic EAM Functions 2* The purpose of this role is to provide the maintenance planner with a broad range of functions necessary for planning and executing maintenance activities. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.

12.2 Finance

12.2.1 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.

12.2.1.1 Authorizations in Financial Accounting

The following table shows the security-relevant authorization objects that are used by Financial Accounting.

For additional authorization objects that are specific to the components in Financial Accounting (such as FI-GL and FI-SL), see the corresponding sections of this Security Guide.

Standard Authorization Objects in Financial Accounting

Authorization Object	Description
F_WEB_ADRS	Display/Change of Address Data via Web Interface
F_KKINTER	Authorization for Interest Posting
F_PAYRQ	Authorization Object for Payment Requests
F_BKPF_BLA	Accounting Document: Authorization for Document Types
F_BKPF_BUK	Accounting Document: Authorization for Company Codes
F_BKPF_BUP	Accounting Document: Authorization for Posting Periods

F_BKPF_GSB	Accounting Document: Authorization for Business Areas
F_BKPF_KOA	Accounting Document: Authorization for Account Types
F_BKPF_VW	Accounting Document: Display/Change Default Values Document Type/Posting Key
F_PAYOH_AV	Release and Rejection Reasons
F_FBCJ	Cash Journal: General Authorization
F_KK_CJROL	Cash Journal: Maintenance of Responsibilities
F_KMT_MGMT	Account Assignment Model: Authorization for Maintenance and Use
F_WTMG	Withholding Tax Changeover
FOT_B2A_V	Admin. Report Electronic Data Transmission to Authorities
FINS_MIG	Authorization object for migration to SAP Simple Finance, On-Premise Edition
FQM_FLOW	Authorization object for Financial Quantity Management

12.2.1.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *Product Assistance* ▶ *Cross Components* ▶ *Data Protection* ▶.

Relevant Application Objects and Available Deletion Functionality

Application Object	Provided Deletion Functionality
FI documents	ILM object `FI_DOCUMNT` (SAP note 2011278)
Bank statement	ILM object `FI_ELBANK`

Application Object	Provided Deletion Functionality
Check management	ILM object `FI_SCHECK`
Interest data	• Deletion report `RFINTITDEL_DES` • ILM object `FI_INTEREST_DESTRUCTION` (SAP note 1926249)
Payment data	Deletion report `SAPF110R`
Payment order	Deletion report `RFPYORDD`
Dunning data	• Deletion report `SAPF150R_DES` • ILM object `FI_DUNNING_DESTRUCTION` (SAP note 1932584)
Cash Journal data	ILM object `FI_TCJ_DOC` (SAP note 1949312)
Payment requests	ILM object `FI_PAYRQ` (SAP note 2005535)
Payment advice data	Deletion report `RFAVIS20`
Error correction system (ECS)	ILM object `GLE_ECS` (SAP note 1900413)
Down payment chain	ILM object `/SAPPCE/DP` (SAP note 1876387)
Accounting interface posting data	ILM object `MM_ACCTIT`
Asset Accounting	ILM object `AM_ASSET` (SAP note 1860049)

Available Check

Implemented Solution: End of Purpose Check

For more information, see SAP note 2018575.

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`.

12.2.1.3 General Ledger Accounting (FI-GL)

12.2.1.3.1 Authorizations

The following table shows the standard roles that are used by the FI-GL component.

Standard Roles in General Ledger Accounting

Role	Description
SAP_AUDITOR_BA_FI_GL_NEW_A	AIS - General Ledger (New), Authorizations
SAP_EP_RW_AIS_FI_GL	AIS - General Ledger (GLT0)
SAP_EP_RW_AIS_FI_GL_NEW	AIS - General Ledger (New)
SAP_FI_GL_ACCOUNT_CHANGE_REQUE	Request for G/L Account Change or Creation
SAP_FI_GL_ACCT_MASTER_DATA	General Ledger Master Data Maintenance
SAP_FI_GL_BALANCE_CARRYFORWARD	Balance Carryforward
SAP_FI_GL_CHANGE_PARKED_DOCUM	Change Parked G/L Account Documents
SAP_FI_GL_CLEAR_OPEN_ITEMS	Clear Open G/L Account Items
SAP_FI_GL_CONS_PREPARATIONS	Preparations for Consolidation
SAP_FI_GL_CURRENCY_VALUATION	Foreign Currency Valuation: G/L Accounts
SAP_FI_GL_DISPLAY_ACCT_BALANCE	Display G/L Account Balances and Items
SAP_FI_GL_DISPLAY_DOCUMENTS	Display G/L Account Documents
SAP_FI_GL_DISPLAY_MASTER_DATA	Display G/L Account Master Data
SAP_FI_GL_DISPLAY_PARKED_DOCUM	Display Parked Documents
SAP_FI_GL_EXCHANGE_RATE_TABLE	Maintain Currency Exchange Rates
SAP_FI_GL_FIN_STATEMENT_REPORT	Financial Statement Reports
SAP_FI_GL_INTEREST_CALCULATION	Interest Calculation for G/L Accounts
SAP_FI_GL_INTEREST_RATE_TABLES	Maintain Interest Rates
SAP_FI_GL_KEY_REPORTS	Important Reports: General Ledger
SAP_FI_GL_PARK_DOCUMENT	Park G/L Account Documents

SAP_FI_GL_PERIOD_END_CLOSING	Closing Operations: General Ledger Accounting
SAP_FI_GL_PERIODIC_ENTRIES	Entry of Recurring G/L Account Postings
SAP_FI_GL_POST_ENTRY	Make G/L Account Postings
SAP_FI_GL_POST_PARKED_DOCUMENT	Post Parked Document
SAP_FI_GL_RECURRING_DOCUMENTS	Process Recurring Documents
SAP_FI_GL_REORG_MANAGER	Reorganization Manager (FI-GL (New))
SAP_FI_GL_REORG_OBJLIST_OWNER	Object Owner for the Reorganization (FI-GL (New))
SAP_FI_GL_REVERSE-CHANGE	Reverse/Change G/L Account Documents
SAP_FI_GL_SAMPLE_ACCT_MASTER_D	Sample Accounts
SAP_FI_GL_SAMPLE_DOCUMENTS	Edit Sample Documents
SAP_GLE_ADB_EXPERT	Average Daily Balance: Expert
SAP_GLE_ECS_ALL	Error Correction and Suspense Accounting: Expert
SAP_GLE_ECS_DISPLAY	Display Error Correction and Suspense Accounting
SAP_FI_GL_MCA_EXPERT	Multi Currency Accounting: Expert
SAP_FI_GL_MCA_DISPLAY	Display Multi Currency Accounting

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by the FI-GL component.

Standard Authorizations in General Ledger Accounting

Authorization Object	Description
F_ACE_PST	Accrual Engine: Accrual Postings
F_ACE_DST	Accrual Engine: Accrual Objects
F_INVRPMAT	Authorization for Material Journal (Inventory Info System)
F_INVRPWIP	Authorization for WIP Journal (Inventory Info System)
GLE_ECS	Authorization Check for Changing ECS Items
F_T011	Financial Statements: General Maintenance Authorization

F_BKPF_BES	Accounting Document: Account Authorization for G/L Accounts
F_FAGL_CV	Customizing Versions
F_FAGL_SKF	FI: Processing of Statistical Key Figures
F_FAST_CLS	Fast Close Authorizations
F_FAGL_LDR	General Ledger: Authorization for Ledger
F_FAGL_DRU	General Ledger: Authorization for Rule Entries for Validation
F_REORG_PL	General Ledger: Authorization for Reorganization
F_FAGL_SEG	General Ledger: Authorization for Segment
F_FAGL_SLL	General Ledger: Authorization to Switch Leading Ledger
F_RPROC	Intercompany Reconciliation: Authorizations
FAGL_INST	Customer Enhancements for General Ledger
F_T011_BUK	Planning: Authorization for Company Codes
F_SKA1_BUK	G/L Account: Authorization for Company Codes
F_SKA1_KTP	G/L Account: Authorization for Charts of Accounts
F_SKA1_BES	G/L Account: Account Authorization
F_SKA1_AEN	G/L Account: Change Authorization for Certain Fields
K_TP_VALU	Transfer Price Valuations

12.2.1.3.2 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
    - RGRRTE00
    - RGRSTE00
    - RGRVTE00
    - RGRXTE00
    - RGSSTE00
    - RGSVTE00
    - RGRJTI00
    - RGRMTI00
    - RGSSTI00
    - RGSVTI00
  - 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'	
RFBIDET0	Program name (SY-REPID)	Parameter 'Client'	
RFBIKRT0	Program name (SY-REPID)	Parameter 'Client'	
RFFR0E84	Program name (SY-REPID)	Parameter 'Customers/ vendors'	Parameter 'Key Date'
RFFRDDE0	Program name (SY-REPID)	Parameter 'Company Code'	Parameter 'Type'
RFFRLIST	Program name (SY-REPID)		
RFFRMOD1	Program name (SY-REPID)		
RFIDPTFO	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>
RFBIBLT0	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

12.2.1.4 Accounts Payable Accounting (FI-AP)

Standard Roles in Accounts Payable Accounting

Role	Description
SAP_FI_AP_BALANCE_CARRYFORWARD	Vendor Balance Carryforward
SAP_FI_AP_CHANGE-REVERSE_INV	Change/Reverse Vendor Invoices
SAP_FI_AP_CHANGE_LINE_ITEMS	Change Vendor Line Items
SAP_FI_AP_CHANGE_PARKED_DOCUM	Change Parked Vendor Documents
SAP_FI_AP_CHECK_MAINTENANCE	Check Processing
SAP_FI_AP_CLEAR_OPEN_ITEMS	Clear Vendor Line Items

Role	Description
SAP_FI_AP_CORRESPONDENCE	Correspondence – Vendors
SAP_FI_AP_DISPLAY_BALANCES	Display Vendor Balances and Items
SAP_FI_AP_DISPLAY_CHECKS	Display Checks
SAP_FI_AP_DISPLAY_DOCUMENTS	Display Vendor Documents
SAP_FI_AP_DISPLAY_MASTER_DATA	Display Vendor Master Data
SAP_FI_AP_DISPLAY_PARKED_DOCUM	Display Parked Vendor Documents
SAP_FI_AP_INTEREST_CALCULATION	Vendor Interest Calculation
SAP_FI_AP_INTERNET_FUNCTIONS	Internet Functions in Accounts Payable Accounting
SAP_FI_AP_INVOICE_PROCESSING	Entry of Vendor Invoices
SAP_FI_AP_KEY_REPORTS	Important Reports from Accounts Payable Accounting
SAP_FI_AP_MANUAL_PAYMENT	Manual Payment
SAP_FI_AP_PARK_DOCUMENT	Park Vendor Documents
SAP_FI_AP_PAYMENT_BILL_OF_EXCH	Payment Transaction with Bill of Exchange
SAP_FI_AP_PAYMENT_CHECKS	Payment Program with Check Processing
SAP_FI_AP_PAYMENT_PARAMETERS	Display of Payment Run Parameters
SAP_FI_AP_PAYMENT_PROPOSAL	Create and Process Proposal for a Payment Run
SAP_FI_AP_PAYMENT_RUN	Payment Run Update Run without Printing Payment Medium
SAP_FI_AP_PCARD	Payment Card (Procurement Card)
SAP_FI_AP_PERIOD_END_ACTIVITY	Accounts Payable Accounting Period Closing
SAP_FI_AP_POST_PARKED_DOCUM	Post Parked Vendor Document
SAP_FI_AP_RECURRING_DOCUMENTS	Vendor Recurring Entry Documents
SAP_FI_AP_SAMPLE_DOCUMENTS	Edit Sample Documents: Accounts Payable Accounting
SAP_FI_AP_VENDOR_MASTER_DATA	Vendor Master Data Maintenance
SAP_FI_AP_WITHHOLDING_TAX	Withholding Tax Processing
SAP_FI_AP_VALUATION	Valuation of Accounts Payable Items

Authorization Objects That Are Used by Accounts Payable and Accounts Receivable

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_BKPF_BED	Accounting Document: Account Authorization for Customers	X		
F_BKPF_BEK	Accounting Document: Account Authorization for Vendors		X	
F_BKPF_BES	Accounting Document: Account Authorization for G/L Accounts			X
F_BKPF_BLA	Accounting Document: Authorization for Document Types	X	X	X
F_BKPF_BUK	Accounting Document: Authorization for Company Codes	X	X	X
F_BKPF_BUP	Accounting Document: Authorization for Posting Periods	X	X	X
F_BKPF_GSB	Accounting Document: Authorization for Business Areas	X	X	X
F_BKPF_KOA	Accounting Document: Authorization for Account Types	X	X	X
F_BKPF_VW	Accounting Document: Change Default Values Document Type/Posting Key	X	X	X
F_LFA1_AEN	Vendor: Change Authorization for Certain Fields		X	
F_LFA1_APP	Vendor: Application Authorization		X	

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_LFA1_BEK	Vendor: Accounts Authorization		X	
F_LFA1_BUK	Vendor: Authorization for Company Codes		X	
F_LFA1_GEN	Vendor: Central Data		X	
F_LFA1_GRP	Vendor: Accounts Group Authorization		X	
F_KNA1_AEN	Customer: Change Authorization for Certain Fields	X		
F_KNA1_APP	Customer: Application Authorization	X		
F_KNA1_BED	Customer: Accounts Authorization	X		
F_KNA1_BUK	Customer: Authorization for Company Codes	X		
F_KNA1_GEN	Customer: Central Data	X		
F_KNA1_GRP	Customer: Accounts Group Authorization	X		
F_KNA1_KGD	Customer: Change Authorization for Accounts Groups	X		
F_KNB1_ANA	Customer: Authorization for Account Analysis	X		
F_SKA1_AEN	G/L Account: Change Authorization for Certain Fields			X
F_SKA1_BES	G/L Account: Account Authorization			X
F_SKA1_BUK	G/L Account: Authorization for Company Codes			X

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_SKA1_KTP	G/L Account: Authorization for Charts of Accounts			X
F_IT_ALV	Line Item Display: Change and Save Layouts	X	X	
F_KMT_MGMT	Account Assignment Model: Authorization for Maintenance and Use	X	X	
F_T060_ACT	Information System: Account Type/Activity for Evaluation View	X	X	
F_AVIK_AVA	Payment Advice Note: Authorization for Payment Advice Note Types	X	X	
F_AVIK_BUK	Payment Advice Note: Authorization for Company Codes	X	X	
F_BNKA_BUK	Banks: Authorization for Company Codes	X	X	
F_BNKA_MAN	Banks: General Maintenance Authorization		X	
F_KNKK_BED	Credit Management: Accounts Authorization	X		
F_MAHN_BUK.	Automatic Dunning: Authorization for Company Codes	X		
F_MAHN_KOA	Automatic Dunning: Authorization for Account Types	X		
F_PAYR_BUK	Check Management: Action Authorization for Company Codes		X	

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_REGU_BUK	Automatic Payment: Action Authorization for Company Codes		X	
F_REGU_KOA	Automatic Payment: Action Authorization for Account Types		X	
F_T042_BUK	Customizing Payment Program: Authorization for Company Codes		X	
F_BNKA_MAN	Banks: General Maintenance Authorization		X	
F_KNKA_AEN	Credit Management: Change Authorization for Certain Fields	X		
F_KNKA_KKB	Credit Management: Authorization for Credit Control Area	X		

12.2.1.5 Accounts Receivable Accounting (FI-AR)

Standard Roles in Accounts Receivable Accounting

Role	Description
SAP_FI_AR_BALANCE_CARRYFORWARD	Customer Balance Carryforward
SAP_FI_AR_BILL_OF_EXCHANGE	Process Bill of Exchange
SAP_FI_AR_CHANGE-REVERSE	Change/Reverse Customer Postings
SAP_FI_AR_CHANGE_LINE_ITEMS	Change Customer Items
SAP_FI_AR_CHANGE_PARKED_DOCUM	Change Parked Documents
SAP_FI_AR_CLEAR_OPEN_ITEMS	Clear Customer Items
SAP_FI_AR_CREDIT_MASTER_DATA	Credit Management Master Data

Role	Description
SAP_FI_AR_CUST_DOWN_PAYMENTS	Processing of Customer Payments
SAP_FI_AR_DISPLAY_CREDIT_INFO	Display Credit Data
SAP_FI_AR_DISPLAY_CUST_INFO	Display Customer Information
SAP_FI_AR_DISPLAY_DOCUMENTS	Display Customer Documents
SAP_FI_AR_DISPLAY_MASTER_DATA	Display Customer Master Data
SAP_FI_AR_DISPLAY_PARKED_DOCUM	Display Parked Customer Document
SAP_FI_AR_DUNNING_PROGRAM	Dunning Program
SAP_FI_AR_INTEREST_CALCULATION	Customer Interest Calculation
SAP_FI_AR_INTERNET_FUNCTIONS	Internet Functions for Accounts Receivable Accounting
SAP_FI_AR_KEY_REPORTS	Important Reports for Accounts Receivable Accounting
SAP_FI_AR_MASTER_DATA	Customer Master Data Maintenance
SAP_FI_AR_PARK_DOCUMENT	Park Customer Documents
SAP_FI_AR_PAYMENT_CARD_PROCESS	Payment Card Processing
SAP_FI_AR_PERIOD_END_PROCESS	Closing Operations: Accounts Receivable Accounting
SAP_FI_AR_POST_ENTRIES	Post Customer Invoices and Credit Memos
SAP_FI_AR_POST_MANUAL_PAYMENTS	Post Incoming Payments Manually
SAP_FI_AR_POST_PARKED_DOCUMENT	Post Parked Customer Document
SAP_FI_AR_PRINT_CORRESPONDENCE	Correspondence with Customers
SAP_FI_AR_RECURRING_DOCUMENTS	Customer Recurring Entry Documents
SAP_FI_AR_SAMPLE_DOCUMENTS	Customer Sample Documents
SAP_FI_AR_VALUATION	Valuation of Customer Items

Authorization Objects That Are Used by Accounts Payable and Accounts Receivable

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_BKPF_BED	Accounting Document: Account Authorization for Customers	X		
F_BKPF_BEK	Accounting Document: Account Authorization for Vendors		X	
F_BKPF_BES	Accounting Document: Account Authorization for G/L Accounts			X
F_BKPF_BLA	Accounting Document: Authorization for Document Types	X	X	X
F_BKPF_BUK	Accounting Document: Authorization for Company Codes	X	X	X
F_BKPF_BUP	Accounting Document: Authorization for Posting Periods	X	X	X
F_BKPF_GSB	Accounting Document: Authorization for Business Areas	X	X	X
F_BKPF_KOA	Accounting Document: Authorization for Account Types	X	X	X
F_BKPF_VW	Accounting Document: Change Default Values Document Type/Posting Key	X	X	X
F_LFA1_AEN	Vendor: Change Authorization for Certain Fields		X	
F_LFA1_APP	Vendor: Application Authorization		X	

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_LFA1_BEK	Vendor: Accounts Authorization		X	
F_LFA1_BUK	Vendor: Authorization for Company Codes		X	
F_LFA1_GEN	Vendor: Central Data		X	
F_LFA1_GRP	Vendor: Accounts Group Authorization		X	
F_KNA1_AEN	Customer: Change Authorization for Certain Fields	X		
F_KNA1_APP	Customer: Application Authorization	X		
F_KNA1_BED	Customer: Accounts Authorization	X		
F_KNA1_BUK	Customer: Authorization for Company Codes	X		
F_KNA1_GEN	Customer: Central Data	X		
F_KNA1_GRP	Customer: Accounts Group Authorization	X		
F_KNA1_KGD	Customer: Change Authorization for Accounts Groups	X		
F_KNB1_ANA	Customer: Authorization for Account Analysis	X		
F_SKA1_AEN	G/L Account: Change Authorization for Certain Fields			X
F_SKA1_BES	G/L Account: Account Authorization			X
F_SKA1_BUK	G/L Account: Authorization for Company Codes			X

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_SKA1_KTP	G/L Account: Authorization for Charts of Accounts			X
F_IT_ALV	Line Item Display: Change and Save Layouts	X	X	
F_KMT_MGMT	Account Assignment Model: Authorization for Maintenance and Use	X	X	
F_T060_ACT	Information System: Account Type/Activity for Evaluation View	X	X	
F_AVIK_AVA	Payment Advice Note: Authorization for Payment Advice Note Types	X	X	
F_AVIK_BUK	Payment Advice Note: Authorization for Company Codes	X	X	
F_BNKA_BUK	Banks: Authorization for Company Codes	X	X	
F_BNKA_MAN	Banks: General Maintenance Authorization		X	
F_KNKK_BED	Credit Management: Accounts Authorization	X		
F_MAHN_BUK.	Automatic Dunning: Authorization for Company Codes	X		
F_MAHN_KOA	Automatic Dunning: Authorization for Account Types	X		
F_PAYR_BUK	Check Management: Action Authorization for Company Codes		X	

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_REGU_BUK	Automatic Payment: Action Authorization for Company Codes		X	
F_REGU_KOA	Automatic Payment: Action Authorization for Account Types		X	
F_T042_BUK	Customizing Payment Program: Authorization for Company Codes		X	
F_BNKA_MAN	Banks: General Maintenance Authorization		X	
F_KNKA_AEN	Credit Management: Change Authorization for Certain Fields	X		
F_KNKA_KKB	Credit Management: Authorization for Credit Control Area	X		

12.2.1.6 Bank Accounting (FI-BL)

Important SAP Notes

For a list of additional security-relevant SAP HotNews and SAP Notes, see the SAP Service Marketplace at **http://service.sap.com/securitynotes**.

12.2.1.6.1 Authorizations

The following table shows the standard roles that are used by the FI-BL component.

Standard Roles of Bank Accounting

Role	Description
SAP_FI_BL_ACCOUNT_REPORTS	Financial Status Information
SAP_FI_BL_BANK_MASTERDAT_DISPL	Display Bank Master Data

SAP_FI_BL_BANK_MASTER_DATA	Maintain Bank Master Data
SAP_FI_BL_BANK_STATEMENT	Process Bank Statement
SAP_FI_BL_BANK_STATEMENT_EXT	Process Bank Statement **i Note** You require this authorization if you want to use the bank statement overview. You can only display the bank statement overview in the SAP Business Client.
SAP_FI_BL_BILL_OF_EX_PRESENT	Presenting a Bill of Exchange
SAP_FI_BL_BILL_OF_EX_REPORTS	Reports About Bill of Exchange Position
SAP_FI_BL_CASHED_CHECKS	Cashed Checks
SAP_FI_BL_CASH_JOURNAL	Cash Journal
SAP_FI_BL_CHECK_DELETE	Deletion of Checks
SAP_FI_BL_CHECK_DEPOSIT	Check Deposit
SAP_FI_BL_CHECK_MANAGEMENT	Check Management
SAP_FI_BL_CHECK_MGMENT_DISPLAY	Display Managed Checks
SAP_FI_BL_INTRADAY_STATEMENT	Import Intraday Bank Statement Information (USA)
SAP_FI_BL_LOCKBOX	Processing of Lockbox - Data
SAP_FI_BL_ONLINE_PAYMENT	Execute Online Payments
SAP_FI_BL_PAYMENT_TRANSACTIONS	Payment Processing
SAP_FI_BL_PAYME_ADVICE_REPORTS	Reports About Payment Advice Notes
SAP_FI_BL_POR_PROCEDURE	Incoming Payment Using ISR Procedure (Switzerland)
SAP_FI_BL_RETURNED_BILL_OF_EX	Returned Bill of Exchange

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by the FI-BL component.

Standard Authorization Objects of Bank Accounting

Authorization Object	Description

F_BL_BANK	Authorization for house banks and payment methods.
F_BNKA_BUK	Banks Authorization for Company Codes
F_FBCJ	Cash Journal General Authorization
F_FEBB_BUK	Bank Account Statement Company Code
F_FEBC_BUK	Check Deposit/Lockbox Company Code
F_BNKA_MAN	Banks General Maintenance Authorization
F_PAYRQ	Authorization object for payment requests
F_PAYR_BUK	Check Management: Action authorization for company codes
F_REGU_BUK	Automatic payment: Action authorization for company codes
F_REGU_KOA	Automatic payment: Action authorization for account types
F_RPCODE	Repetitive Code
F_RQRSVIEW	Bank Ledger: Viewer for Request Response Messages
F_T042_BUK	Customizing Payment Program Authorization for Company Codes

12.2.1.6.2 Data Storage Security

For information on communication with external systems, see the general part of this Guide under Financial Accounting [page 47].

> → Recommendation
>
> When you use the *electronic bank statement*, SAP strongly advises you run a virus software check on the data retrieved from the bank in you system **before** importing the data into the SAP system, as **no** virus scan is made by SAP in the electronic bank statement. For more information, see SAP Note 599541.

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

The following lists show the logical file names and paths that are used in Bank Accounting, and the programs for which these file names and paths apply:

Logical File Names Used in Bank Accounting

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

- FI_RFEBKAT0_FILE
  - Program using this logical file name:
    - RFEBKAT0
- FI_RFEBKATX_FILE
  - Program using this logical file name:
    - RFEBKATX
- FI_RFEBKAT1_FILE
  - Program using this logical file name:
    - RFEBKAT1
- FI_RFEBEST0_FILE
  - Program using this logical file name:
    - RFEBEST0
- FI_RFEBLBT1_FILE
  - Program using this logical file name:
    - RFEBLBT1
- FI_RFEBLBT2_FILE
  - Program using this logical file name:
    - RFEBLBT2

Parameters used in this context: <PARAM_1> Program Name

Logical Path Names Used in Bank Accounting

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

12.2.1.7 Asset Accounting (FI-AA)

Important SAP Notes

For a list of additional security-relevant SAP HotNews and SAP Notes, see the SAP Service Marketplace at *http://service.sap.com/securitynotes*.

Standard Roles

Role	Description
SAP_AUDITOR_BA_FI_AA	AIS Fixed Assets
SAP_AUDITOR_BA_FI_AA_A	AIS - Fixed Assets (Authorizations)
SAP_FI_AA_ASSET_ARCHIVING	Archiving Activities

Role	Description
SAP_FI_AA_ASSET_CAPITALIZATION	Capitalization of Asset under Construction
SAP_FI_AA_ASSET_ENVIRONMENT	Worklist and Tools in Asset Accounting
SAP_FI_AA_ASSET_EXPLORER	Asset Explorer
SAP_FI_AA_ASSET_INFOSYSTEM	Asset Accounting Information System
SAP_FI_AA_ASSET_MASTER_DATA	Asset Master Data Maintenance
SAP_FI_AA_ASSET_REVALUATION	Revaluation Activities
SAP_FI_AA_ASSET_TRANSACTIONS	Asset Transactions
SAP_FI_AA_CURRENT_SETTINGS	Current Settings
SAP_FI_AA_EVERY_MANAGER	Activities for Cost Center Manager
SAP_FI_AA_GROUP_ASSET	Maintain Group Asset
SAP_FI_AA_KEY_REPORTS	Important Reports in Asset Accounting
SAP_FI_AA_PERIODIC_PROCESSING	Periodic Processing
SAP_FI_AA_PROBLEM_ANALYSIS	Tools for Analyzing Problems
SAP_FI_AA_YEAR_END_CLOSING	Year-End Closing

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.

12.2.1.8 Special Purpose Ledger (FI-SL)

Standard Roles in Special Purpose Ledger

Role	Description
SAP_AUDITOR_BA_FI_SL	AIS - Special Purpose Ledger
SAP_AUDITOR_BA_FI_SL_A	AIS - Special Purpose Ledger (Authorizations)
SAP_FI_SL_ACTUAL_ASSESSMENT	Special Purpose Ledger Actual Assessment
SAP_FI_SL_ACTUAL_DISTRIBUTION	Special Purpose Ledger Actual Distribution
SAP_FI_SL_ACTUAL_POSTINGS	Special Purpose Ledger Actual Postings
SAP_FI_SL_BATCH_JOBS	Run Special Purpose Ledger Jobs in Background
SAP_FI_SL_CURRENCY_TRANSLATION	Special Purpose Ledger Currency Translation
SAP_FI_SL_DISPLAY_DOCUMENTS	Display Special Purpose Ledger Balances and Documents
SAP_FI_SL_DISPLAY_PLAN	Display Special Purpose Ledger Plan
SAP_FI_SL_MODIFY_PLAN	Modify Special Purpose Ledger Planning
SAP_FI_SL_PLAN_ASSESSMENT	Edit Plan Assessment
SAP_FI_SL_PLAN_DISTRIBUTION	Plan Distribution
SAP_FI_SL_ROLLUP	Special Purpose Ledger Rollup

Authorization Objects in Special Purpose Ledger

Object	Description
G_022_GACT	FI-SL Customizing: Transactions
G_800S_GSE	Special Purpose Ledger Sets: Set
G_802G_GSV	Special Purpose Ledger Sets: Variable
G_806H_GRJ	FI-SL Rollup
G_820_GPL	FI-SL Planning: Planning Parameters
G_821S_GSP	FI-SL Planning: Distribution Keys

Object	Description
G_880_GRMP	FI-SL Customizing: Global Companies
G_881_GRLD	FI-SL Customizing: Ledger
G_888_GFGC	FI-SL Customizing: Field Movements
G_ADMI_CUS	Central Administrative FI-SL Tools
G_ALLOCTN	Special Purpose Ledger - Assessment/Distribution
G_GLTP	Special Purpose Ledger - Database (Ledger, Record Type, Version)
G_REPO_GLO	FI-SL: Global Reporting (Global Company)
G_REPO_LOC	FI-SL: Local Reporting (Company Code)
F_T011_BUK	Planning: Authorization for Company Codes

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> *Program Name*	FI_ROOT
RGRLTE00			
RGRMTE00			
RGRRTE00			
RGRSTE00			
RGRVTE00			
RGRXTE00			

Program	Logical File Name Used by the Program	Parameter Used in Context	Logical Path Name Used by the Program
RGSSTE00			
RGSVTE00			
RGRJTI00			
RGRMTI00			
RGSSTI00			
RGSVTI00			
SAPMGLRV	FI_ROLLUP	<PARAM_1> *Program Name* (SY-CPROG)	FI_ROOT
SAPFGRWE	FI_REPORT_WRITER	<PARAM_1> *Program Name* (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.

12.2.1.9 Country Specifics

12.2.1.9.1 China

12.2.1.9.1.1 Bill of Exchange Management

12.2.1.9.1.1.1 Authorizations

Bill of Exchange Management uses the authorization concept provided by the SAP Net Weaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to *Bill of Exchange Management*.

The SAP NetWeaver 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 *Role Administration*.

Standard Roles

The following table shows the standard roles that are used by *Bill of Exchange Management*:

Role	Description
FUCN_CASHIER	A user with the Cashier role is responsible for the processing operations for a bill of exchange
FUCN_TREASURY_MANAGER	A user with the Treasury Manager role is responsible for reviewing and approving the bill of exchange
FUCN_ACCOUNTANT	A user with the Accountant role is responsible for claiming an open invoice by bill of exchange and posting FI documents

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by *Bill of Exchange Management*.

Authorization Object	Description
F_BOEA_GSB	You use this authorization object to determine what actions a user can perform for a bill of exchange document for a given business area. A user can perform certain actions on a bill of exchange document only if they have the authorization.
F_BOEA_BUK	You use this authorization object to determine what actions a user can perform for a bill of exchange document for a given company code. A user can perform certain actions on a bill of exchange document only if they have the authorization.

Authorization Object	Description
F_BOEA_CUS	You use this authorization object to determine what actions a user can perform for a bill of exchange document for a given customer. A user can perform certain actions on a bill of exchange document only if they have the authorization.
F_BOEA_PRC	You use this authorization object to determine what actions a user can perform for a bill of exchange document for a given profit center. A user can perform certain actions on a bill of exchange document only if they have the authorization.
F_BOEA_VEN	You use this authorization object to determine what actions a user can perform for a bill of exchange document for a given vendor. A user can perform certain actions on a bill of exchange document only if they have the authorization.
F_BOE_DRAV	You use this authorization object to determine who has authorization to change draft bills of exchange document that are created by others.

12.2.1.9.1.1.2 Internet Communication Framework Service

You should only activate the services needed for the applications running in your system. In the SAP Business Client, the following services, which you can find under the path `default_host/sap/bc/webdynpro/sap`, are needed.

For application from WD ABAP Page Builder (`BC-WD-ABA-PB`):

- `WDR_CHIP_PAGE`

Bill of Exchange ICF Configuration

The `SICF` services should be activated in `sap/bc/webdynpro/sap`

- `BOE_ACTION_REQUEST`
- `BOE_BLANK_NOTES`
- `BOE_CENTRAL_HISTORY`
- `BoE_CHART_OVP`
- `BOE_COUNTING`
- `BOE_DOC`
- `BOE_HOME`
- `BOE_IMPORT_EXCEL`
- `BOE_OVP_POWL`
- `BOE_OVP_REPORT`
- `BOE_QUICK_ACCESS_OVP`

Features

Use the transaction `SICF` to activate these services.

If your firewalls use URL filtering, take note of 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*.

12.2.1.9.1.2 Financial Accounting and Operations

12.2.1.9.1.2.1 Authorizations

The *Financial Accounting and Operations* uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to the *Financial Accounting and Operations*.

The SAP NetWeaver 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 *Role Administration*.

Standard Roles

The following table shows the standard roles that are used by the *Financial Accounting and Operations*:

Role	Description
`FUCN_ACCOUNTANT`	Accountant whose tasks are document-entry-centric
`FUCN_GL_ACCOUNTANT`	A senior accountant whose major task is to review and verify documents entered by other accountants in the department

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by the *Financial Accounting and Operations*.

Authorization Object	Description
F_DECOLAYR	SAP Financials has a software layer for the creation, change, and display of FI accounting documents in addition to the classical back-end programs. This software layer is the basis for new applications in Financials. This authorization object secures the RFC-enabled function modules of that software layer against unauthorized access. Users that use the new applications for FI accounting documents need the relevant authorization for this object.
F_FUD_DOCV	Users that want to process verification documents need the relevant authorization for this object

12.2.1.9.1.2.2 Internet Communication Framework Service

Use

You should only activate the services needed for the applications running in your system. In the SAP Business Client, the following services, which you can find under the path `default_host/sap/bc/webdynpro/sap`, are needed:

- For application from WD ABAP Page Builder (BC-WD-ABA-PB):
  - `WDR_CHIP_PAGE`
- For applications from SAP Controlling (CO):
  - `FCOM_USER_DETAIL`
  - `FCOM_ACTIVITYTYPE`
  - `FCOM_COSTCENTER`
  - `FCOM_INTERNALORDER_ADAPTATION`
- For applications from Content for ERP Financials (CA-GTF-SP-FIN):
  - `BSSP_DOCUMENT_FLOW`
- For Financial Accounting and Operations (FI):
  - `FUCN_AP_REP_APD`
  - `FUCN_AP_REP_APDBJ`
  - `FUCN_AP_REP_APDD`
  - `FUCN_AP_REP_APR`
  - `FUCN_AP_REP_APRBJ`
  - `FUCN_AR_REP_ARD`

- FUCN_AR_REP_ARDBJ
- FUCN_AR_REP_ARDD
- FUCN_AR_REP_ARR
- FUCN_AR_REP_ARRBJ
- FUCN_GL_REP_CJR
- FUCN_GL_REP_CJRBJ
- FUCN_GL_REP_GLR
- FUCN_GL_REP_GLRBJ
- FUCN_GL_REP_GLRD
- FUCN_GL_REP_JLR
- FUCN_GL_REP_JLRBJ
- FUCN_GL_REP_JLR_BY_BA
- FUCN_GL_REP_JLR_BY_PRCTR
- FUCN_GL_REP_JLR_BY_SEG
- FUCN_REP_MONITOR
- FUCN_WOC_REPORT
- FUCN_WORK_CONTEXT
- FUCN_FIDOC_AUTHOR_FPMPOWL
- FUCN_FIDOC_CANCEL_AUTHOR_POWL
- FUCN_FIDOC_VERIFIER_FPMPOWL
- FUCN_FIDOC_NUMBER_SEARCH
- FUCN_FIDOC_SEARCH
- FUCN_FIDOC_IMPORT_DIALOG
- FUCN_GL_BOL

Features

Use the transaction SICF to activate these services.

If your firewalls use URL filtering, take note of 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*.

12.2.2 Controlling

12.2.2.1 Authorizations

The Controlling component uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to the Controlling component. The SAP NetWeaver 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.

Business Roles

The table below shows the business roles that are used by the Controlling component.

Role	Description
SAP_BR_OVERHEAD_ACCOUNTANT	Cost Accountant - Overhead
SAP_BR_SALES_ACCOUNTANT	Cost Accountant - Sales
SAP_BR_PRODN_ACCOUNTANT	Cost Accountant - Production
SAP_BR_INVENTORY_ACCOUNTANT	Cost Accountant - Inventory
SAP_BR_MANAGER_COST	Manager - Finance Info

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by the Controlling component.

Standard Roles in Controlling

Authorization Object	Field	Value	Description
K_CRM_REP (Authorization Check for Cost Integration CRM – CO)	• SORG (Service Organization) • VART (Business Transaction Type) • ACTVT (Activity)	A5	Display reports

Authorization Object	Field	Value	Description
K_FPB_EXP (Authorization Object for Express Planning)	• EXP_SCEN (Planning Scenario) • EXP_INST (Express Planning Instance) • ACTVT (Activity)	02	Change Assigns authorization to enter data and execute express planning.
		03	Display You have the authorization to display external express planning data.
		39	Check Assigns authorization to check express planning data and to approve or reject the data entered.
K_PVARIANT (Authorization for Screen Variants)	• PVARIANT (Screen Variant for Manual Actual Postings in CO) • VRGNG (Business Transaction)		Assigns authorization to define posting variants for each business transaction.
K_MLMBDISP (CO Material Ledger: Display Material Valuation Document)	• BWKEY (Valuation area)		Assigns authorization to display the material valuation document.
K_ML_MTART (CO Material Ledger: Material Type)	• ACTVT (Activity) • MTART (Material type)	02	Change Assigns authorization to execute and post single-level material price determination and change price determination.
		03	Display Assigns authorization to display material ledger data.
K_ML_VA (CO Material Ledger: Valuation Area)	• ACTVT (Activity) • BWKEY (Valuation area)	02	Change Assigns authorization to perform multilevel material price determination. However, you also need the authorization object K_ML_MTART (CO Material Ledger: Material Type).
		03	Display Assigns authorization to display material ledger data and material ledger documents.

Authorization Object	Field	Value	Description
		16	Execute Assigns authorization for executing and displaying materials for the costing run.
		40	Create in DB
		45	Allow Assigns authorization for executing price determination and closing entries.
K_KLPR_VA (CO Material Price Change: Valuation Area)	• ACTVT (Activity) • BWKEY (Valuation area)	03	Display
		16	Execute
		44	Flag
K_CBPR_VA	• KOKRS (Controlling Area) • ACTVT (Activity)	02	Change Assigns authorization for changing business process groups.
		03	Display Assigns authorization for displaying business process groups.
K_CBPR_PLA	• KOKRS (Controlling Area) • PRZNR (Business Process) • ACTVT (Activity)	02	Change Assigns authorization for displaying and changing planning of business processes.
		03	Display Assigns authorization for displaying planning of business processes.
K_CKPH_SET	• KOKRS (Controlling Area) • ACTVT (Activity)	02	Change Assigns authorization for changing cost object groups.
		03	Display Assigns authorization for displaying cost object groups.

Authorization Object	Field	Value	Description
K_ABC	• AUTHAREA (Authorization Area for Business Processes) • CO_ACTION (Actions for CO-OM Authorization Check) • KSTAR (Cost Element)		Assigns authorization for maintenance actions in business process master data, manual business process planning, the template, and the information system.
K_CSLA_SET	• KOKRS (Controlling Area) • ACTVT (Activity)	02	Change Assigns authorization for changing activity type groups.
		03	Display Assigns authorization for displaying activity type groups.
		06	Delete
K_ CSLA (CO-CCA: Activity Types Master)	• KOKRS (Controlling Area) • ACTVT (Activity)	01	Create or generate Assigns authorization to create activity types.
		02	Change Assigns authorization to change activity types.
		03	Display Assigns authorization to display activity types.
		06	Delete This is not used at present.
		08	Display change documents Assigns authorization to look at change documents on the activity types.
K_CSKS_BUD (CO-CCA: Cost Center Budget Planning)	• KOKRS (Controlling Area) • KOSTL (Cost Center) • ACTVT (Activity)	02	Change Assigns authorization to change the budget of cost centers.
		03	Display Assigns authorization to display the budget of cost centers.

Authorization Object	Field	Value	Description
K_ CSKS_SET (CO-CCA: Cost Center Groups)	• KOKRS (Controlling Area) • ACTVT (Activity)	02	Change Assigns authorization to change cost center groups.
		03	Display Assigns authorization to display cost center groups.
		06	Delete
K_ CSKS (CO-CCA: Cost Center Master)	• KOKRS (Controlling Area) • KOSTL (Cost Center) • ACTVT (Activity)	01	Create or generate Assigns authorization to create cost centers.
		02	Change Assigns authorization to change cost centers.
		03	Display Assigns authorization to display cost centers.
		06	Delete This is not used at present.
		08	Display change documents Assigns authorization to look at change documents on cost centers.
		63	Activate Assigns authorization to activate inactive cost centers.
K_ CSKS_PLA (CO-CCA: Cost Center Planning)	• KOKRS (Controlling Area) • KOSTL (Cost Center) • ACTVT (Activity)	02	Change Assigns authorization to change the planning of cost centers.
		03	Display Assigns authorization to display the planning of cost centers.

Authorization Object	Field	Value	Description
K_ CSKA_SET (CO-CCA Cost Element Groups)	• KTOPL (Chart of Accounts) • ACTVT (Activity)	02	Change Assigns authorization to change cost element groups.
		03	Display Assigns authorization to display cost element groups.
		06	Delete
K_ CSKB (CO-CCA: Cost Element Master)	• KOKRS (Controlling Area) • CO_KAINT (Cost Element Classification (Primary/Secondary) • ACTVT (Activity)	01	Create or generate Assigns authorization to create cost elements.
		02	Change Assigns authorization to change cost elements.
		03	Display Assigns authorization to display cost elements.
		06	Delete This is not used at present.
		08	Display change documents Assigns authorization to view cost element change documents.
K_ CSKB_PLA (CO-CCA: Cost Element Planning)	• KOKRS (Controlling Area) • KSTAR (Cost Element) • ACTVT (Activity)	02	Change Assigns authorization to change the planning of cost elements.
		03	Display Assigns authorization to display the planning of cost elements.
K_CCA (CO-CCA: Gen. Authorization Object for Cost Center Accounting)	• RESPAREA (CO-OM Responsibility Area) • CO_ACTION (Actions for CO-OM Authorization Check) • KSTAR (Cost Element)		Assigns authorization for the maintenance of cost center master data, manual cost center planning, and the information system.

Authorization Object	Field	Value	Description
K_REPO_CCA (CO-CCA: Reporting on Cost Centers/Cost Elements)	• KOKRS (Controlling Area) • KOSTL (Cost Center) • KSTAR (Cost Element) • ACTVT (Activity)	27	Display totals records Assigns authorization for summary record reporting.
		28	Display line items Assigns authorization for line item reporting.
		29	Display saved data Assigns authorization for reporting of stored data.
K_KA03_SET (CO-CCA: Statistical Key Figure Groups)	• KOKRS (Controlling Area) • ACTVT (Activity)	02	Change Assigns authorization to change statistical key figure groups.
		03	Display Assigns authorization to display statistical key figure groups.
K_ORDER (CO-OPA: General authorization object for internal orders)	• RESPAREA (CO-OM Responsibility Area) • AUFART (Order Type) • AUTHPHASE (Internal order authorization: Authorization phase) • CO_ACTION (Actions for CO-OM Authorization Check) • KSTAR (Cost Element)		Assigns authorization for the following actions while working with internal orders: • Maintenance of order master data • Manual order planning • Budgeting of orders • Actions in the information system
K_AUFK_SET (CO-OPA: Order Groups)	• HNAME (Group Name) • ACTVT (Activity)	02	Change Assigns authorization to change order groups.
		03	Display Assigns authorization to display authorization objects in CO-PA planning.
K_KELP_GP (CO-PA Planning: Integrated Planning)	• CEERKRS (Operating concern) • ACTVT (Activity)	16	Execute Assigns authorization to restrict the way integrated planning is used.

Authorization Object	Field	Value	Description
K_KELP_VER (CO-PA Planning: Plan Version)	• CEVERSI (Plan version (CO-PA))		Assigns authorization to process plans depending on plan version.
K_KELP_RC (CO-PA Planning: Planning Layouts)	• CEERKRS (Operating concern) • CEFORM (Form) • ACTVT (Activity)	01	Create or generate Assigns authorization to create planning layouts.
		02	Change Assigns authorization to change planning layouts and plan structures.
		03	Display Assigns authorization to display planning layouts and plan structures.
		21	Transport Assigns authorization to transport planning layouts.
		60	Import Assigns authorization to import planning layouts.
		65	Reorganize Assigns authorization to reorganize planning layouts.
K_WIP (CO-PC-OBJ: WIP Calculation and Results Analysis)	• WERKS (PLANT) • ACTVT (Activity)	02	Change Assigns authorization to change the data for work in process (WIP) calculation and results analysis.
		03	Display Assigns authorization to display the data for WIP calculation and results analysis.
K_WIP (CO-PC-OBJ: WIP Calculation and Results Analysis)	• WERKS (PLANT) • ACTVT (Activity)	02	Change Assigns authorization to change the data for work in process (WIP) calculation and results analysis.

Authorization Object	Field	Value	Description
		03	Display Assigns authorization to display the data for WIP calculation and results analysis.
K_WIP_BU (CO-PC-OBJ: WIP Calculation and Results Analysis)	• BUKRS (Company Code) • ACTVT (Activity)	02	Change Assigns authorization to change processed objects in WIP calculation and results analysis.
		03	Display Assigns authorization to display processed objects in WIP calculation and results analysis.
K_WIP_PC (CO-PC-OBJ: WIP Calculation and Results Analysis)	• PRCTR (Profit Center) • ACTVT (Activity)	02	Change Assigns authorization to change processed objects in WIP calculation and results analysis.
		03	Display Assigns authorization to display processed objects in WIP calculation and results analysis.
K_CBEW (CO-PC: Concurrent Costing - Cstg Master Data)	• ACTVT (Activity)	01	Create or generate
		02	Change
		03	Display
		06	Delete
K_CKPH (CO-PC: Cost Objects)	• KTRAT (Cost Object Category) • ACTVT (Activity)	01	Create or generate Assigns authorization to create cost object IDs.
		02	Change Assigns authorization to change cost object IDs.
		03	Display Assigns authorization to display cost object IDs.

Authorization Object	Field	Value	Description
		06	Delete Assigns authorization to delete cost object IDs.
		72	Plan
		A5	Display reports
K_KEKO (CO-PC: Product Costing)	• KLVAR (Costing Variant) • BUKRS (Company Code) • ACTVT (Activity)	03	Display Assigns authorization to display product costing.
		06	Delete Assigns authorization for executing a reorganization run and for archiving cost estimates.
		16	Execute Assigns authorization for creating and changing a cost estimate, and for creating, changing, executing, and deleting a costing run.
		39	Check
K_CKBOB (CO-PC: Product Drill-down)	• WERKS (Plant) • ACTVT (Activity)	16	Execute Assigns authorization to display a report that was created with product drilldown reporting.
		A5	Display report Assigns authorization to carry out product drilldown reporting.
K_PKSA (CO-PC: Production Cost Collector)	• WERKS (Plant) • ACTVT (Activity)	01	Create or generate Assigns authorization to create a product cost collector in any plant.
		02	Change Assigns authorization to change a product cost collector in any plant.

Authorization Object	Field	Value	Description
		03	Display (master data) Assigns authorization to display a product cost collector in any plant.
		A5	Display reports (cost report)
K_FVMK (CO-PC: Release/Marking - Product Costing)	• BUKRS (Company Code) • ACTVT (Activity)	43	Release Assigns authorization to to release standard cost estimates.
		44	Flag Assigns authorization to mark standard cost estimates.
		45	Allow Assigns authorization to allow marking and releasing of standard cost estimates.
K_SUM_ORD (CO-PC: Summarization – Orders)	• IDENT (Hierarchy ID) • KOKRS (Controlling Area) • ACTVT (Activity)	03	Display Assigns authorization to display a summary of order costs.
		16	Execute Assigns authorization to summarize order costs.
		A5	Display reports Assigns authorization to display reports for order costs.
K_SUM_PROJ (CO-PC: Summarization – Projects)	• IDENT (Hierarchy ID) • KOKRS (Controlling Area) • ACTVT (Activity)	03	Display Assigns authorization to display a summary of project costs.
		16	Execute Assigns authorization to summarize project costs.
		A5	Display reports Assigns authorization to display reports for project costs.

Authorization Object	Field	Value	Description
K_TEMPL (CO: Auth. Template (ABC-allocation, formula planning, other))	• KOKRS (Controlling Area) • TPLCLASS (Valid Environments) • TEMPLATE (Template) • ACTVT (Activity)		
K_VRGNG (CO: Bus. Trans., Actual Postings and Plan/act. Allocations)	• KOKRS (Controlling Area) • CO_VRGNG (CO Business Transaction) • ACTVT (Activity)	01	Create or generate Assigns authorization to create manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).
		02	Change Assigns authorization to change manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).
		03	Display Assigns authorization to display manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).
		06	Delete
		16	Execute
		48	Simulate
K_ZBASSL (CO: Calculation base)	• BASSL (Calculation Base for Overheads) • ACTVT (Activity)	02	Change Assigns authorization to change the overhead rate base.
		03	Display Assigns authorization to display the overhead rate base.

Authorization Object	Field	Value	Description
K_ZKALSM (CO: Costing sheet)	• KALSM (Procedure) • ACTVT (Activity)	02	Change Assigns authorization to change the costing sheet.
		03	Display Assigns authorization to display the costing sheet.
K_ZENTSL (CO: Credit)	• ENTSL (Credit for overhead) • ACTVT (Activity)	02	Change
		03	Display
K_KMBO_DCT (CO: Document Type for Manual Funds Reservation)	• BUKRS (Company Code) • KBLART (Doc.Type: Manual document entry) • ACTVT (Activity)	01	Create or generate Assigns authorization to create funds reservations with a particular document type.
		02	Change Assigns authorization to change funds reservations with a particular document type.
		03	Display Assigns authorization to display funds reservations with a particular document type.
		06	Delete Assigns authorization to reduce funds reservations with a particular document type.
		24	Archive Assigns authorization to archive funds reservations with a particular document type.
K_KFPP_DCT (CO: Document Type for Transfer Price Agreements)	• KOKRS (Controlling Area) • KFPBLA (Document type: Transfer price agreement/allocation) • ACTVT (Activity)	01	Create or generate Assigns authorization to create transfer price agreements with particular document types.

Authorization Object	Field	Value	Description
		02	Change Assigns authorization to change transfer price agreements with particular document types.
		03	Display Assigns authorization to display transfer price agreements with particular document types.
		06	Delete Assigns authorization to delete transfer price agreements with particular document types.
		24	Archive Assigns authorization to archive transfer price agreements with particular document types.
K_KFPI_DCT (CO: Document Type for Transfer Price Allocations)	• KOKRS (Controlling Area) • KFPBLA (Document type: Transfer price agreement/allocation) • ACTVT (Activity)	01	Create or generate Assigns authorization to create transfer price allocations with particular document types.
		03	Display Assigns authorization to display transfer price allocations with particular document types.
		06	Delete Assigns authorization to delete transfer price allocations with particular document types.
		24	Archive Assigns authorization to archive transfer price allocations with particular document types.
K_KA_RCS (CO: Drill-down reporting - line-/column structures)	• CEAPPL (Application class for drilldown reporting) • TABLE (Table Name) • CEFORM (Form)	01	Create or generate Assigns authorization to create row and column structures for drilldown reporting.

Authorization Object	Field	Value	Description
	• ACTVT (Activity)	02	Change Assigns authorization to change row and column structures for drill-down reporting.
		03	Display Assigns authorization to display row and column structures for drill-down reporting.
		21	Transport
		60	Import
		65	Reorganize Assigns authorization to reorganize row and column structures for drill-down reporting.
K_SUM_CO (CO: General CO Summarization Without Classification)	• IDENT (Hierarchy ID) • KOKRS (Controlling Area) • ACTVT (Activity)	03	Display Assigns authorization to display general controlling summarization (without classification).
		16	Execute Assigns authorization to summarize the costs for the summarization hierarchy in the controlling area.
		A5	Display reports Assigns authorization to display a report for the summarization hierarchy in the controlling area.
K_KA_RPT (CO: Interactive Drill-down Reporting – Reports)	• CEAPPL (Application class for drilldown reporting) • TABLE (Table Name) • CEREPID (Report) • ACTVT (Activity)	01	Create or generate
		02	Change
		03	Display
		04	Print, edit messages
		16	Execute
		21	Transport

Authorization Object	Field	Value	Description
		28	Display line items
		29	Display saved data
		32	Save
		60	Import
		61	Export
		65	Reorganize
		66	Refresh
		L0	All functions
		L1	Function range level 1
		L2	Function range level 2
K_ORGUNIT (CO: Organizational Units Used in Actual Postings)			
K_ZZUSSL (CO: Overhead)	• ZUSSL (Overhead rate) • ACTVT (Activity)	02	Change Assigns authorization to change overhead rates for overheads.
		030	Display Assigns authorization to display overhead rates for overheads.
K_ZSCHL (CO: Overhead key)	• ZUSSL (Overhead rate) • ACTVT (Activity)	02	Change Assigns authorization to change the overhead key for overheads.
		03	Display Assigns authorization to display the overhead key for overheads.
K_TKA50 (CO: Planner Profiles)	• BRGRU (Authorization Group) • ACTVT (Activity)	01	Create or generate Assigns authorization to create authorization for planner profiles.
		02	Change Assigns authorization to change authorization for planner profiles.

Authorization Object	Field	Value	Description
		03	Display Assigns authorization to display authorization for planner profiles.
		06	Delete
		16	Execute
K_REPO_USR (CO: Reporting / User Settings)	• ACTVT (Activity) • KUSRGR (Indicator for user group)	02	Change Assigns authorization to change user settings for overhead cost controlling.
		03	Display Assigns authorization to display user settings for overhead cost controlling.
K_KA_TREC (CO: Summarization Levels)	• ACTVT (Activity) • CEAPPL (Application class for drilldown reporting) • TABLE (Table Name)	02	Change Assigns authorization to change summarization levels.
		03	Display
		07	Activate, generate
		66	Refresh Assigns authorization to update summarization levels.
		71	Analyze Assigns authorization to analyze the access log.
K_KA09_KVS (CO: Version)	• BRGRU (Authorization Group) • ACTVT (Activity)	02	Change
		03	Display
		72	Plan
		DP	Delete plan
K_KC_PL (EC-BP: Authorization for Planning Layouts)	• CFASPET (Aspect (application area)) • CEFORM (Form) • ACTVT (Activity)		Assigns authorization to create, change, and display planning layouts. It also assigns authorization to display and change plan data.

Authorization Object	Field	Value	Description
K_KC_DE (EC-EIS Authorization - Entry Layout / Data Entry)	• CFASPET (Aspect (application area)) • CEFORM (Form) • ACTVT (Activity)	01	Create or generate Assigns authorization to create planning and data entry layouts.
		02	Change Assigns authorization to change planning and data entry layouts.
		03	Display Assigns authorization to display planning and data entry layouts.
		29	Display saved data Assigns authorization for the layout used to display data.
		79	Enter Assigns authorization to enter and modify data with the layout.
K_ KC_HI (EC-EIS Authorizations for Hierarchies)	• CFAPPLC (Application class for DD objects (not used)) • CFFIENM (Field Name) • CFHVERS (Hierarchy variant) • ACTVT (Activity)	01	Create or generate
		02	Change
		03	Display
		06	Delete
K_ KC_PRC (EC-EIS: Authorization for Presentation of Form)	• CFASPET (Aspect (application area)) • CEFORM (Form) • ACTVT (Activity)	01	Create or generate Assigns authorization to create a form.
		02	Change Assigns authorization to change a form.
		03	Display Assigns authorization to display a form.
		16	Execute Assigns authorization to use a form in the information system.

Authorization Object	Field	Value	Description
K_ KC_DSK (EC-EIS: Authorization for Structures and Key Figures)	• CFASPET (Aspect (application area)) • CFAPPLC (Application class for DD objects (not used)) • CFOKCOD (EC-EIS/BP function code) • TCD (Transaction Code)		
K_ KC_DS (EC-EIS: Authorizations for Data Structure Maintenance)	• CFASPET (Aspect (application area)) • CFKYRSP (Application) • CFOKCOD (EC-EIS/BP function code) • TCD (Transaction Code)		Assigns authorization for maintaining and displaying data structure and key figures.
K_ KC_DB (EC-EIS: Authorizations for the Data Basis)	• CFASPET (Aspect (application area)) • CFRECTY (Record type) • CFVERSO (Data area (previously version)) • CFPERDE (Period) • CFVALTY (Value type) • CFOKCOD (EC-EIS/BP function code) • TCD (Transaction Code)		
K_ KC_FC (EC-EIS: Function Code Authorization)	• ACTVT (Activity	01	Create or generate
		02	Change
		03	Display
		06	Delete
		16	Execute
K_PCAI_UEB (EC-PCA: Actual Data Transfer)	• KOKRS (Controlling Area)		Assigns authorization to transfer actual data.
K_PCAD_UM (EC-PCA: Assessment/Distribution)	• GLRRCTY (Record Type) • ACTVT (Activity)	01	Create or generate Assigns authorization to create cycles.

Authorization Object	Field	Value	Description
		02	Change Assigns authorization to change cycles.
		03	Display Assigns authorization to display cycles and to obtain an overview of assessments.
		06	Delete Assigns authorization to delete cycles.
		16	Execute Assigns authorization to perform assessment and distribution.
K_PCAB_DEL (EC-PCA: Delete Transaction Data)	• GLRLDNR (Ledger)		Assigns authorization to delete transaction data for profit centers.
K_PCAF_UEB (EC-PCA: FI Data Transfer)	• BUKRS (Company Code)		
K_PCAL_GEN (EC-PCA: Generate and activate ledger)	• KOKRS (Controlling Area) • ACTVT (Activity)	03	Display Assigns authorization to display ledger settings.
		62	Create automatic ledger Assigns authorization to create automatic ledger.
		63	Activate Assigns authorization to activate profit center ledger.
		64	Generate Assigns authorization to regenerate a ledger.
K_PCAM_UEB (EC-PCA: MM Data Transfer)	• ACTVT (Activity)	90	Copy Assigns authorization to transfer data from materials management (MM).

Authorization Object	Field	Value	Description
K_PCAP_UEB (EC-PCA: Plan Data Transfer)	• KOKRS (Controlling Area) • CEVERSN (Version) • CEGJAHR (Fiscal Year)		Assigns authorization to transfer plan data to profit centers.
K_PCAP_SET (EC-PCA: Planning Hierarchy)	• KOKRS (Controlling Area) • ACTVT (Activity)	01	Create or generate Assigns authorization to create profit center hierarchies.
		02	Change Assigns authorization to change profit center hierarchies.
		03	Display Assigns authorization to display profit center hierarchies.
		06	Delete Assigns authorization to delete profit center hierarchies.
K_ PCAS_PRC (EC-PCA: Profit Centers)	• KOKRS (Controlling Area) • ACTVT (Activity)	01	Create or generate Assigns authorization to create profit centers.
		02	Change Assigns authorization to change profit centers and time-based fields.
		03	Display Assigns authorization to display profit centers and the master data index.
		06	Delete Assigns authorization to delete profit centers.
		21	Transport Assigns authorization to transport Customizing settings.
		42	Convert to DB Assigns authorization to convert line items.
		63	Activate Assigns authorization to activate inactive profit centers.

Authorization Object	Field	Value	Description
Activate Assigns authorization to activate inactive profit centers.	• KOKRS (Controlling Area)		Assigns authorization to realign profit center data for retroactive changes to profit center assignments in CO master data.
K_PCA (EC-PCA: Responsibility Area, Profit Center)	• RESPAREA (CO-OM Responsibility Area) • CO_ACTION (Actions for CO-OM Authroization Check) • KSTAR (Cost Element)		
K_PCAS_UEB (EC-PCA: SD Data Transfer)	• ACTVT (Activity)	90	Copy Assigns authorization to transfer data from sales and distribution (SD).
K_PCAR_SRP (EC-PCA: Standard Reports and Datasets)	• GLRLDNR (Ledger) • ACTVT (Activity)	02	Change
		07	Activate, generate Assigns authorization to generate profit center reports.
		16	Execute Assigns authorization to execute profit center reports.
		42	Convert to DB Assigns authorization to convert profit center reports.
		60	Import Assigns authorization to import standard reports and datasets.
		61	Export Assigns authorization to export standard reports and datasets.
K_PCAR_REP (EC-PCA: Summary and Line Item Reports)	• BUKRS (Company Code) • PRCTR (Profit Center) • KSTAR (Cost Element) • ACTVT (Activity)	01	Create or generate
		02	Change
		03	Display Assigns authorization to display documents.
		06	Delete

Authorization Object	Field	Value	Description
		27	Display totals records Assigns authorization to carry out reporting of summary records.
		28	Display line items Assigns authorization to carry out reporting of line items.
		29	Display saved data Assigns authorization to display saved data.
		76	Enter Assigns authorization to create documents.
K_ML_MGV (Material Ledger: Master Data of Quantity Structure Tool)	• ACTVT (Activity) • WERKS (Plant)	01	Create or generate
		02	Change
		03	Display
K_KEPL_TC (Profit Planning)	• ACTVT (Activity)	02	Change Assigns authorization to change and delete plan data.
		03	Display Assigns authorization to display plan data.
		24	Archive Assigns authorization to archive plan data.
		65	Reorganize Assigns authorization to reorganize long texts for plan data.
		B3	Derive Assigns authorization to carry out characteristic derivation before authroization checked for CO-PA authorizations.

Authorization Object	Field	Value	Description
K_KEPL_FR (Profit Planning: Initial Screen)	• CEERKRS (Operating concern) • ACTVT (Activity)	02	Change
		03	Display
		16	Execute
		21	Transport
		GL	General overview
K_KEI_TC (Profitability Analysis: Actual Data)	• ACTVT (Activity)	01	Create or generate Assigns authorization to create line items.
		02	Change Assigns authorization to perform periodic valuation or top-down actual distribution.
		03	Display Assigns authorization to display line items.
		06	Delete Assigns authorization to delete the data in the error file CEERROR.
		24	Archive Assigns authorization to archive line items.
K_KEKD_TC (Profitability Analysis: Conditions)	• ACTVT (Activity)	01	Create or generate Assigns authorization to create condintion tables and pricing reports.
		02	Change Assigns authorization to change condintion tables and pricing reports.
		03	Display Assigns authorization to display condintion tables and pricing reports.

Authorization Object	Field	Value	Description
		16	Execute Assigns authorization to execute condition lists.
K_KED_UM (Profitability Analysis: Cost Center Assessment)	• CEERKRS (Operating concern) • CEPLIKZ (Plan/Actual Indicator) • ACTVT (Activity)	01	Create or generate Assigns authorization to create cycles.
		02	Change Assigns authorization to change and delete cycles.
		03	Display Assigns authorization to display cycles.
		16	Execute Assigns authorization to execute assessments.
		58	Display takeover Assigns authorization to display an overview of cost center assessments.
K_KER_TC (Profitability Analysis: Derivation Rule Values)	• ACTVT (Activity)	01	Create or generate
		02	Change Assigns authorization to change derivation rules.
		03	Display Assigns authorization to display derivation rules.
K_KES_TC (Profitability Analysis: Derivation Strategy)	• ACTVT (Activity)	01	Create or generate
		02	Change Assigns authorization to change derivation strategies.
		03	Display Assigns authorization to display derivation strategies.

Authorization Object	Field	Value	Description
K_KEA_ALE (Profitability Analysis: Distribution)	• CEERKRS (Operating concern) • ACTVT (Activity)	01	Create or generate
		02	Change
		03	Display
		16	Execute
		64	Generate
K_KEA_TC (Profitability Analysis: Maintain Operating Concern)	• ACTVT (Activity)	01	Create or generate Assigns authorization to create operating concerns.
		02	Change Assigns authorization to change operating concerns.
		03	Display Assigns authorization to display operating concerns.
		06	Delete Assigns authorization to delete operating concerns.
		60	Import Assigns authorization to import operating concerns.
		67	Translate Assigns authorization to translate operating concerns.
		D1	Copy Assigns authorization to copy operating concerns.
K_KEA_NET (Profitability Analysis: Realignments)	• CEERKRS (Operating concern) • ACTVT (Activity)	01	Create or generate Assigns authorization to create, change, and test realignments.
		03	Display Assigns authorization to display and test realignments.

Authorization Object	Field	Value	Description
		16	Execute Assigns authorization to execute realignments including scheduling and starting background jobs.
K_KEA_ERG (Profitability Analysis: Set Operating Concern)	• CEERKRS (Operating concern)		
K_KEDT_TC (Profitability Analysis: Transfer Data to CO-PA)	• ACTVT (Activity)	02	Change Assigns authorization to customize the transfer of data.
		16	Execute Assigns authorization to transfer external actual data and plan data and post SD billing data.
		58	Display takeover
K_KEB_BER (Profitability Report: Authorization Objects)	• CEERKRS (Operating concern) • ACTVT (Activity)	02	Change
		03	Display
K_KEB_RC (Profitability Report: Forms)	• CEERKRS (Operating concern) • CEFORM (Form) • ACTVT (Activity)	01	Create or generate
		02	Change
		03	Display
		21	Transport
		60	Import
K_KEB_REP (Profitability Report: Report Name)	• CEERKRS (Operating Concern) • CEREPID (Report) • ACTVT (Activity)	01	Create or generate Assigns authorization to create reports.
		02	Change Assigns authorization to change reports including saving the report structure from the list.
		03	Display Assigns authorization to display reports.

Authorization Object	Field	Value	Description
		04	Print, edit messages Assigns authorization to print reports.
		16	Execute Assigns authorization to execute reports.
		21	Transport Assigns authorization to transport reports.
		28	Display line items Assigns authorization to execute reports and display line items from the report list.
		32	Save Assigns authorization to save the report list with data.
		60	Import Assigns authorization to import reports from client 000.
		61	Export Assigns authorization to export reports.
		L0	All functions
		L1	Function range level 1
		L2	Function range level 2
K_KEB_TC (Profitability Reports)	• ACTVT (Activity)	01	Create or generate Assigns authorization to create reports and change key figure scheme.

Authorization Object	Field	Value	Description
		02	Change Assigns authorization as follows: • To change and delete reports • Test monitor for profitability reports • Assign a hierarchy for account-based CO-PA • Maintain variables • Maintain the report tree
		03	Display Assigns authorization to display reports.
		16	Execute Assigns authorization to execute reports.
		65	Reorganize Assigns authorization to reorganize the following: • Report data • Reports • Forms • Layouts
		66	Refresh Assigns authorization to update reports and schedule variant groups.
		B3	Derive Assigns authorization to carry out characteristic derivation before authorization checks for CO-PA authorizations.

Authorization Object	Field	Value	Description
K_KC_DB_VS (SAP-EIS Authorization for Data Basis Version & Plan/Act Ind.)	• CFASPET (Aspect (application area)) • CFVERSION (Version) • CFPLANT (Plan/Act. indicator (EC-EIS/EC-BP)) • CFOKCOD (EC-EIS/BP function code)		Assigns authorization for the aspect, version, and plan/actual indicator.
K_KC_PR (SAP-EIS: Authorization for Presentation)	• CFHIEID (User group) • CFLFDID (Sequence number for hierarchical node) • CFREPID (Report) • CFJDEST (Stroage place of SAP-EIS report) • CFOKCOD (EC-EIS/BP function code) • TCD (Transaction Code)		
K_KC_PBR (SAP-EIS: Authorization for Presentation Objects)	• CFASPET (Aspect (application area)) • ACTVT (Activity)	02	Change Assigns authorization to create and change an authorization object.
		03	Display Assigns authorization to display an authorization object.
K_TEST (Test)	• ACTVT (Activity)		
K_TP_VALU (Transfer Price Valuations)	• KOKRS (Controlling Area) • VALUTYP (Valuation View) • ACTVT (Activity)	02	Change Assigns authorization to change the valuation view.
		03	Display Assigns authorization to display the valuation view.
		10	Post

The table below shows the security-relevant authorization objects that are used by the Controlling component but are only needed for industry solutions.

Standard Authorization Objects

Authorization Object	Field	Value	Description
K_PRICE001 (Authorization for Price Maintenance, Catch Weight Solution)	• BUKRS (Company Code) • WERKS (Plant) • CWPRICLABL (Price Type) • ACTVT (Activity)	02	Change
		03	Display
K_PRS_LS (CO Authorization for Prof. Services Lean Staffing)	• PRCTR (Profit Center) • ACTVT (Activity)	02	Change
		03	Display
		06	Delete

The table below shows the security-relevant authorization objects that are used by the Controlling component but are only needed for industry solutions.

Standard Authorization Objects

Authorization Object	Field	Value	Description
K_PEP (CO Authorization Object for Period-End Partner (PEP))	• ACTVT (Activity)	06	Delete Assigns authorization to delete log entries in the Period-End Partner (PEP).
		13	Execute
K_MLNUSER (CO Material Ledger: Individual settlement; (no longer used))	• BWKEY (Valuation area)		Assigns authorization to close the material ledger for specific materials and display material ledger master data.
K_MLPUSER (CO Material Ledger: Plant settlement (no longer used))	• BWKEY (Valuation area)		Assigns authorization to close the material ledger for a plant and carry out exact analyses of data.

For general information on the authorizations in Controlling, see the documentation for Controlling on the *SAP Help Portal* at http://help.sap.com under *Methods in Controlling* > *Authorizations and under Accounting* > *Controlling (CO)* > *Profitability Analysis (CO-PA)* > *Information System* > *Authorization Objects in the Information System*. Information on the authorizations for the *Controlling functions* in *Manager Self-Service (MSS)* and for the role of the *Business Unit Analyst (BUA)* can be found in this Security Guide under *Cross-Application Components* and then Self-Services.

Critical Combinations

The critical combinations for Controlling are as follows:

- The roles for Controlling are based on the area menus rather than on U.S. Sarbanes-Oxley Act compliance.
- The master data folders in each transaction should be assigned to a master data officer rather than to a controlling end user to ensure the integrity of the data.
- In the planning transaction, authorizations can be assigned to many users.
- In addition to maintaining authorizations for managers, you should consider using the personalization framework for manager self-service.

The table below shows the roles that also contain authorization for logistics.

Standard Authorization Objects that Contain Authorization for Controlling and Logistics

SAP_EP_RW_CO_KKAM	FI - CO - Product Cost by Sales Order
SAP_EP_RW_CO_KKPM	FI - CO - Product Cost by Period
SAP_EP_RW_CO_KKSM	FI - CO - Product Cost by Order
SAP_EP_RW_CO_CK00	FI - CO - Product Cost Planning

12.2.2.2 Profit Center Accounting (EC-PCA)

Important SAP Notes

The following composite SAP Note contains important information about the security of the *Profit Center Accounting* (EC-PCA) component:

Title	SAP Note
Composite SAP note: Security of Enterprise Controlling	1518587

Authorizations

Standard Roles

The following table shows the standard roles that are used by the component.

Role	Description
SAP_AUDITOR_BA_EC_PCA	AIS – Profit Center Accounting

Role	Description
SAP_AUDITOR_BA_EC_PCA_A	AIS – Profit Center Accounting (Authorizations)
SAP_EC_PCA_ARCHIVING	Profit Center Accounting Archiving
SAP_EC_PCA_MODEL	Maintain Cycles for Assessment, Distribution, and Reposting (EC-PCA)
SAP_EC_PCA_MODEL_TP_DISPLAY	Display Transfer Prices
SAP_EC_PCA_MODEL_TP_MAINTAIN	Maintain Transfer Prices
SAP_EC_PCA_OBJECT_DISPLAY	Display Profit Center Master Data
SAP_EC_PCA_OBJECT_MAINTAIN	Maintain Profit Center Master Data
SAP_EC_PCA_PEREND	Period-End Closing in Profit Center Accounting
SAP_EC_PCA_PEREND_POSTINGS	Data Entry for Profit Center Accounting
SAP_EC_PCA_PLAN_CLOSING	Plan Closing in Profit Center Accounting
SAP_EC_PCA_PLANNING	Planning in Profit Center Accounting
SAP_EC_PCA_REPORT	Profit Center Accounting – Line Items and Totals Records
SAP_EC_PCA_REPORT1	Profit Center Accounting – Drilldown Reports
SAP_EC_PCA_REPORT2	Profit Center Accounting – Report Painter Reports
SAP_EC_PCA_REPORT3	Profit Center Accounting – Reports from Other Components

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by the component.

Authorization Object	Description
K_PCA	EC-PCA: Responsibility Area, Profit Center
K_PCAB_DEL	EC-PCA: Delete Transaction Data
K_PCAD_UM	EC-PCA: Assessment/Distribution
K_PCAF_UEB	EC-PCA: FI Data Transfer
K_PCAI_UEB	EC-PCA: Actual Data Transfer
K_PCAL_GEN	EC-PCA: Generate and Activate Ledger
K_PCAM_UEB	EC-PCA: MM Data Transfer

Authorization Object	Description
K_PCAP_SET	EC-PCA: Planning Hierarchy
K_PCAP_UEB	EC-PCA: Plan Data Transfer
K_PCAR_REP	EC-PCA: Summary and Line Item Reports
K_PCAR_SRP	EC-PCA: Standard Reports and Datasets
K_PCAS_PRC	EC-PCA: Profit Center
K_PCAS_UEB	EC-PCA: SD Data Transfer
K_PCA_REAL	EC-PCA: Realignment for PrCtr Assignments to CO Master Data

12.2.2.3 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).

12.2.2.3.1 Communication Destinations

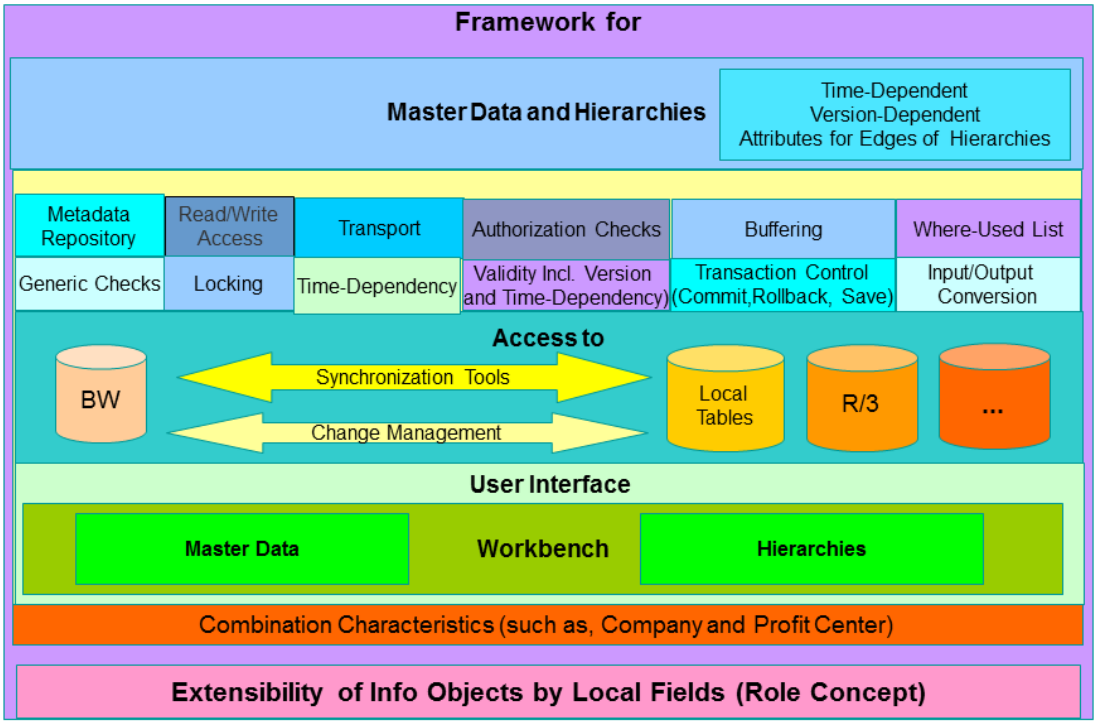
Technical users are required for communication over ALE, for batch reporting, and for third-party providers that access Controlling data.

12.2.3 Master Data Framework

12.2.3.1 Technical System Landscape

Use

The following graphic gives an overview of the technical system landscape for the *Master Data Framework* .



For more information about the technical system landscape, see the sources listed in the table below.

Subject	Guide/Tool	SAP Service Marketplace
Technical description of *Master Data Framework* and the underlying technical components, such as *SAP NetWeaver*	Master Guide	service.sap.com/instguides
Technical configuration High availability	Technical Infrastructure Guide	service.sap.com/ti
Security		service.sap.com/security

12.2.3.2 Authorizations

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by *Master Data Framework*.

Authorization Object	Description
R_UGMD_CHA	Master data access for all types of characteristics
R_UGMD_SNG	Master data access on the level of single values of combination characteristics
S_TABU_LIN	Master data access on the level of individual characteristics
FB_SRV_DMS	Authorization for data model synchronization (change monitor)
FB_SRV_GC	Authorization for *MDF Garbage Collector*

The authorization objects listed above are also described in the system documentation.

12.2.3.3 Communication Channel Security

Use

ERP and *Business Information Warehouse* (*SAP BW*) communicate with each other using RFC within *Master Data Framework* .

RFC connections can be protected using Secure Network Communications (SNC).

For more information, see *Transport Layer Security* in the *SAP NetWeaver* Security Guide.

12.2.4 Joint Venture Accounting

12.2.4.1 Authorizations

Standard Roles

The table below shows the standard roles that are used by JVA.

Role	Description
SAP_EP_RW_GJVP	RW - Joint Venture Accounting

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by JVA.

Authorization Object	Description
J_JVA_CUS	Joint Venture Accounting: Customizing
J_JVA_JOA	Joint Venture Accounting: Joint Operating Agreement Master
J_JVA_PRC	Joint Venture Accounting: Processing
J_JVA_REP	Joint Venture Accounting: Reporting
J_JVA_VNT	Joint Venture Accounting: Venture Master

12.2.4.2 Communication Channel Security

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to application server	DIAG	All application data	For example, passwords, business data, credit card information
Front-end client using a Web browser to application server	HTTP(S)	All application data	For example, passwords, business data, credit card information
Application server to application server	RFC, HTTP(S)	Integration data	Business data, credit card information

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.

12.2.5 Receivables Management

12.2.5.1 Authorizations in Settlement Management

Settlement uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Field	Value	Description
`W_WBRC_CR`	*Reason for Complaint*	**01** Add or create complaints **02** Change complaints **03** Display complaints **16** Execute (process complaints) **A3** Change status of complaints manually	Authorization for complaint reason

Authorization Object	Field	Value	Description
W_WBRK_FKA	*Settlement Document Type*	**01** Add or create documents **02** Change documents **03** Display documents **04** Print, edit messages **24** Archive documents **25** Reload documents from archive **43** Release documents to Accounting (*) **85** Cancel documents that have been forwarded to Accounting (*) **99** Create settlement document lists	Authorization for settlement document type
W_WBRK_ORG	• *Company Code* • *Purchasing Organization* • *Purchasing Group* • *Sales Organization* • *Distribution Channel* • *Division*	**01** Add or create documents **02** Change documents **03** Display documents **04** Print, edit messages **24** Archive documents **25** Reload documents from archive **43** Release documents to Accounting (*) **85** Cancel documents that have been forwarded to Accounting (*) **99** Create settlement document lists	Authorization for organizational data
WLF_IV	*Settlement Document List Type*	**01** Create or generate **03** Display	Clearing Workbench

Authorization Object	Field	Value	Description
W_COCO	*Condition Contract Type*	**01** Add or create documents **02** Change documents **03** Display documents **04** Print, process messages **24** Archive documents **25** Reload documents from archive **66** Apply condition contract retrospectively to posted invoices	Authorizations for condition contract
W_COCO_ORG	• *Sales Organization* • *Distribution Channel* • *Division* • *Purchasing Organization* • *Purchasing Group*	**01** Add or create documents **02** Change documents **03** Display documents **04** Print, process messages **43** Release **84** Settle	Authorizations for condition contract organizational data

(*) To check this activity, you must explicitly activate the check as required.

12.3 Manufacturing

12.3.1 Authorizations in Manufacturing

Manufacturing 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Roles: Basic Data

Role	Description
SAP_PP_BD_RTG_MAINTAIN	Work Scheduling - Maintenance
SAP_PP_BD_WKC_DISPLAY	Work Center Display
SAP_PP_BD_WKC_MAINTAIN	Work Center Maintenance
SAP_PP_MATERIAL_MANAGEMENT	Materials Management Production
SAP_PP_PS_PRT	Project System – Production Resources/Tools
SAP_LO_PP_RTG_DISPLAY	Routing Display
SAP_LO_PP_RTG_MAINTAIN	Routing Maintenance
SAP_LO_PP_WRKC_DISPLAY	Work Center Display
SAP_LO_PP_WRKC_MAINTAIN	Work Center Maintenance

Roles: Capacity Planning (PP-CRP)

Role	Description
SAP_PP_CAPA_PLAN	Plan Capacities
SAP_PP_CAPA_PLAN_EVAL	Evaluate Capacity Planning

Roles: Kanban (PP-KAB)

Role	Description
SAP_PP_KAB_CONTROL	KANBAN Control
SAP_PP_KAB_REPORTING	KANBAN Evaluation

Roles: Production Planning (PP-MP)

Role	Description
SAP_PP_MP_FORECAST	Material Forecast
SAP_PP_MP_LONG_TERM_PLANNING	Long-term planning

Role	Description
SAP_PP_MP_MPS_PLANNING	Master Production Scheduling

Roles: Material Requirements Planning (PP-MRP)

Role	Description
SAP_PP_MRP_COORDINATION	MRP PP - Coordination
SAP_PP_MRP_EVALUATIONS	MRP PP - Evaluation
SAP_PP_MRP_MASTER_DATA	MRP PP – Master Data
SAP_PP_MRP_PLANNED_ORDER	MRP PP – Planned Order
SAP_PP_MRP_PLANNING	MRP PP – Planning Execution

Roles: Production Orders

Role	Description
SAP_PP_SFC_CONFIRMATIONS	Production Order - Confirmations
SAP_PP_SFC_GM	Production Order – Goods Movements
SAP_PP_SFC_MAT_MANAGEMENT	Production Order – Materials Management
SAP_PP_SFC_OCM	Production Order - Order Change Management
SAP_PP_SFC_ORDER_EXCEPTIONS	Production Order – Reprocessing
SAP_PP_SFC_ORDERS	Production Order – Processing
SAP_PP_SFC_PERFORMANCE	Production Order – Production Information System
SAP_PP_SFC_PRODUCTION_OPERATOR	Production Operator in Production
SAP_PP_SFC_PRT	Production Order – Production Resource/Tool
SAP_PP_SFC_WM	Production Order - Warehouse Management

Roles: Repetitive Manufacturing (PP-REM)

Role	Description
SAP_PP_REM_CONFIRMATION	Repetitive Manufacturing - Backflushing
SAP_PP_REM_MASTERDATACHANGE	Repetitive Manufacturing – Change Master Data

Role	Description
SAP_PP_REM_MASTERDATADISPL	Repetitive Manufacturing – Display Master Data
SAP_PP_REM_PLANNING	Repetitive Manufacturing - Planning
SAP_PP_REM_PRODUCTION	Repetitive Manufacturing - Production
SAP_PP_REM_REPORTING	Repetitive Manufacturing - Evaluations

Roles: Process Industries (PP-PI)

Role	Description
SAP_PP_PI_BATCH_RECORD_	Edit Batch Record
SAP_PP_PI_BATCH_RECORD_SUPER	Approve Batch Record
SAP_PP_PI_CAPA_EVAL_STD	Perform Capacity Evaluations
EXP SAP_PP_PI_CAPACITY_EXP	Edit Capacity
SAP_PP_PI_CTRL_RECIPE_EXP	Monitor Control Recipe
SAP_PP_PI_CUST_PROCMGMT	Customizing for Process Management
SAP_PP_PI_DOWNTIME_EXP	Record Downtime
SAP_PP_PI_DOWNTIME_SUPER	Settings for Downtimes
SAP_PP_PI_GOODS_MOVE_EXP	Enter Goods Movement for Order
SAP_PP_PI_GOODS_MOVE_HU_EXP	Enter Goods Movements with Handling Units
SAP_PP_PI_GOODS_MOVE_HU_SUPER	Cancel Goods Movements with Handling Units
SAP_PP_PI_MA_BATCH_REC_WL_CUM	MiniApp: Worklist for Batch Records - Accumulated
SAP_PP_PI_MA_PI_SHEET_WL_CUM	MiniApp: Worklist for PI Sheets - Accumulated
SAP_PP_PI_MA_PROC_ORDER_WL_CUM	MiniApp: Worklist for Process Orders - Accumulated
SAP_PP_PI_MASTER_RECIPE_EXP	Edit Master Recipe
SAP_PP_PI_MASTER_RECIPE_STD	Display Master Recipe
SAP_PP_PI_MAT_STAGING_EXP	Execute Material Staging for Order
SAP_PP_PI_MAT_STAGING_STD	Display Material Staging for Order
SAP_PP_PI_MFG_COCKPIT_1_EXP	Edit Manufacturing Cockpit for Manager/Engineer

Role	Description
SAP_PP_PI_MFG_COCKPIT_2_EXP	Edit Manufacturing Cockpit for Plant Manager
SAP_PP_PI_MPARTS_INFO_STD	Evaluate Missing Parts Info System
SAP_PP_PI_ORDER_CONF_EXP	Enter Order Confirmation
SAP_PP_PI_ORDER_CONF_STD	Display Order Confirmation
SAP_PP_PI_ORDER_CONF_SUPER	Correct Order Confirmations
SAP_PP_PI_ORDER_INFO_STD	Evaluate Order Info System
SAP_PP_PI_ORDER_RECORD_EXP	Store Order Record
SAP_PP_PI_ORDER_RECORD_STD	Display Order Record
SAP_PP_PI_PI_SHEET_EXP	Maintain PI Sheet
SAP_PP_PI_PI_SHEET_SUPER	Check PI Sheet and Set to “Technically Complete”
SAP_PP_PI_PROC_MESSAGE_EXP	Edit Process Message
SAP_PP_PI_PROC_ORDER_EXP_CHNG	Change Process Order
SAP_PP_PI_PROC_ORDER_EXP_CREA	Create Process Order
SAP_PP_PI_PROC_ORDER_STD	Display Process Order
SAP_PP_PI_PROD_CAMPAIGN_EXP	Edit Production Campaign
SAP_PP_PI_PROD_CAMPAIGN_STD	Display Production Campaign
SAP_PP_PI_PROD_VERSION_EXP	Edit Production Version
SAP_PP_PI_PROD_VERSION_STD	Display Production Version
SAP_PP_PI_RESOURCE_EXP	Edit Resource
SAP_PP_PI_RESOURCE_STD	Display Resource
SAP_PP_PI_RESOURCE_SUPER	Resource Settings
SAP_PP_PI_SF_INFO_STD	Evaluate Shop Floor Information System
SAP_PP_PI_STD_TEXT_EXP	Edit Standard Text

Roles: Plant maintenance (PM)

Role	Description
SAP_SR_THTECHOB_TAKEOVER_1	NWBC Role for Takeover of Technical Objects
SAP_SR_THTECHOB_HANDOVER_1	NWBC Role for Handover of Technical Objects
SAP_COCKPIT_EAMS_GENERIC_FUNC	Generic EAM Functions
SAP_COCKPIT_EAMS_MAINT_WORKER	Maintenance Worker

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
C_AENR_BGR	CC Change Master - Authorization Group
C_AENR_ERW	CC Eng. Chg. Mgmt. Enhanced Authorization Check
C_AENR_RV1	CC Engineering change mgmt - revision level for materials
C_AENR_RV2	CC Engineering Change Mgt - revision level for documents
C_AFFW_TWK	CIM: Reworking error records from autom. goods movements
C_AFKO_ATY	CIM: Order category
C_AFKO_AWA	CIM: Authorization for Prod.Order/Order Type/Plant/Activity
C_AFKO_AWK	CIM: Plant for order type of order
C_AFRU_AWK	CIM: Confirmation
C_ARPL_ART	CIM: Work center category
C_ARPL_WRK	CIM: Work center- plant
C_AUTO_JIT	ISAUTO_JIT: Sequenced JIT Calls (seqJC)
C_BACKFL	REM: Backflushing
C_COCF_SRA	Shift Report - Work Center
C_COCF_SRH	Shift Report - Work Center Hierarchy
C_COOPC1	OPC Interface: Access to OPC Items

Authorization Object	Description
C_COOPC2	OPC Interface: Access to Events and Alarms
C_CREC_WRK	PP-PI: Control Recipe - Plant CIM: Capacity leveling
C_CREX_WRK	PP-PI: External Control Recipe Execution (PI-PCS)
C_CRFH_BRG	CIM: Production resources/tools master - authorization group
C_CRPI_BER	PP-PI: Authorizations for PI Sheet
C_EVAL_WRK	PP-PI: Process Message Evaluation / Evaluation Versions
C_FVER_WRK	PP-PI: Production Version - Plant
C_HU_PROD	Packing in Production (HU Creation)
C_JIT_CALL	PP-FLW JIT Calls
C_JIT_OUT	IS-A-JIT: JIT Outbound Calls
C_KANBAN	PP KANBAN Processing
C_KAPA_ABG	CIM: Capacity leveling
C_KAPA_PLA I	CIM: Capacity planning
C_LINE	LD: Processing Lines
C_MESS_WRK	PP-PI: Process Messages - Plant
C_PCMP	PP-PI: Production Campaign
C_POI	Authorization Object for Production Optimization Interface
C_PPBD	Authorizations for Planned Independent Requirements
C_PPBD_REO	Demand Management Reorg. - Activities
C_PRLG_WRK	PP-PI: Entry in Process Message Record
C_PROCCHAR	PP-PI: Ext. Access to Message/Instruction Characteristics
C_RMSF_DVW	RM-FRM: Formula Views
C_RMSF_MOD	RM-FRM: Formula Modeling
C_RMSLWUI	Authorization Check for Label
C_RMSL_LBL	Authorization Check for Label

Authorization Object	Description
C_RMSR_BB	Building Blocks
C_RMSR_CR	Calculation Rules in Process Parameters
C_RMSR_RC	Access to Recipes
C_RMSR_RS	Change Recipe Status
C_RMST_LAY	Managing Output Layouts
C_RMS_MCH	Authorization for Mass Changes to Data
C_RMX_CI	Trial Management: Access to Customer-Specific Fields
C_RMX_TASK	Monitor Tasks in Trial Management
C_RMX_TRIA	Authorization Check for Trials
C_ROUT	Authorizations for Routings
C_ROUT_MAT	Update Material Master from Routings
C_SAFK	REM: Repetitive Manufacturing
C_SEQUENCE	LASP: Sequencing
C_SPEC_BGR	Specification System: Authorization Object
C_STUE_BER	CS BOM Authorizations
C_STUE_MAS	CS BOMs - Mass changes
C_STUE_NOH	CS Authorization to process BOMs without a change number
C_STUE_WRK	CS BOM Plant (Plant Assignments)
C_VARLIST	Authorization for Objects in Variable Lists

12.3.2 Production Engineering

12.3.2.1 Authorizations for Production BOM Management

Production BOM Management 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Role	Description
SAP_BR_PRODN_ENG_DISC	Production Engineer - Discrete Manufacturing During the product engineering phase, the product engineer designs and develops products which involves the designing of new products or product lines to take advantage of current process technology and to improve quality and reliability. Or, an existing product has to be changed due to changing market or customer requirements. The result of this product phase is drawings and a list of all the parts required to produce the product. This list is the bill of material. This business role is required for discrete manufacturing.
SAP_BR_PRODN_ENG_PROC	Production Engineer - Process Manufacturing The corresponding business role required for the process industry.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Field	Value	Description
C_STUE_BER	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
	BEGRU		Authorization Group
	STLAN	1 (Production) 4 (Plant Maintenance)	BOM Usage
	STLTY	M (Material BOM)	BOM Category
C_STUE_NOH	NOHIS		Authorization to Edit BOMs without a Change Number
C_STUE_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	CSWRK		Plant
C_AENR_BGR	ACTVT	22 (Enter, Include, Assign)	Activity
	BEGRU		Authorization Group
C_AENR_ERW	ACTVT	22 (Enter, Include, Assign)	Activity
	AEFUN		Change Number Function
	AENST		Status of Change Number
	BEGRU		Authorization Group
	RLKEY		Release Key for Change Master
C_AENR_RV1	ACTVT	01 (Create or generate)	Activity
C_TCLA_BKA	KLART	023 (Batch)	Class Type
C_DRAD_OBJ	ACTVT		Activity
	DOKAR		Document Type
	DOKOB	STKO_DOC STPO_DOC	Linked SAP Object

Authorization Object	Field	Value	Description
	STATUS		Document Status

12.3.2.2 Authorizations for Master Recipe/Routing Management

Process and Master Recipe/Routing Management 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 SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Role	Description
SAP_BR_PRODN_ENG_DISC	Production Engineer - Discrete Manufacturing
SAP_BR_PRODN_ENG_PROC	Production Engineer - Process Manufacturing

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for the role: SAP_BR_PRODN_ENG_DISC (Production Engineer - Discrete Manufacturing).

Authorization Object	Field	Value	Description
C_AENR_BGR	ACTVT	22 (Enter, Include, Assign)	Activity
	BEGRU		Authorization Group

Authorization Object	Field	Value	Description
C_AENR_ERW	ACTVT	22 (Enter, Include, Assign)	Activity
	AEFUN		Change Number Function
	AENST		Status of Change Number
	BEGRU		Authorization Group
	RLKEY		Release Key for Change Master
C_ARPL_ART	AP_ART		Work Center Category
C_ARPL_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
C_FVER_WRK	ACTVT		Activity
	WERKS		Plant
C_ROUT	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	PLNTY	N (Routing)	Task List Type
	STATU		Status
	VERWE	1 (Production) 4 (Plant maintenance)	Task List Usage
	WERKS		Plant
C_STUE_BER	ACTVT	03 (Display)	Activity
	BEGRU		Authorization Group
	STLAN	1 (Production) 4 (Plant maintenance)	BOM Usage
	STLTY	K (Order BOM) M (Material BOM) S (Standard BOM)	BOM Category

Authorization Object	Field	Value	Description
C_TCLA_BKA	KLART	018 (Task List Class) 019 (Work Center Class)	Class Type

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for the role: SAP_BR_PRODN_ENG_PROC (Production Engineer - Process Manufacturing).

Authorization Object	Field	Value	Description
C_AENR_BGR	ACTVT	22 (Enter, Include, Assign)	Activity
	BEGRU		Authorization Group
C_AENR_ERW	ACTVT	22 (Enter, Include, Assign)	Activity
	AEFUN		Change Number Function
	AENST		Status of Change Number
	BEGRU		Authorization Group
	RLKEY		Release Key for Change Master
C_ARPL_ART	AP_ART		Work Center Category
C_ARPL_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
C_FVER_WRK	ACTVT		Activity
	WERKS		Plant
C_ROUT	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	PLNTY	2 (Master Recipe)	Task List Type
	STATU		Status

Authorization Object	Field	Value	Description
	VERWE	1 (Production) 4 (Plant maintenance)	Task List Usage
	WERKS		Plant
C_STUE_BER	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	BEGRU		Authorization Group
	STLAN	1 (Production) 4 (Plant maintenance)	BOM Usage
	STLTY	D (Document Structure E (Equipment BOM) K (Order BOM) M (Material BOM) S (Standard BOM) T (Functional Location BOM)	BOM Category
C_STUE_NOH	NOHIS		Authorization to edit BOMs without a change number
C_STUE_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	CSWRK		Plant
Q_GP_CODE	QCODEGRP		Code Group
	QKATART		Catalog
Q_PLN_FEAT	PLNTY	Master Recipe	Task List Type

12.3.3 Production Planning

12.3.3.1 Authorizations for Material Requirements Planning

Material Requirements Planning 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 SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Role	Description
SAP_BR_MATL_PLNR_EXT_PROC	Material Planner - External Procurement
SAP_BR_PRODN_PLNR	Production Planner

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for the roles SAP_BR_MATL_PLNR (Material Planner - External Procurement) and SAP_BR_PRODN_PLNR (Production Planner).

Authorization Object	Field	Value	Description
M_MTDI_ORG	DISPO		MRP Controller (Materialls Planner)

Authorization Object	Field	Value	Description
	MDAKT	A (MRP: Current Stock/ Requirements List) R (MRP: current material overview) B (MRP: total planning) E (MRP: single-item planning)	Activity Types in Materials Planning
	WERKS		Plant
M_PLAF_ORG	DISPO		MRP Controller (Materialls Planner)
	MDAKT	A (MRP: current stock/ requirements list) F (MRP: Firm Planned Order) H (MRP: Create Planned Order) S (MRP: MRP list, coll. display/planned order coll. conversion) U (MRP: planned order, individual conversion) V (MRP: change planned order)	Activity Types in Materials Planning
	WERKS		Plant
M_BANF_BSA	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	BSART		Purchasing Document Type
M_BANF_EKG	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKGRP		Purchasing Group

Authorization Object	Field	Value	Description
M_BANF_EKO	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKORG		Purchasing Organization
M_BANF_LGO	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
	LGORT		Storage Location
M_BANF_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
M_BEST_BSA	ACTVT	03 (Display)	Activity
	BSART		Purchasing Document Type
M_BEST_EKG	ACTVT	03 (Display)	
	EKGRP		Purchasing Group
M_BEST_EKO	ACTVT	03 (Display)	Activity
	EKORG		Purchasing Organization
M_BEST_LGO	ACTVT	03 (Display)	Activity
	WERKS		Plant
	LGORT		Storage Location
M_BEST_WRK	ACTVT	03 (Display)	Activity
	WERKS		Plant
M_LPET_BSA	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity

Authorization Object	Field	Value	Description
	BSART		Purchasing Document Type
M_LPET_EKG	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKGRP		Purchasing Group
M_LPET_EKO	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKORG		Purchasing Organization
M_LPET_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
C_AFKO_ATY	ACTVT	01 (Create or generate)	Activity
	AUTYP	10 (Production order) 40 (Process order)	Order Category
C_AFKO_AWA	ACTVT	01 (Create or generate)	Activity
	AUTYP	10 (Production order) 40 (Process order)	Order Category
	AUFART		Order Type
	WERKS		Plant
C_AFKO_AWK	WERKS		Plant
	AUFART		Order Type
V_VBAK_AAT	AUART		Sales Document Type
	ACTVT	03 (Display)	Activity

Authorization Object	Field	Value	Description
M_FCDM_ORG	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 43 (Release)	Activity
	WERKS		Plant
	DISPO		MRP Controller (Material Planner)
M_MTDI_ORG	MDAKT	P (MRP: create planning file entry)	Activity types in materials planning
	WERKS		Plant
	DISPO		MRP Controller (Material Planner)
C_PPBD	AKTTYP	A (Display) H (Add) V (Change)	Activity category in transaction (Cr/Ch/D)
	WERKS		Plant
S_PROGRAM	P_GROUP	PPH_MRP required for scheduling MRP runs PP_MRP1 required for scheduling order conversion runs	ABAP Program Authorization Group
	P_ACTION	BTCSUBMIT (Schedule programs for background processing) SUBMIT (Execute ABAP program) VARIANT (Edit variants and execute ABAP program)	User Action in ABAP Program
S_BTCH_JOB	JOBACTION	DELE (Delete Background Jobs) RELE (Release Jobs (Released Automatically When Scheduled)) SHOW(Display Job Queue)	Job operations

Authorization Object	Field	Value	Description
	JOBGROUP		Summary of jobs for a group

12.3.3.2 Authorizations for Production Planning and Detailed Scheduling

Production Planning and Detailed Scheduling uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_BR_PRODN_PLNR	Production Planner

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
C_APO_PROD	APO Authorization Object: Master Data, Products
C_APO_LOC	APO Authorization Object: Master Data, Locations
C_APO_MALO	APO Authorization Object: PP/DS, Location Product
C_APO_RES	APO Authorization Object: Master Data, Resources

Authorization Object	Description
C_APO_RELO	APO Authorization Object: PP/DS, Resource
C_APO_RESN	APO Authorization Object: Master Data, Resource Network
C_APO_VERS	APO Authorization Object: Planning Versions
C_APO_RTO	APO Authorization Object: Production Data Structure
C_APO_PPL	APO Authorization Object: PP/DS, Production Planner
C_APO_CAL	APO Authorization Object: Planning Calendar
C_APO_PCM	APO Authorization Object: Production Campaign (Manual)
C_APO_EXPR	APO Authorization Object: External Procurement Relationships
C_APO_AMON	APO Authorization Object: Alert Monitor
C_APO_SETM	APO Authorization Object: Master Data, Setup Matrices
C_APO_SETG	APO Authorization Object: Master Data, Setup Groups
C_APO_MATR	APO Authorization Object: Rules for Setup Matrix Generation
C_APO_GRPR	APO Authorization Object: Rules for Setup Group Generation
C_APO_PPC	APO Authorization Object: Production Backflush
C_APO_SSA	APO Authorization Object: Release Handling for Sales Scheduling Agreement

12.3.3.3 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 SAP NetWeaver 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 SAP NetWeaver Security Guide.

12.3.4 Manufacturing Execution for Discrete Industries

12.3.4.1 Authorizations for Production Processing

Production Processing 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 SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Role	Description
SAP_BR_PRODN_SUPERVISOR_DISC	Production Supervisor - Discrete Manufacturing
SAP_BR_PRODN_SUPERVISOR_PROC	Production Supervisor - Process Industry
SAP_BR_PRODN_OPTR_DISC	Production Operator - Discrete Manufacturing
SAP_BR_PRODN_OPTR_PROC	Production Operator - Process Industry

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for the role `SAP_BR_PRODN_SUPERVISOR_DISC` Production Supervisor - Discrete Manufacturing.

Authorization Object	Description
C_AFFW_TWK	CIM: Reworking error records from autom. goods movements
C_AFKO_ATY	CIM: Order category
C_AFKO_AWA	CIM: Authorization for Prod.Order/Order Type/Plant/Activity
C_AFKO_AWK	CIM: Plant for order type of order
C_AFRU_AWK	CIM: Confirmation
C_FVER_WRK	PP-PI: Production Version - Plant
C_KAPA_ABG	CIM: Capacity leveling
M_PLAF_ORG	Organization Levels for Planned Order Processing
M_MSEG_BWA	Goods Movements: Movement Type

Authorization Object	Description
M_MSEG_BWF	Goods Receipt for Production Order: Movement Type
M_MSEG_LGO	Goods Movements: Storage Location
M_MSEG_WWA	Goods Movements: Plant
M_MSEG_WWF	Goods Receipt for Production Order: Plant
C_NAV_PROF	Navigation Profile
C_TCLA_BKA	Authorization for Class Types
S_PROGRAM Field: P_GROUP and Value PP_SFC1 required to schedule order release runs	ABAP: Program Flow Checks
S_BTCH_JOB	Background Processing: Operations on Background Jobs
M_MTDI_ORG	Organizational Levels for Material Requirements Planning
M_MIPA_ORG	Updating Backorders

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for the role `SAP_BR_PRODN_SUPERVISOR_PROC` Production Supervisor - Process Industry.

Authorization Object	Description
S_BTCH_JOB	Background Processing: Operations on Background Jobs
S_PROGRAM Field: P_GROUP and Value PP_SFC1 required to schedule order release runs	ABAP: Program Flow Checks
C_KLAH_BKP	Authorization for Class Maintenance
C_TCLA_BKA	Authorization for Class Types
M_MSEG_BWA	Goods Movements: Movement Type
M_MSEG_BWF	Goods Receipt for Production Order: Movement Type
M_MSEG_LGO	Goods Movements: Storage Location

Authorization Object	Description
M_MSEG_WWA	Goods Movements: Plant
M_MSEG_WWF	Goods Receipt for Production Order: Plant
M_PLAF_ORG	Organization Levels for Planned Order Processing
C_AFFW_TWK	CIM: Reworking error records from autom. goods movements
C_AFKO_ATY	CIM: Order category
C_AFKO_AWA	CIM: Authorization for Prod.Order/Order Type/Plant/Activity
C_AFKO_AWK	CIM: Plant for order type of order
C_AFRU_AWK	CIM: Confirmation
C_CREC_WRK	PP-PI: Control Recipe - Plant
C_FVER_WRK	PP-PI: Production Version - Plant
C_KAPA_ABG	CIM: Capacity leveling
C_STUE_BER	CS BOM Authorizations
Q_CHAR_PRC	Recording Authorization for Insp. Results in an Operation
Q_INSP_FIN	Inspection Completion with Open Char./Insp.Pts Req. Conf.
Q_MATERIAL	Material Authorization

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for the roles `SAP_BR_PRODN_OPTR_DISC` Production Operator - Discrete Industry and `SAP_BR_PRODN_OPTR_PROC` Production Operator - Process Industry.

Authorization Object	Description
C_TCAL_BKA	Authorization for Class Types
C_NAV_PROF	Navigation Profile
M_MSEG_BWA	Goods Movements: Movement Type
M_MSEG_BWF	Goods Receipt for Production Order: Movement Type

Authorization Object	Description
M_MSEG_LGO	Goods Movements: Storage Location
M_MSEG_WWA	Goods Movements: Plant
M_MSEG_WWF	Goods Receipt for Production Order: Plant
C_AFFW_TWK	CIM: Reworking error records from autom. goods movements
C_AFKO_ATY	CIM: Order category
C_AFKO_AWA	CIM: Authorization for Prod.Order/Order Type/Plant/Activity
C_AFKO_AWK	CIM: Plant for order type of order
C_CFRU_AAWK	CIM: Confirmation
C_FVER_WRK	PP-PI: Production Version - Plant
C_KAPA_ABG	CIM: Capacity leveling

12.3.4.2 Authorizations for Repetitive Manufacturing

Repetitive Manufacturing 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Role	Description
SAP_BR_PRODN_SUPERVISOR_RPTV	Production Supervisor: Repetitive Manufacturing

Role	Description
SAP_BR_PRODN_OPTR_RPTV	Production Operator: Repetitive Manufacturing

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used for the role SAP_BR_PRODN_SUPERVISOR_RPTV (production supervisor).

Authorization Object	Field	Value	Description
C_KAPA_ABG	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete) 16 (Execute)	Activity
C_SAFK	MDAKT	V (MRP: Change planned order)	Activity types in materials planning
	WERKS		Plant
T_TCLA_BKA	KLART	013	Class type
M_MIPA_ORG	ACTVT	03 (Display)	Activity
	WERKS		Plant

The table below shows the security-relevant authorization objects that are used for the role SAP_BR_PRODN_OPTR_RPTV (production operator).

Authorization Object	Field	Value	Description
C_BACKFL	BF_CANCEL	X (Yes)	Reversing backflushes
	BF_CONCLU	1 (Decoupled confirmation) 2 (Postprocessing)	Final postings
	BF_POST	1 (Post without correction) 2 (Display BOM/routing) 3 (Change BOM/routing)	Authorization for posting/correcting

Authorization Object	Field	Value	Description
	BF_REPPT	1 (Post previous RPs subsequently) 2 (Reset RP quantities)	Reporting points (subsequent posting)
	BF_SCRAP	X (Yes)	Authorization for the scrap backflush
	BF_TYPE	B (Assembly backflush) K (Component backflush) L (Activity backflush)	Backflush types
	LGORT		Storage location
	WERKS		Plant
C_AFFW_TWK	AUTYP	10 (PP Production order) 40 (Process order)	Order category
	WERKS		Plant
M_MSEG_BWA	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	BWART	101, 102, 261, 262, 531, 532, 543, 544, 545, 546	Movement Type (Inventory Management)
M_MSEG_BWF	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	BWART	101, 102, 261, 262, 531, 532, 543, 544, 545, 546	Movement Type (Inventory Management)
M_MSEG_LGO	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
	LGORT		Storage Location
	BWART	101, 102, 261, 262, 531, 532, 543, 544, 545, 546	Movement Type (Inventory Management)

Authorization Object	Field	Value	Description
M_MSEG_WWA	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
	WERKS		Plant
M_MSEG_WWF	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
	WERKS		Plant
C_BCKFLUSH	ACTVT	24 (Archive)	Activity
		31 (Confirm)	
		A8 (Process mass data)	
	WERKS		Plant

12.3.4.3 Authorizations for Subcontracting and External Procurement

Subcontracting and External Procurement 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Role	Description
SAP_BR_PRODN_PLNR	Production Planner
SAP_BR_MATL_PLNR_EXT_PROC	Material Planner - External Procurement

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Field	Value	Description
M_MTDI_ORG	DISPO		MRP Controller (Materialls Planner)
	MDAKT	A (MRP: Current Stock/ Requirements List) R (MRP: current material overview) B (MRP: total planning) E (MRP: single-item planning)	Activity Types in Materials Planning
	WERKS		Plant
M_PLAF_ORG	DISPO		MRP Controller (Materialls Planner)
	MDAKT	A (MRP: current stock/ requirements list) F (MRP: Firm Planned Order) H (MRP: Create Planned Order) S (MRP: MRP list, coll. display/planned order coll. conversion) U (MRP: planned order, individual conversion) V (MRP: change planned order)	Activity Types in Materials Planning
	WERKS		Plant

Authorization Object	Field	Value	Description
M_BANF_BSA	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	BSART		Purchasing Document Type
M_BANF_EKG	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKGRP		Purchasing Group
M_BANF_EKO	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKORG		Purchasing Organization
M_BANF_LGO	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
	LGORT		Storage Location
M_BANF_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
M_BEST_BSA	ACTVT	03 (Display)	Activity
	BSART		Purchasing Document Type
M_BEST_EKG	ACTVT	03 (Display)	
	EKGRP		Purchasing Group
M_BEST_EKO	ACTVT	03 (Display)	Activity
	EKORG		Purchasing Organization
M_BEST_LGO	ACTVT	03 (Display)	Activity

Authorization Object	Field	Value	Description
	WERKS		Plant
	LGORT		Storage Location
M_BEST_WRK	ACTVT	03 (Display)	Activity
	WERKS		Plant
M_LPET_BSA	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	BSART		Purchasing Document Type
M_LPET_EKG	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKGRP		Purchasing Group
M_LPET_EKO	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EKORG		Purchasing Organization
M_LPET_WRK	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
C_AFKO_ATY	ACTVT	01 (Create or generate)	Activity
	AUTYP	10 (Production order) 40 (Process order)	Order Category
C_AFKO_AWA	ACTVT	01 (Create or generate)	Activity
	AUTYP	10 (Production order) 40 (Process order)	Order Category
	AUFART		Order Type
	WERKS		Plant

Authorization Object	Field	Value	Description
C_AFKO_AWK	WERKS		Plant
	AUFART		Order Type
V_VBAK_AAT	AUART		Sales Document Type
	ACTVT	03 (Display)	Activity
M_FCDM_ORG	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 43 (Release)	Activity
	WERKS		Plant
	DISPO		MRP Controller (Material Planner)
M_MTDI_ORG	MDAKT	P (MRP: create planning file entry)	Activity types in materials planning
	WERKS		Plant
	DISPO		MRP Controller (Material Planner)
C_PPBD	AKTTYP	A (Display) H (Add) V (Change)	Activity category in transaction (Cr/Ch/D)
	WERKS		Plant
S_PROGRAM	P_GROUP	PPH_MRP	ABAP Program Authorization Group
	P_ACTION	BTCSUBMIT (Schedule programs for background processing) SUBMIT (Execute ABAP program) VARIANT (Edit variants and execute ABAP program)	User Action in ABAP Program

Authorization Object	Field	Value	Description
S_BTCH_JOB	JOBACTION	DELE (Delete Background Jobs) RELE (Release Jobs (Released Automatically When Scheduled)) SHOW(Display Job Queue)	Job operations
	JOBGROUP		Summary of jobs for a group

12.3.4.4 Authorizations for Kanban

Kanban 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard role covering the most frequent business transactions. You can use this role as a template for your own roles.

Role	Description
SAP_BR_PRODN_OPTR_DISC	Production Operator - Discrete Manufacturing

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
C_TCAL_BKA	Authorization for Class Types
C_NAV_PROF	Navigation Profile
M_MSEG_BWA	Goods Movements: Movement Type
M_MSEG_BWF	Goods Receipt for Production Order: Movement Type
M_MSEG_LGO	Goods Movements: Storage Location
M_MSEG_WWA	Goods Movements: Plant
M_MSEG_WWF	Goods Receipt for Production Order: Plant
C_AFFW_TWK	CIM: Reworking error records from autom. goods movements
C_AFKO_ATY	CIM: Order category
C_AFKO_AWA	CIM: Authorization for Prod.Order/Order Type/Plant/Activity
C_AFKO_AWK	CIM: Plant for order type of order
C_CFRU_AAWK	CIM: Confirmation
C_FVER_WRK	PP-PI: Production Version - Plant
C_KAPA_ABG	CIM: Capacity leveling

12.3.4.5 Authorizations for Just-in-Time-Processing

Just-in-Time Processing (JIT) uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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

12.3.4.6 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 http://help.sap.com/s4hana_op_1610_001 ▶ *Product Assistance* ▶ *Cross Components* ▶ *Data Protection* ▶.

Relevant Application Objects and Available Deletion Functionality

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

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*.

12.3.4.7 Authorizations for Production Backflush

Production Backflush uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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

12.3.4.8 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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*.

12.3.5 Quality Management

12.3.5.1 Authorizations in Quality Management

Quality management uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_BR_QUALITY_ENGINEER	Quality Engineer
SAP_BR_QUALITY_MANAGER	Quality Manager
SAP_BR_QUALITY_PLANNER	Quality Planner
SAP_BR_QUALITY_AUDITOR	Quality Auditor
SAP_BR_CALIBRATION_TECHNICIAN	Calibration Technician

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Fields	Description	Comment
AUDIT_AUTH	Authorization Group Activities for Authorizations Audit Type	Authorizations in Audit Processing	
Q_CAT_GRP	Code Group Catalog Code Group Status	Catalog Maintenance of Code Groups and Codes	
Q_CAT_SSET	Selected Set Plant Catalog Status of Selected Set	Catalog Maintenance of Selected Sets	

Authorization Object	Fields	Description	Comment
Q_CERT_PRF	Certificate Type Transaction Code	Maintenance of Certificate Profiles	
Q_CHAR_PRC	Plant Work Center Initial Status of Inspection Characteristic (Sample) Final Status of the Inspection Characteristic (Sample)	Recording Authorization for Inspection Results in an Operation	
Q_CP	Activity Plant	Control Plan Maintenance	
Q_FMEA	Authorization Group Activities for Authorizations FMEA Type	Authorizations Within FMEA Processing	
Q_GP_CODE	Code Group Catalog	Use of Code Groups	
Q_INSPTYPE	Plant Inspection Type	Inspection Type for the Inspection Lot	
Q_INSP_FIN	Plant Inspection Type	Inspection Completion with Open Characteristics for Inspection Points Usually Requiring Confirmation	
Q_MASTERD	Authorization Group QM Basic Data Activity for QM Master Data Authorizations	Authorization for Master Data	
Q_MATERIAL	Material Authorization Group for Activities in QM Activity for QM Material Authorization Plant	Material Authorization	

Authorization Object	Fields	Description	Comment
Q_OC_CODE	Plant Work Center Selected Set of the Usage Decision Code Group of the Usage Decision Usage Decision Code Inspection Lot, Partial Lot, Single Unit, Interval	Use of Usage Decision Codes for Completion at Operation Level	
Q_PLN_FEAT	Task List Type	Maintaining Task List Characteristics for a Task List Type	
Q_QMEL	Notification Type Transaction Code Plant	Quality Notification Types	
Q_ROUT	Activity Task List Type Plant Task List Usage Status	Maintain Inspection Plan	
Q_SPC	Plant SPC Criterion	Change to Control Charts	
Q_STA_QMTB	Inspection Method Status	Maintain Inspection Methods Depending on Status	
Q_STA_QPMK	Master Inspection Characteristic Status	Maintain Master Inspection Characteristics Depending on Status	
Q_STCK_CHG	Plant Stock Type Authorizations for Stock Postings	Change Stock Posting Fields in Usage Decision Transactions	

Authorization Object	Fields	Description	Comment
Q_TCODE	Transaction Code	QM Transaction Authorization	You can use this authorization object in combination with other QM authorization objects that do not have a field for activities assigned. By assigning a concrete transaction code, you can distinguish, for example, between displaying or changing an object.
Q_UD_CODE	Plant Inspection Lot, Partial Lot, Single Unit, Interval Selected Set of the Usage Decision Code Group of the Usage Decision Usage Decision Code	Using Usage Decision Codes	
Q_VORG_MEL	Business Transaction Notification Type	Business Process Quality Notifications	
B_NOTIF_EX	Notification Type Activity category in transaction (Create/Change/Delete)	Extended Change of Notification Type	

Critical Combinations

We strongly recommend that you do not grant authorization for results recording and usage decision for the same inspection lot to one single user.

12.3.5.2 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For quality management the following services are needed for the respective Web Dynpro applications:

- QI_INSPECTIONLOT_DETAIL_APP
- QI_RECORD_RESULTS_APPL
- QI_RECORD_RESULTS_ETI_APPL

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 SAP NetWeaver Security Guide.

12.3.5.3 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	Digital signature
Quality master data replication	IDoc	Master inspection characteristics Master inspection methods Codes Inspection plan	
Communication with external subsystem for inspection	RFC, SOAP	Inspection lot data Inspection results	
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 SAP NetWeaver Security Guide.

12.3.6 Maintenance Operations

12.3.6.1 Authorizations in Plant Maintenance

Plant Maintenance uses the authorization concept provided by the SAP 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Roles for Plant Maintenance

Role	Description
`SAP_COCKPIT_EAMS_MAINT_WORKER2`	*Maintenance Worker 2* This role contains all the functions that a maintenance worker requires to carry out their work effectively and safely. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.

Role	Description
SAP_COCKPIT_EAMS_GENERIC_FUNC2	*Generic EAM Functions 2* The purpose of this role is to provide the maintenance planner with a broad range of functions necessary for planning and executing maintenance activities. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.

12.4 R&D / Engineering

12.4.1 Product Safety and Stewardship

12.4.1.1 Product Development for Discrete Industries

12.4.1.1.1 Authorizations

Product Development for Discrete Industries uses the authorization concept provided by the SAP NetWeaver AS for ABAP Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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_PPE_PS	Integrated Product and Process Engineering (iPPE): PS – iPPE Interface (Component Assignment)
C_PPE_PSI	Integrated Product and Process Engineering (iPPE): PS – iPPE Interface (Interface)
I_CCM_ACT	Configuration Control: Allows forced installation/removal
I_CCM_EBOM	Configuration Control: Allows the change of Equipment BOMs
I_CCM_STRC	Configuration Control: Allows the maintenance of structure gaps
I_IE4N	Configuration Control: Controls the usage of the various IE4N modes

12.4.1.2 Authorizations in Recycling Administration

Recycling Administration uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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

Role	Description
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	*Compliance Manager for Recycling*
SAP_ISREA_HEAD_SUSTAINABILITY	*Head of Sustainability and Environment*
SAP_ISREA_MASTERDATA_EXPERT	*Specialist for Recycling Master Data*
SAP_ISREA_PACKAGING_ENGINEER	*Packaging Engineer*
SAP_ISREA_SPECIALIST	*Specialist for Recycling Accounting*
com.sap.pct.erp.rea.financial_accountant	SAP Enterprise Portal role *Financial Accountant*
com.sap.pct.erp.rea.person_responsible_master data	SAP Enterprise Portal role *Person Responsible Master Data*
com.sap.pct.erp.rea.superadmin_masterdata	SAP Enterprise Portal role *Superadministrator Master Data*
com.sap.pct.erp.rea.compliance_manager	SAP Enterprise Portal role *Compliance Manager*
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 *Financial Accountant*
SAP_SR_REA_PERS_RESP_MD_5	Role in SAP Business Client that corresponds to the SAP Enterprise Portal role *Person Responsible Master Data*
SAP_SR_REA_SUPER_ADMIN_MD_5	Role in SAP Business Client that corresponds to the SAP Enterprise Portal role *Superadministrator Master Data*

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by Recycling Administration.

Authorization Object	Name	Description
/J7L/LDE	*REA Lean Data Entry*	Controls the authorizations for the applications for lean data entry

Authorization Object	Name	Description
J_7L_CONF	*REA: Authorization for Configuration*	Controls the authorizations for the import and export of recycling partner master data
J_7L_VARIA	*REA: Authorization for Variants*	Controls the access to master data objects in the Recycling Administration component depending on the respective variant
J_7L_CUST	*REA: Customizing*	Controls the authorizations for Customizing in the Recycling Administration component
J_7L_INFO	*REA: Information System*	Controls the authorizations for the applications in the information system of the Recycling Administration component
J_7L_PERIO	*REA: Declarations to Recycling Partners*	Controls the authorizations for declarations
J_7L_INFC	*REA: Interfaces and Batch Programs*	Controls the authorizations for programs for mass processing (background processing)
J_7L_STAMM	*REA: Master Data*	Controls the authorizations for editing master data in the Recycling Administration component

12.4.2 Product Lifecycle Management

12.4.2.1 Maintenance, Repair, and Overhaul

12.4.2.1.1 Authorizations (Specification 2000)

Specification 2000 (IS-ADEC-SPC) uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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

12.4.2.1.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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*.

12.4.2.1.3 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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*.

12.4.2.1.4 Authorizations (Manufacturer Part Number)

Manufacturer Part Number (MPN) uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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

12.4.2.1.5 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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*.

12.5 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	*Sales and Distribution*

Class	Description
LE_T	*Logistics Execution - Transportation*
LE_V	*Logistics Execution - Shipping*
WG	For Global Trade Management (GTM): *Retailing* • *Trading Contract: Authorization for Organizational Data* (W_WBHK_ORG) • *Trading Contract: Authorization for Trading Contract Type* (W_WBHK_TCT)

12.5.1 Authorizations in Sales

Sales uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver Security Guide also apply.

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

> **i** Note
>
> For more information about how to create roles, see the SAP NetWeaver Security Guide under User Administration and Authentication.

Business Roles

Business roles denote a role of a persona, for example, *Administrator* or *Internal Sales Representative*. They are an aggregation of the applications relevant for a certain persona.

In SAP S/4HANA, business roles are technically represented by single roles. They exist on the front-end server and do not contain authorizations. They serve demonstration purposes and trial use cases. You would typically create your own business roles as single roles or composite roles in the transaction PFCG. Assigning the required back-end authorizations is a separate step which is performed in the transaction in PFCG of the corresponding back-end clients.

Sales and Distribution

The following table shows the business roles used by *Sales and Distribution* (SD) as template roles:

Role	Description
SAP_BR_BILLING_CLERK	*Billing Clerk*
SAP_BR_INTERNAL_SALES_REP	*Internal Sales Representative*

Role	Description
SAP_BR_PRICING_SPECIALIST	*Pricing Specialist*
SAP_BR_SALES_MANAGER	*Sales Manager*
SAP_BR_SALES_PROCESS_MANAGER	*Order-to-Cash Process Manager*

Standard Authorization Objects

Sales and Distribution

The following table shows the main security-relevant authorization objects used by *Sales and Distribution* (SD):

Authorization Object	Description
V_KNA1_BRG	Customer: Account Authorization for Sales Areas
V_KNA1_VKO	Customer: Authorization for Sales Organizations
V_KONH_VKO	Condition: Authorization for Sales Organizations
V_KONH_VKS	Condition: Authorization for Condition Types
V_VBAK_AAT	Sales Document: Authorization for Sales Document Types
V_VBAK_VKO	Sales Document: Authorization for Sales Areas
V_VBRK_FKA	Billing: Authorization for Billing Types
V_VBRK_VKO	Billing: Authorization for Sales Organizations
POC_AUTH	Process Observer: Process Instance
POC_DEFN	Process Observer: Process Definition

Global Trade Management

The following table shows the security-relevant authorization objects used by *Global Trade Management* (GTM):

Authorization Object	Description
W_WBGT_FIX	GTM: Setup of Enhancement Table WBGT
W_WBHK_ORG	Trading Contract: Authorization for Organizational Data
W_WBHK_TCT	Trading Contract: Authorization for Trading Contract Type

Authorization Object	Description
W_WTEW	Authorizations for Trading Execution Workbench
WB2_SHD_UI	Assignments: Authorization for shadow document types

More Information

For authorization information about *Shipping* (LE-SHP), see Authorizations in Logistics Execution [page 197].

12.5.2 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 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
/SAPSLL/LEG_ARCH GTS	Archiving
/SAPSLL/LEG_LCE_APP GTS	Legal Control Export: Specialist
/SAPSLL/LEG_LCI_APP GTS	Legal Control Import: Specialist
/SAPSLL/LEG_SPL_APP GTS	Sanctioned Party List: Specialist

Role	Description
/SAPSLL/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 SAP NetWeaver Security Guide.

12.5.3 Deletion of Personal Data in Sales

Use

Applications in the line of business *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 the product assistance for SAP S/4HANA on the SAP Help Portal at http://help.sap.com/s4hana_op_1610_001 ▶ *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
Agreements	Archiving object SD_AGREEM
Condition records	Archiving object SD_COND

Application	Provided Deletion Functionality
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	• Archiving object WB2 • Report WB2_UPDATE_EOP_FROM_ARCHIVE
Campaigns	Data destruction object SD_CAMPAIGN_DESTRUCTION

Relevant Application Objects and Available EoP Functionality

Application	Implemented Solution (EoP or WUC)	Further Information
• *Sales & Distribution* (ERP_SD)	EoP check	This EoP check includes business in the areas of the following: • Sales • Billing • Delivery
• *Empties Management in SD* (ERP_SD_BIL_EM)	EoP check	This EoP check includes business in the areas of the following: • Supplier Empties data from invoice receipt • Customer Empties account for customers
• *Global Trade Management Position Management* (LO_GT_PM) • *Global Trade Management Trading Contract* (LO_GT_TC) • *Global Trade Management Trading Expenses* (LO_GT_TE) • *Global Trade Management TEW* (LO_GT_TEW)	EoP check	This EoP check includes business in *Global Trade Management* (LO-GT).

More Information

For more information about data archiving and data destruction functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at http://help.sap.com/s4hana_op_1610_001 under *Product Assistance* > *Enterprise Business Applications* > *Sales* > *Sales and Distribution (SD)*.

12.5.4 Country Specifics

12.5.4.1 China

12.5.4.1.1 Global Trade Localization for China

12.5.4.1.1.1 Authorizations

SAP Global Trade Localization for China uses the authorization concept provided by SAP Net Weaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to *SAP Global Trade Localization for China*.

The SAP NetWeaver 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 *Role Administration*.

Standard Roles

The following table shows the standard roles that are used by *SAP Global Trade Localization for China*:

Role	Description
`SAP_GTCN_TAX_REFUND_ACCOUNTANT`	A user with the tax refund accountant role can upload tax refund files; map purchase invoices and billing documents; and post tax refund differences in the system.

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by *SAP Global Trade Localization for China*:

Authorization Object	Description
F_TR_FILE	Using this authorization object, you determine which activities can be carried out with the *Tax Refund File* (GTCN_TAX_REFUND_FILE_SEARCH) program
F_TR_LIST	Using this authorization object, you determine which activities can be carried out with the *Tax Refund List* (GTCN_TR_LIST_SEARCH) program
F_TR_UPLO	Using this authorization object, you determine which activities can be carried out with the following programs: • *Upload the Tax Refund Rate Excel* (RP_GTCN_TAX_REFUND_RATE_UPLOAD) • *Maintain Tax Refund Information* (FM_TAX_REFUND_UPDATE)
F_TR_REP	Using this authorization object, you determine which activities can be carried out with the following programs: • *Tax Refund File Report* (GTCN_TAXREF_REPORT_TR_FILE) • *Tax Refund Information from Sales* (GTCN_TAXREF_REPORT_FROM_SD) • *Tax Refund Information from Purchase* (GTCN_TR_REFUND_FROM_PURCHASE) • *Tax Refund List Report* (GTCN_REFUND_LIST_REPORT_N)

12.6 Sourcing and Procurement

12.6.1 Authorizations

Purchasing, External Service Procurement, and Invoice Verification use the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_MM_PUR_ADDITIONAL_FUNC	Non-Assigned Purchasing Functions
SAP_MM_PUR_ARCHIVE	Archive Purchasing Documents
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

Role	Description
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
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

Role	Description
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
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: • 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: • 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_MAITAIN	GR/IR Clearing Account Maintenance

Role	Description
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: • Business Audit - Individual Account Closing • Profit and Loss Statement • Material Expense
SAP_AUDITOR_BA_MM_IV_A	This authorization role provides read access for the audit area: • Business Audit - Individual Account Closing • Profit and Loss Statement • Material Expense

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

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

Authorization Object	Description
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
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

Authorization Object	Description
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
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
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

Authorization Object	Description
M_RECH_SPG	Invoices: Blocking Reasons
M_RECH_UPL	Invoice: Upload
F_BKPF_BUK	Accounting Document

12.6.2 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 SAP NetWeaver 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

Authorization Object	Description
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
M_RAHM_WRK	Plant in Outline Agreement
M_RAHM_LGO	Storage Location in Outline Agreement

12.6.3 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

Authorization Object	Description
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
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

12.6.4 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 http://help.sap.com/s4hana_op_1610_001 *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`
Physical Inventory Documents	Archiving Physical Inventory Documents (MM-IM)	Archiving object `MM_INVBEL`
Invoice Documents	Archiving Invoice Documents (MM-IV)	Archiving object `MM_REBEL`
Special Stocks	Archiving Special Stock Records (LO-MD-MM)	Archiving object `MM_SPSTOCK`

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at http://help.sap.com/s4hana_op_1610_001 under *Product Assistance* *Enterprise Business Applications* *Sourcing and Procurement* *Materials Management (MM)* *Data Archiving in Materials Management (MM)*.

Relevant Application and Available Solution

Application	Implemented Solution (EoP or WUC)	Further Information
Materials Management (MM)	End of purpose check (EoP)	This includes the business in the areas of: • Purchasing • External Service Procurement • Invoice Verification • Inventory Management

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*.

12.6.5 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.

12.6.6 Supplier and Category Management

12.6.6.1 Authorizations

Supplier Information and Master Data uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
/SRMSMC/CATEGORY_MANAGER	Category Manager
/SRMSMC/DNB_REQUESTOR	Role for Requesting Reports from D&B
/SRMSMC/EVALUATION_APPRAISER	Appraiser
/SRMSMC/ACTIVITY_MANAGER	Activity Manager
/SRMSMC/ACTIVITY_PARTICIPANT	Participant in Activity
/SRMSMC/QUESTIONNAIRE_MANAGER	Questionnaire Manager
/SRMSMC/TRANSLATOR	Translator
/SRMSMC/DISPLAY_ALL	Display Role for All Objects in Supplier and Category Management
/SRMSMC/REPORT_EXEC_ADMIN	Technical Role with Authorization to Start Reports in Supplier and Category Management
/SRMSMC/BG_SUP_EVAL_BUYSIDE	RFC Background Processing in Supplier Evaluation

We recommend that you do not assign the *Appraiser* and the *Category Manager* role to the same person. Under exceptional circumstances, such as Category Managers filling out questionnaires for other colleagues, you can grant both roles to the same person.

> **i Note**
>
> Please note, that each user has to be assigned to a business partner *Employee*(I_EMPLOYEE)to have access to Supplier and Category 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* .

Authorization Objects Specific to Supplier Information and Master Data

The table below shows the security-relevant authorization objects that are specific to Supplier Information and Master Data:

Authorization Object	Field	Value	Description
/SRMSMC/DB	ACTVT	Reload	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. Enables users to interact with an instance of a business object of Supplier Information and Master Data in a specific way. The authorization object is used in the /SRMSMC/DNB_REQUESTOR role.
/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	As the type of business object that the user can access, you can specify the values listed.

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.

Personalization Object “SLC: PFCG Role Attributes”

The personalization object *SLC: PFCG Role Attributes* (`/SRMSMC/PFCG_ROLE_ATTRIBUTES`) offers the following checkboxes:

- `Appraiser Role`
- `Category Manager Role`
- `Questionnaire Manager Role`
- `Activity Manager Role`
- `Activity Participant Role`

Setting one of the above checkboxes in a role has the following effects on users to whom the role has been assigned:

- The users can perform the activities intended for this role. Note that, in addition to the checkbox in the personalization object, performing these activities also depends on the authorization objects assigned to the role.
- Only users for whom the personalization object checkbox is selected are considered during a search, for example for an appraiser or for a purchaser responsible.
  Example:
  For a user to be found in a search for a purchaser responsible, the `Category Manager Role`, the `Questionnaire Manager Role`, or the `Activity Manager Role` checkbox is required, depending on the process where the search is performed.

12.6.6.2 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 SAP NetWeaver Security Guide.

12.6.6.3 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 22] and Application-Specific Virus Scan Profile (ABAP) [page 194].

12.6.6.4 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 22].

12.7 Supply Chain

12.7.1 Efficient Logistics and Order Fulfillment

12.7.1.1 Authorizations in Inventory Management

Inventory Management uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_BR_INVENTORY_MANAGER	Inventory Manager
SAP_BR_WAREHOUSE_CLERK	Warehouse Clerk

Role	Description
SAP_BR_INVENTORY_ACCOUNTANT	Inventory Accountant

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Field	Description
M_ISEG_WDB	Activity Plant	Phys. Inv: Difference Posting in Plant
M_ISEG_WIB	Activity Plant	Phys. Inv: Phys. Inv Document in Plant
M_ISEG_WZL	Activity Plant	Phys. Inv: Count in Plant
M_ISEG_WZB	Activity Plant	Phys. Inv: Count and Difference Posting in Plant
M_MSEG_BMB	Activity Movement Type (Inventory Management)	Material Documents: Movement Type
M_MBNK_ALL	Activity	Material Documents: Number Range Maintenance
M_MSEG_WMB	Activity Plant	Material Documents: Plant
M_MRES_BWA	Activity Movement Type (Inventory Management)	Reservations: Movement Type
M_MRES_WWA	Activity Plant	Reservations: Plant
M_MWOF_ACT	Activity	Control for Split Valuation of Value (MBWO)

Authorization Object	Field	Description
M_SKPF_VGA	Activity Transaction for Inventory Sampling	Inventory Sampling: Transaction
M_SKPF_WRK	Activity Plant	Inventory Sampling: Plant
M_MSEG_BWA	Activity Movement Type (Inventory Management)	Goods Movement: Movement Type
M_MSEG_LGO	Activity Plant Storage Location Movement Type (Inventory Management)	Goods Movement: Storage Location
M_MSEG_WWA	Activity Plant	Goods Movements: Plant
M_MSEG_BWF	Activity Movement Type (Inventory Management)	Goods Receipt for Production Order: Movement Type
M_MSEG_WWF	Activity Plant	Goods Receipt for Production Order: Plant
M_MSEG_BWE	Activity Movement Type (Inventory Management)	Goods Receipt for Purchase Order: Movement Type
M_MSEG_WWE	Activity Plant	Goods Receipt for Purchase Order: Plant

12.7.1.2 Authorizations in Logistics Execution

Logistics Execution uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Roles for Decentralized Warehouse Management, Transportation, and Shipping

Role	Description
SAP_LE_GATE_KEEPER	Register Persons and Means of Transport at Checkpoint
SAP_LE_GATE_KEEPER_WEB	Register Persons and Means of Transport at Checkpoint (WEB)
SAP_LE_GOODS_ISSUE_DELIVERY	Post Goods Issue for Outbound Deliveries
SAP_LE_GOODS_RECEIPT_DELIVERY	Post Goods Receipt for Inbound Deliveries
SAP_LE_INB_DELIVERY_DISPLAY	Display Inbound Deliveries
SAP_LE_INB_DEL_PROCESSING	Process Inbound Deliveries
SAP_LE_INB_MONITORING	Monitor Inbound Delivery Process
SAP_LE_INB_STATISTICS	Standard Analyses for the Inbound Delivery
SAP_LE_LOAD_DELIVERY	Load Outbound Deliveries
SAP_LE_MASTER_DATA_MAINTENANCE	Master Data Maintenance
SAP_LE_OUTBOUND_POD	Proof of Delivery for Outbound Deliveries (POD)
SAP_LE_OUTB_DELIVERY_DISPLAY	Display Outbound Deliveries
SAP_LE_OUTB_DEL_PROCESSING	Process Outbound Deliveries
SAP_LE_OUTB_MONITORING	Monitor Outbound Delivery Process
SAP_LE_OUTB_STATISTICS	Standard Analyses for the Outbound Delivery
SAP_LE_PACKING_DELIVERY	Pack Deliveries
SAP_LE_PACKING_STATION	Packing Station (WEB)
SAP_LE_PICKING_WAVES	Process Wave Picks

Role	Description
SAP_LE_POD_HANDHELD	Proof of Delivery in Handheld Terminal from Customer's View
SAP_LE_POD_WEB	Proof of Delivery in Internet from Customer's View
SAP_LE_SHIPPING_NOTIFICATION	Process Inbound Deliveries from Supplier's View in Internet
SAP_LE_TMS_ARCHIVING	Archiving of Transportation and Shipment Cost Documents
SAP_LE_TMS_BACKGROUND	Background Transactions in Shipment
SAP_LE_TMS_CAPACITY_ANALYSIS	Perform Analyses for Utilization and Free Capacity
SAP_LE_TMS_CARRIER_WEB	Internet Transactions for the Forwarding Agent
SAP_LE_TMS_CURRENT_ANALYSIS	Perform Current Evaluations for Shipments
SAP_LE_TMS_DISPLAY	Display Documents in Shipment
SAP_LE_TMS_EXECUTION	Execute Planned Shipments
SAP_LE_TMS_EXTERNAL_TPS	Interface to External Transportation Planning System
SAP_LE_TMS_MAINTAIN_SCD	Create, Process, and Display Shipment Costs
SAP_LE_TMS_MAINTAIN_SCD_COND	Maintain Conditions in Shipment Costs Environment
SAP_LE_TMS_MAINT_SHP_MASTER	Maintain Master Data in the Transportation Environment
SAP_LE_TMS_MONITOR_PLANNING	Monitor Shipment Planning
SAP_LE_TMS_MONITOR_SHPCOSTS	Monitor Shipment Costs Calculation and Settlement
SAP_LE_TMS_OTHERS	Other Transportation Transactions (Without Composite Role)
SAP_LE_TMS_PLANNING	Create, Change, and Display Shipments
SAP_LE_TMS_RULES	Define Rules for Multiple Shipment Creation
SAP_LE_TMS_STATISTIC_ANALYSIS	Perform Statistical Analyses for Shipments
SAP_LE_TMS_TP_SERVICE_AGENT	Interface for Shipment Planning in Cooperation with Forwarding Agents
SAP_LE_WMS_APPOINTMENTS	Door Appointments
SAP_LE_WMS_CYCLE_COUNTING	Perform Cycle Counting in WM
SAP_LE_WMS_INFORMATION	Warehouse Information
SAP_LE_WMS_LIS_STATISTICS	LIS WM Statistics Data

Role	Description
SAP_LE_WMS_LOAD	Workload in Warehouse
SAP_LE_WMS_MONITORING	Warehouse Monitoring
SAP_LE_WMS_ONE_TIME_TASK	One-Time Tasks in WM
SAP_LE_WMS_PC_PROCESSING	Edit Posting Change Notice in WM
SAP_LE_WMS_PHYS_INVENTORY	Physical Inventory in WM
SAP_LE_WMS_PHYS_INVENTORY_CNT	Physical Inventory Count in WM
SAP_LE_WMS_PHYS_INVENTORY_MON	Physical Inventory Analysis and Monitoring in WM
SAP_LE_WMS_QUALITY_MANAGEMENT	WM Quality Management
SAP_LE_WMS_R2R3_COUPLING	R/2-R/3 Coupling in WM
SAP_LE_WMS_REPLENISHMENT_WMPP	Replenishment WM-PP
SAP_LE_WMS_REPLENISH_INTERNAL	Internal WM Replenishment
SAP_LE_WMS_RF_ADMIN	Administration of Radio Frequency Link in WM
SAP_LE_WMS_RF_PROCESSING	Radio Frequency (RF) in WM
SAP_LE_WMS_STATISTICS	Analysis in WM
SAP_LE_WMS_STOCK_ADJUSTMENTS	Stock Adjustment WM-IM
SAP_LE_WMS_TO_EXCEPTION_HANDL	Exception Handling of Transfer Orders in WM
SAP_LE_WMS_TO_PREPARATION	Transfer Order Processing in WM
SAP_LE_WMS_TR_PROCESSING	Transfer Requirement Processing in WM
SAP_LE_WMS_WHSE_MAINTENANCE	Warehouse Maintenance
/SAPMP/RTS	Controls Whether a User can Assign Reel Type for a Plant

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Standard Authorization Objects: Decentralized Warehouse Management

Authorization Object	Description
L_BWLVS	Movement Type in the Warehouse Management System
L_LGNUM	Warehouse Number/Storage Type
L_SFUNC	Special Functions in Warehouse Management
L_TCODE	Transaction Codes in the Warehouse Management System

Standard Authorization Objects: Transportation

Authorization Object	Description
V_VFKK_FKA	Shipment Cost Processing: Auth. for Shipment Cost Type
V_VTTK_SHT	Shipment Processing: Authorization for Shipment Type
V_VTTK_TDL	Shipment Processing: Authorization for Forwarding Agents
V_VTTK_TDS	Shipment Processing: Auth. for Transport Planning Points
V_VTTK_TSA	Transportation Proc.: Authorization for Shipment Type Status

Standard Authorization Objects: Shipping

Authorization Object	Description
V_LECI_CKP	Checkpoint: Authorization for Checkpoint
V_LIKP_VST	Delivery: Authorization for Shipping Points
V_VBSK_GRA	Deliveries: Authorization for Delivery Group Type

12.7.1.3 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 SAP NetWeaver Security Guide.

12.7.1.4 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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*.

12.7.2 Extended Warehouse Management

12.7.2.1 Authorizations

Extended Warehouse Management (EWM) uses the authorization concept provided by the SAP NetWeaver AS for 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 SAP NetWeaver 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 SAP NetWeaver Security Guide under *User Administration and Authentication*.

Standard Roles

You can find the roles relevant to EWM by using the following search terms:

- The search term **`*/SCWM*`** lists all SAP standard roles relevant for EWM.
  The role short text helps you find the role covering your business needs. The documentation of the role provides you with a detailed description of the role content.
- The search term **`*/SCWM/*DAS*`** lists all roles that are relevant for SAP Dock Appointment Scheduling.

Alternatively, you can use transaction `SUIM` to find the PFCG roles for EWM. In transaction `SUIM`, choose *Roles* > *Roles by Complex Selection Criteria*. Then enter the above mentioned search criteria (for example **`*/SCWM*`**) in the *Role* field.

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

Especially if in a system many warehouses are modelled it may be a requirement that people working in one warehouse should not be able to access data from another warehouse.

In many EWM authorization fields for this purpose a specific authorization field is contained.

For example:

- `/SCWM/LGNU` *Warehouse Number/Warehouse Complex*
  This is the most often used authorization field. It is used, for example, in EWM monitor authorization object `/SCWM/MO`.
- `/SCWM/ORG` *Location/Organizational Unit*
  This is the most often used authorization field. It is used, for example, in EWM monitor authorization object `/SCWM/MO`.
- `/SCMB/LGNU` *Warehouse Number/Warehouse Complex*

Warehouse in Customizing or Administration

In other cases (like administration or customizing) no specific authorization objects are used. Here the generic authorization objects to limit the access to tables and views can be used.

- S_TABU_NAM (Table Access by Generic Standard Tools)
- S_TABU_LIN (Authorization for Organizational Unit)

> ✤ Example

The customizing for "storage bin types" has the assigned customizing object `/SCWM/T303`. The underlying database table `/SCWM/T303` has as part of the key the field `LGNUM` (warehouse number) with data element `/SCWM/LGNUM`.

- With S_TABU_NAM it can be limited whether someone can access at all the customizing for /SCWM/T303.
- With `S_TABU_LIN` you can in addition limit the access based on organization criteria.
  Here you can use authorization field `ORG_CRIT` (Organization criterion for key-specific authorization) and use value `/SCWM/LGNUM` (*Warehouse Number/Warehouse Complex*) to be able to enter a warehouse in `ORG_FIELD1`.

For more information, see the documentation of the two authorization objects in transaction `SU21`.

BRFplus

At some places, BRFplus is used in EWM (for example in Labor Management).

BRFplus does not know organization units like the warehouse number. Therefore if a separation of BRFplus entities should be done based on warehouses, this has to be considered during the implementation phase so that alternative mechanism of BRFplus can be used.

In general the authorization concept of BRFplus is described in the SAP Help Portal at http://help.sap.com/https://help.sap.com/viewer/9d5c91746d2f48199bd465c3a4973b89/7.5.7/en-US/5101d1274ccc458b888952ce2c1485fb.html

In the how-to guide for BRFplus usage in Labor Management example are shown how a separation regarding authorization could be done. See how-to guides for EWM at http://help.sap.com/ewm.

Critical Combinations

Expert Role

EWM provides the expert role EWM: Warehouse Expert (`/SCWM/EXPERT`). This role contains almost all transactions and authorizations for EWM and the corresponding Customizing. Therefore, we recommend that you assign this role very carefully and only to very specific users, and that you do not assign this role to normal users or users who work in specific EWM areas only.

Appointment Planner for Carrier

> **i Note**
>
> This role is 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 role for this: Appointment Planner for Carrier in Dock Appointment Scheduling (`/SCWM/DAS_EXT_CARR_PLANNER`). This role contains only one Web Dynpro screen in the *Maintain Appointments – Textual* menu (`/SCWM/DSAPP_LIST`). This screen allows the appointment planners for carriers to view and create appointments. The Web Dynpro application *Direct Access to Appointment – Textual* (`/SCWM/DSAPP_MAINT`) is also available, but it is not visible in the user menu as it is started indirectly from the *Maintain Appointments – Textual* screen. The role also contains very limited number of authorization objects.

> **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/DSLP`) 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: 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

> **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 your 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

> **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.

EWMt 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*)

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.

12.7.2.2 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 SAP NetWeaver Security Guide.

12.7.2.3 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 SAP NetWeaver Security Guide.

12.7.2.4 Enterprise Services Security

For general information, see the chapters on Web Services Security in the SAP NetWeaver Security Guide and in the SAP Process Integration Security Guide.

12.7.2.5 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 209].
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.
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 209].
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. For information about security for SAP Plant Connectivity, see the security guide for SAP Plant Connectivity on SAP Service Marketplace at https://service.sap.com/securityguides.

12.8 Analytics Technology

12.8.1 Process Performance Monitoring

12.8.1.1 Process Observer

12.8.1.1.1 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 SAP NetWeaver 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 SAP NetWeaver 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: • 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: • Define a process • Define BRFplus rules • Create a process simulation
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: • 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: • 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_SIDEPANEL`)	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.

Role	Description
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: • 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.

12.8.1.1.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *Product Assistance* ▶ *Cross Components* ▶ *Process Observer (CA-EPT-POC)* ▶ *Process Monitoring and Analytics* ▶ *Process Monitoring Setup*.

12.8.1.1.3 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 http://help.sap.com/s4hana_op_1610_001 ▶ *Product Assistance* ▶ *Cross Components* ▶ *Process Observer (CA-EPT-POC)* ▶ *Operations* ▶ *Reports* ▶ *Reports Used in Operations for Process Monitoring*.

12.9 Enterprise Technology

12.9.1 Central Master Data

12.9.1.1 Authorizations and Roles used by Central Master Data

The Central Master Data uses the authorization concept provided by the SAP NetWeaver AS for 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 SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_BR_BUPA_MASTER_SPECIALIST	Master Data Specialist - Business Partner Data
SAP_BR_PRODMASTER_SPECIALIST	Master Data Specialist - Product Data
SAP_BR_BPC_EXPERT	Configuration Expert - Business Process Configuration

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Description
B_BUPA_GRP	Business Partner: Authorization Groups
B_BUPA_RLT	Business Partner: BP Roles
B_BUPA_BZT	Business Partner Relationships: Relationship Categories
F_KNA1_APP	Customer: Application Authorization
F_KNA1_BED	Customer: Account Authorization
F_KNA1_BUK	Customer: Authorization for Company Codes
F_KNA1_GEN	Customer: Central Data
F_KNA1_GRP	Customer: Account Group Authorization
V_KNA1_BRG	Customer: Account Authorization for Sales Areas
V_KNA1_VKO	Customer: Authorization for Sales Organizations
F_LFA1_APP	Supplier: Application Authorization
F_LFA1_BEK	Supplier: Account Authorization
F_LFA1_BUK	Supplier: Authorization for Company Codes
F_LFA1_GEN	Supplier: Central Data
F_LFA1_GRP	Supplier: Account Group Authorization
M_LFM1_EKO	Purchasing Organization in Supplier Master Record

12.9.1.2 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.

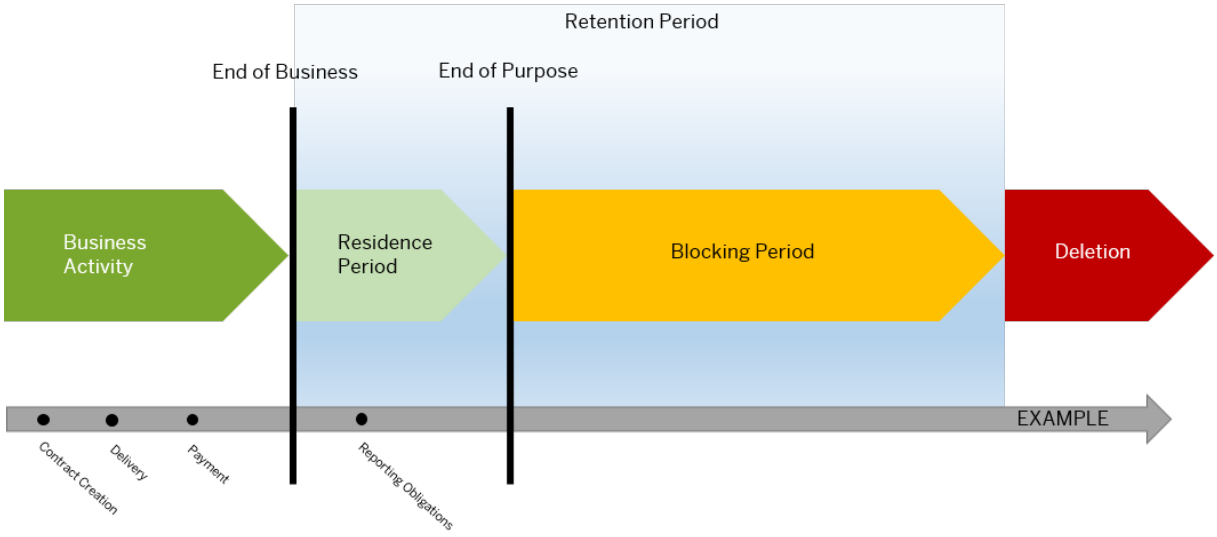
The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. The business partner, customer and supplier master data uses SAP ILM to support the blocking and deletion of personal data as described in 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
Business Partner Data	Archiving object: `CA_BUPA` ILM object: `CA_BUPA` Prerequisites: • Business function `BUPA_ILM_BF` is activated • To use ILM enablement, the EoP check is mandatory before archiving or deletion (transaction `BUPA_PRE_EOP`).
Customer Master Data	Archiving object: `FI_ACCRECV` ILM object: `FI_ACCRECV` Prerequisites: • 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`).
Supplier Master Data	Archiving object: `FI_ACCPAYB` ILM object: `FI_ACCPAYB` Prerequisites: • 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`).
Contact Person related to business partner, customer and supplier master data	Destruction object: `FI_ACCKNVK` ILM object: `FI_ACCKNVK` Prerequisites: • 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
Business Partner (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`).
Business Partner Relationship (BUB)	End of purpose (EoP) check	EoP is determined based on the Valid-To field of the relationship.
ERP Customer Master (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.
ERP Supplier Master (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.
ERP Contact Persons (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

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 residence and retention policies for the customer master and supplier master (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 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 http://help.sap.com/s4hana_op_1610_001 under *Product Assistance* > *Cross Components* > *Data Protection*.

12.9.2 Middleware

12.9.2.1 SAP Application Interface Framework

Use

This guide provides an overview of the security considerations that are specific to the SAP Application Interface Framework.

Features

The SAP Application Interface Framework uses flexible authorization rules to allow you to restrict access to data and to monitoring and error handling. This security feature enforces compliance by following the need-to-know principle when restricting access to interface data.

When you have given users the authorization to change and correct interface data, the system tracks all changes that are made and allows you to trace which user made which change.

The configuration of security and authorizations in the SAP Application Interface Framework includes the following objects, roles, and data:

- Standard authorization objects (see Authorization Objects [page 223])
- Predefined role templates (see *Role Templates*)
- The integration of custom-defined authorization objects (see Set Up Interface-Specific and Key Field-Specific Authorizations [page 262])
- Personal data
  To secure your data properly, it is also required that you understand the personal data stored by the SAP Application Interface Framework (see *Considerations about Data Protection*)

12.9.2.1.1 Authorization Objects

The SAP Application Interface Framework allows you to specify various authorization settings. In this section, each authorization object is explained with its description, technical attributes, and use.

12.9.2.1.1.1 Authorization Object for Interface Processing

Definition

The authorization object `/AIF/PROC` is used by the system to check the user's authorization for processing a data message of a given interface in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
`ACTVT`	Activity	You can enter the following activities: Import (60) Export (61) Resubmit (A4)
`/AIF/NS`	Namespace	This field refers to a namespace in the SAP Application Interface Framework
`/AIF/IF`	Interface Name	This field refers to an interface name in the SAP Application Interface Framework

Field Name	Heading	Authorization Object Setting
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
/AIF/VNS	Variant Namespace	This field refers to a variant namespace name in the SAP Application Interface Framework
/AIF/VNAME	Name of Interface Variant	This field refers to a variant name in the SAP Application Interface Framework

Use

Messages are processed by a specific user. This user requires the authorization to (re-) process data messages in the SAP Application Interface Framework.

Example

The user PIAPPL is assigned the authorization to process data messages for all namespaces, interface names, interface versions, and, if applicable, variant namespace and name.

12.9.2.1.1.2 Authorization Object for Customizing Steps

Definition

The authorization object /AIF/CUST is used by the system to check the user's authorization for a Customizing activity in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Change (02) Display (03)

Field Name	Heading	Authorization Object Setting
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/MC	Customizing view	For the available values, see the table below

Use

The *Namespace* (/AIF/NS) field can contain any namespace name. By entering a value in the namespace field, you can limit the user's authorization for Customizing activities to the specified namespaces.

> **Example**
>
> An interface developer is authorized to create, edit, and delete interfaces in namespace **X** but not **Y**.

Allowed Values for the Namespace Field

For the *Namespace* (/AIF/MC) field, the following values are allowed:

Value	Description
/AIF/ACTIONS	Define Actions
/AIF/ALERT	Define Recipients
/AIF/BDC_V_CONF	Define Pre-Interface Determination for Batch Input
/AIF/CFUNC	Define Custom Functions
/AIF/CHECKS	Define Checks
/AIF/CLINK	Define Custom Data Link
/AIF/CTEXT	Define Custom Message Text
/AIF/ERROR_GLB	Global Features
/AIF/ERROR_HDL	Define Applications
/AIF/ERROR_IF	Define Interface-Specific Features
/AIF/ERROR_NS	Define Namespace-Specific Features
/AIF/FIXVALUES	Define Fix Values
/AIF/LFA_SETTINGS	Settings for AIF File Adapter

Value	Description
/AIF/POC	Configuration for POC Integration
/AIF/SMAP	Define Structure Mapping
/AIF/VALMAPS	Define Value Mappings
/AIF/VARIANT_MAPPINGS_ALL	Define Variant Mappings
/AIF/VC_SERIAL	Define Serialization Settings
/AIF/VC_TJ_CONF	Configure Data Transfer
/AIF/VREP_AC_ASG	Assign Automatic Reprocessing Action
/AIF/VREP_AC_DEF	Define Automatic Reprocessing Action
/AIF/V_ALRT_USR2	Define Recipients of Other Users
/AIF/V_ALRT_USR3	Define Recipients of Own User
/AIF/V_BDC_IF	Assign Batch Input Session and Creator
/AIF/V_ENGINES	Define Custom-Specific Engines
/AIF/V_FINF	Define Interfaces
/AIF/V_FINF_ENG	Define Interfaces (Engine Fields)
/AIF/V_FINF_IDOC	Define Interfaces (IDoc fields)
/AIF/V_FINF_TL	Define Trace Level
/AIF/V_HINTS	Define Custom Hints
/AIF/V_IDOCSTAT	Mapping of IDoc Status to AIF Status
/AIF/V_IFKEY	Define Interface Key Fields for Variants
/AIF/V_NS	Define Namespace
/AIF/V_PERS_RTCG	Define Runtime Configuration Group
/AIF/V_RFC_FCOL	Define RFC Function Module Collection
/AIF/V_RFC_FUNCS	Assign Functions to RFC Function Module Collection
/AIF/V_SYSNAMES	Define Business Systems
/AIF/V_VALID_PER	Define Validity Period

12.9.2.1.1.3 Authorization Objects for Error Handling

Definition

The authorization object /AIF/ERR is used by the system to check the user's authorization for error handling in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Execute (16) (means selecting from index tables) Archive (24) (means starting the archiving report using SARA) Reload (25) (means restoring archived data using SARA) Read (33) (means reading message content from persistence) Write (34) (means updating message content in persistence) Display archive (56) Administer (70) (means starting an external technical monitoring tool like qRFC for PI messages) Analyze (71) (means displaying application log messages) Remove (75) (means canceling a message) Resubmit (A4) (means restarting a message) General overview (GL) (means starting external monitoring like XML monitoring for PI messages or WE02 for IDocs)
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/IF	Interface Name	This field refers to an interface name in the SAP Application Interface Framework

Field Name	Heading	Authorization Object Setting
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework

Use

Using the activity field, you specify the actions that a user can execute in the system. For example, you might want to specify a user who only has read access to the transaction. You can further limit the authorization by namespace, interface name, and interface version. As a result, the user can execute the specified activities only for the defined namespace/interface name/interface version combination.

12.9.2.1.1.4 Authorization Object for Technical Error Handling

Definition

The authorization object /AIF/TECH is used by the system to check the user's authorization for the technical mode of error handling in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activity: Activate (63)

Use

This authorization object does not have any parameters or activities. If a user does not have the authorization, the *Technical Mode* checkbox in the selection screen and the *Technical Mode* pushbutton in the main screen of the *Monitoring and Error Handling* transaction are hidden.

12.9.2.1.1.5 Authorization Object for Emergency Corrections

Definition

The authorization object `/AIF/EMC` is used by the system to check the user's authorization for emergency corrections in the error handling of the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
`ACTVT`	Activity	You can enter the following activities (see description for authorization object `/AIF/ERR` for details): Execute (16) Read (33) Write (34) Administer (70) Analyze (71) Remove (75) Resubmit (A4) General overview (GL)
`/AIF/NS`	Namespace	This field refers to a namespace in the SAP Application Interface Framework

Use

Using the activity field, you specify the actions the user can execute in emergency correction mode in the *Monitoring and Error Handling* transaction. You can further limit the authority to execute the actions in emergency correction mode based on the interface namespace.

When executing the *Monitoring and Error Handling* transaction, the user first has to enter a namespace and press the `ENTER` key. The system then checks the authorization for emergency corrections and displays the *Emergency Correction Mode* checkbox, if applicable.

12.9.2.1.1.6 Authorization Objects for Custom Functions

Definition

The authorization object /AIF/CFUNCis used by the system to check the user's authorization for custom functions for error handling in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Create or generate (01) Change (02) Display (03) Delete (06) Execute (16) (means executing in the *Monitoring and Error Handling* transaction)
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/IF	Interface Name	This field refers to an interface name in the SAP Application Interface Framework
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
/AIF/NSREC	Namespace of Recipient	Not used at the moment; enter *
/AIF/VISI	Visibility	Specifies for which users the custom function is visible. You can enter the following values: **A** means "Just for current user" **B** means "For a list of users" (maintained in transaction /AIF/CUST_FUNC *Define Custom Functions* > *Assign Users*) **C** means "For all users"
/AIF/OTHUS	Authorization for other users	Not used at the moment; enter *

Use

Using the activity field, you specify the actions the user can execute in custom functions in the *Monitoring and Error Handling* transaction and the corresponding maintenance views for custom functions.

12.9.2.1.1.7 Authorization Objects for Custom Hints

Definition

The authorization object `/AIF/HINTS` is used by the system to check the user's authorization for custom hints for error handling in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
`ACTVT`	Activity	You can enter the following activities: Create or generate (01) Change (02) Display (03) Delete (06)
`/AIF/NS`	Namespace	This field refers to a namespace in the SAP Application Interface Framework
`/AIF/IF`	Interface Name	This field refers to an interface name in the SAP Application Interface Framework
`/AIF/IFVER`	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
`/AIF/NSREC`	Namespace of Recipient	Not used at the moment; enter *
`/AIF/VISI`	Visibility	Specifies for which users the custom hint is visible. You can enter the following values: **A** means "Just for current user" **B** means "For a list of users" (not used at the moment) **C** means "For all users"

Field Name	Heading	Authorization Object Setting
/AIF/OTHUS	Authorization for other users	Not used at the moment; enter *

Use

Using the activity field, you specify the actions the user can execute in custom hints in the *Monitoring and Error Handling* transaction and the corresponding maintenance views of the custom hints.

12.9.2.1.1.8 Authorization Object for Interface Determination

Definition

The authorization object /AIF/IFDET is used by the system to check the user's authorization for maintaining interface determination in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
/AIF/IDTY	Application Engine Identifier	Type of application engine: 000: Proxy 001: IDoc 002: XML 003: Test File 004: ECH
/AIF/NS	Namespace	Namespace of a customer-specific engine
/AIF/IDCTY	Identifier for a Customer-Specific AIF Interface Type	Identifier of a customer-specific engine
/AIF/IDN1	Name 1 of Interface Type	First key field of an engine
/AIF/IDN2	Name 2 of Interface Type	Second key field of an engine

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activity: Create or generate (01) Change (02) Display (03) Delete (06)

Use

Using the activity field, you specify the actions the user can execute in the corresponding maintenance views of interface determination.

12.9.2.1.1.9 Authorization Object for Value Mapping Maintenance

Definition

The authorization object /AIF/VMAP is used by the system to check the user's authorization to display and/or update value mappings in the *Value Mapping* transaction of the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Change (02) Display (03)
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/VMAP	Value Mapping	This field refers to a value mapping name in the SAP Application Interface Framework
/AIF/BSKEY	Key Name of Business System	This field refers to a business system name

Use

The authorization object protects the display/update of value mappings.

> ⚠ Caution
>
> The authorization is only checked in the *Value Mapping* transaction `/AIF/VMAP` (and derived transaction variants) and not in the *Define Value Mappings* Customizing activity.

12.9.2.1.1.10 Authorization Object for File Adapter

Definition

The authorization object `/AIF/LFA` is used by the system to check the user's authorization to access files in the directories of the application server. This can be done in the file adapter transactions (`/AIF/LFA_UPLOAD_FILE` and `/AIF/LFA_CHECK_SEND`) of the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Display (03) – display file content in the File Adapter Delete (06) – delete files from application server after successful upload Read (33) – read files from application server to AIF Write (34) – write files from AIF to application server Analyze (71) – display file list in F4 help
`/AIF/FDIR`	Directory on Application Server	This field refers to a directory on the application server, for example, `/usr/temp`
`/AIF/FNAM`	Interface File Name	This field refers to the file name, for example, `A*.xml`

Use

The authorization object protects the access to files on the application server.

> ⚠ Caution
>
> The authorization is checked only in the file adapter transactions for files which are located on the application server. For accessing the local PC (the front end, presentation server), this standard authorization concept for accessing files from SAP GUI takes care of security aspects (for example, display the *Allow/deny* popup to the user).

12.9.2.1.1.11 Authorization Object for Serialization

Definition

The authorization object `/AIF/SER` is used by the system to check the user's authorization to display/change the current external index of a serialization object (for example, change index of a specific purchase order number). This can be done in the *Manual Change of External Index* transaction (transaction code `/AIF/SERIAL_INDEX`) of the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
`ACTVT`	Activity	You can enter the following activities: Change (02) – update the external index Display (03) – display the external index
`/AIF/NS`	Namespace	This field refers to the namespace of the serialization object
`/AIF/SEROB`	Serialization Object	This field refers to the name of the serialization object.

Use

The authorization object protects the access to the external index of a serialization object.

12.9.2.1.1.12 Authorization Object for Change Log

Definition

The authorization object /AIF/CDLOG is used by the system to check the user's authorization to display the user name in the *Error Handling Change Log* (transaction code /AIF/EDCHANGES).

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Administer (70) – Display the *Modified By* field

Use

The authorization object protects the access to the user name of log entry in the *Error Handling Change Log*.

12.9.2.1.1.13 Authorization Objects for Custom Message Texts

Definition

The authorization object /AIF/CTEXT is used by the system to check the user's authorization for custom message texts for error handling in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Create or generate (01) Change (02) Display (03) Delete (06)
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework

Field Name	Heading	Authorization Object Setting
/AIF/IF	Interface Name	This field refers to an interface name in the SAP Application Interface Framework
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
/AIF/VISI	Visibility	Specifies for which users the custom message text is visible. You can enter the following values: **A** means “Just for current user” **B** means “For a list of users” (not used at the moment) **C** means “For all users” (not used at the moment)
/AIF/OTHUS	Authorization for other users	Not used at the moment; enter *

Use

Using the activity field, you specify the actions the user can execute in custom message texts in the *Monitoring and Error Handlin*g transaction and the corresponding maintenance views for custom message texts.

12.9.2.1.1.14 Authorization Objects for Custom Data Links

Definition

The authorization object /AIF/CLINK is used by the system to check the user’s authorization for custom data links for error handling in the SAP Application Interface Framework.

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Create or generate (01) Change (02) Display (03) Delete (06)
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/IF	Interface Name	This field refers to an interface name in the SAP Application Interface Framework
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
/AIF/VISI	Visibility	Specifies for which users the custom data link is visible. You can enter the following values: **A** means “Just for current user” **B** means “For a list of users” (not used at the moment) **C** means “For all users” (not used at the moment)
/AIF/OTHUS	Authorization for other users	Not used at the moment; enter *

Use

Using the activity field, you specify the actions the user can execute in custom data links in the *Monitoring and Error Handling* transaction and the corresponding maintenance views for custom data links.

12.9.2.1.1.15 Authorization Object for XML Persistence Messages Deletion

Definition

The authorization object `/AIF/PERSD` is used by the system to check the administrator's authorization to authorize another user to irreversibly delete messages from the XML persistence using the *XML Persistence Messages Deletion* (transaction `/AIF/PERS_DEL`).

Authorization Fields

Field Name	Heading	Authorization Object Setting
`ACTVT`	Activity	You can enter the following activities: Create in DB (40) Delete in DB (41)

Use

The authorization object protects the access to the maintenance view (transaction `/AIF/PERS_DEL_AUTH`) for granting authorizations for the *XML Persistence Messages Deletion*.

For executing the *XML Persistence Messages Deletion*, there is a two-person authorization concept in place. An administration user can authorize another user (but not himself) to execute the report for a specific interface at a specific date.

12.9.2.1.1.16 Authorization Object for Processor Assignment

Definition

The authorization object `/AIF/DPA` is used by the system to check the user's authorization to assign, unassign, or change the assignment of processors in the *Details and Processor Assignment*. In addition, it checks the authorization to create or change the processing status and the comments.

Authorization Fields

Field Name	Heading	Authorization Object Setting
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework

Field Name	Heading	Authorization Object Setting
/AIF/IF	Interface Name	This field refers to an interface name in the SAP Application Interface Framework
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
/AIF/NSREC	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/RECIP	Alert Management Recipient	This field refers to a recipient in the SAP Application Interface Framework.
/AIF/OTHUS	Authorization for Other Users	This field allows the user to change assignments, statuses, and comments also for other processors. An empty value means no authorization, while **X** means that the user has the authorization.
ACTVT	Activity	You can enter the following activities: • Change (02) • Display (03)

Use

Using the activity field, you specify the actions the user can execute in *Details and Processor Assignment* in the *Interface Monitor*.

12.9.2.1.2 Role Templates

Definition

The SAP Application Interface Framework provides predefined template roles that you can use in order to define roles for your specific requirements.

Features

Role Templates

The following role templates are delivered with the SAP Application Interface Framework 3.0:

- `SAP_AIF_ADMIN`: AIF Administrator [page 242]
- `SAP_AIF_ALL`: AIF All Authorizations [page 246]
- `SAP_AIF_ARCHITECT`: AIF Architect [page 247]
- `SAP_AIF_DEVELOPER`: AIF Developer [page 251]
- `SAP_AIF_USER`: AIF Business User [page 255]
- `SAP_AIF_POWER_USER`: AIF Power User [page 257]
- `SAP_AIF_PROCESSING`: AIF Processing [page 261]
- `SAP_AIF_TEST_TEMPL`: AIF Test Template (Non-Productive) [page 262]

Use of Role Templates

When creating your own roles, you can add the SAP Application Interface Framework-specific authorizations based on the role templates in *Role Maintenance* (transaction code `PFCG`) when you maintain the authorization data (in the *Authorizations* tab).

- When no authorization data exists, you are asked for a template
- When authorization data exists, you can add the SAP Application Interface Framework-specific authorizations in the command *Edit – Insert authorization(s) – From template...*

Content of the Role Templates

Each role templates contains a set of authorizations which typical users of the SAP Application Interface Framework would need.

> **i Note**
>
> This is only a proposal that you might need to adapt to your specific situation.

> **i Note**
>
> Most of the authorizations need to be granted by more specific values, for example, namespace and interface.

Example

You use the template `SAP_AIF_USER` to create the roles for your business users doing the monitoring and error handling. For a business user role, you can restrict the authorizations to the interfaces the business users are allowed to see.

You use template `SAP_AIF_DEVELOPER` to create the roles for the users developing the interfaces of the SAP Application Interface Framework.

More Information

Obsolete Roles

In version 2.0, the SAP Application Interface Framework provided predefined single and composite roles that could be used as a template in order to define roles for specific requirements.

With version 3.0, role templates are delivered, which simplifies the implementation significantly. Thus, the following single and composite roles are obsolete and are only provided for compatibility:

> → Recommendation
>
> Use the role templates described in this section and not these obsolete roles.

Obsolete Single Roles

- /AIF/CORRECT_DATA
- /AIF/CUST_CHANGE
- /AIF/CUST_DISPLAY
- /AIF/ERRHDL_CHANGE
- /AIF/ERRHDL_CHANGE_EMC
- /AIF/ERRHDL_DISPLAY
- /AIF/ERRHDL_DISPLAY_EMC
- /AIF/LOG_DISPLAY
- /AIF/MESSAGE_NOTIFICATION
- /AIF/MSG_STAT_SNAP_SHOT
- /AIF/PERFORMANCE_ANALYSIS
- /AIF/PROCESS_INB
- /AIF/PROCESS_OUTB
- /AIF/PROCESS_RES
- /AIF/SWITCH_FRAMEWORK
- /AIF/TEST_TOOL
- /AIF/VMAP_CHANGE
- /AIF/VMAP_DISPLAY
- /AIF/ARC_CREATE
- /AIF/ARC_DISPLAY
- /AIF/ARC_RELOAD

Obsolete Composite Roles

- /AIF/ADMINISTRATOR
- /AIF/DATA_FIXER
- /AIF/INTERFACE_DEVELOPER
- /AIF/KEY_USER
- /AIF/BUSINESS_USER
- /AIF/ALL

12.9.2.1.2.1 AIF Administrator

An *AIF Administrator* is responsible for advanced system configuration like “publishing” custom functions/ hints/message texts, interface determination, archiving, correction report, and so on.

For these tasks, an *AIF Administrator* is provided with the following authorizations:

Authorization Object	Activity	Activity Description
/AIF/CFUNC	1	Create or generate
/AIF/CFUNC	2	Change
/AIF/CFUNC	3	Display
/AIF/CFUNC	6	Delete
/AIF/CFUNC	16	Execute
/AIF/CLINK	1	Create or generate
/AIF/CLINK	2	Change
/AIF/CLINK	3	Display
/AIF/CLINK	6	Delete
/AIF/CTEXT	1	Create or generate
/AIF/CTEXT	2	Change
/AIF/CTEXT	3	Display
/AIF/CTEXT	6	Delete
/AIF/CUST	3	Display
/AIF/ERR	16	Execute
/AIF/ERR	24	Archive
/AIF/ERR	25	Reload
/AIF/ERR	33	Read
/AIF/ERR	56	Display archive
/AIF/ERR	70	Administer
/AIF/ERR	71	Analyze
/AIF/ERR	GL	General overview
/AIF/HINTS	1	Create or generate
/AIF/HINT	2	Change
/AIF/HINT	3	Display

Authorization Object	Activity	Activity Description
/AIF/HINT	6	Delete
/AIF/IFDET	1	Create or generate
/AIF/IFDET	2	Change
/AIF/IFDET	3	Display
/AIF/IFDET	6	Delete
/AIF/LFA	3	Display
/AIF/LFA	6	Delete
/AIF/LFA	33	Read
/AIF/LFA	34	Write
/AIF/LFA	71	Analyze
/AIF/SER	2	Change
/AIF/SER	3	Display
/AIF/TECH	63	Activate
/AIF/VMAP	2	Change
/AIF/VMAP	3	Display

In addition, an *AIF Administrator* is provided with the authorization to the following transaction codes:

Transaction Code	Description
/AIF/CORRECTIONS	Correction Report
/AIF/CUST	Customizing
/AIF/CUST_FUNC	Define Custom Functions
/AIF/CUST_HINTS	Define Custom Hints
/AIF/CUST_LINK	Define Custom Data Link
/AIF/CUST_TEXT	Define Custom Message Texts
/AIF/DEL_STRUC_CACHE	Delete Structure Cache
/AIF/DISPMSGSNAP	AIF Display Snapshot

Transaction Code	Description
/AIF/DOCU	Interface Documentation Tool
/AIF/EDCHANGES	Error Handling Changes Log
/AIF/ERR	Monitoring and Error Handling
/AIF/ERR_BASE	Error Handling Base
/AIF/GENMSGSNAP	AIF Generate Snapshot
/AIF/IDOC_IMPORT	AIF IDOC Import
/AIF/IDXTBL	Index Table Overview
/AIF/IF_TRACE	AIF Interface Trace Level
/AIF/IFMON	Interface Monitor
/AIF/LFA_CHECK_SEND	Read Files from folder; Send to AIF
/AIF/LFA_UPLOAD_FILE	Upload File to AIF
/AIF/LOG	Interface Logs
/AIF/MYRECIPIENTS	Recipients of Current User
/AIF/PERFORMANCE	Performance Tracking
/AIF/PERS_CGR	Runtime Configuration Group
/AIF/PERS_TEST	Test Persistence with Flight Booking
/AIF/RECIPIENTS	Recipients of a User
/AIF/REP_AC_ASGN	AIF Reprocessing Action Assignment
/AIF/REP_AC_DEF	AIF Reprocessing Action Definition
/AIF/SERIAL_INDEX	Manual Change of External Index
/AIF/TEXT_HINTS	Transport Text of Hints
/AIF/TJ_CONFIG	Configure Data Transfer
/AIF/TOPICDEF	AIF Topic Definition
/AIF/TOPICSTATUS	Maintain Topic ID Status
/AIF/TRANSFER	Transfer into AIF Persistence
/AIF/VMAP	Value Mapping

Transaction Code	Description
/AIF/VMAP_BASE	Base Transaction for Value Mappings
/AIF/VPN	Maintain Validity Periods

In addition, an *AIF Administrator* is provided with the change authorization to the following views:

View/View Cluster	Description
/AIF/BDC_V_CONF	Define Pre-Interface Determination for Batch Input
/AIF/CFUNC	Define Custom Functions
/AIF/CLINK	Define Custom Data Link
/AIF/CTEXT	Define Custom Message Text
/AIF/LFA_SETTINGS	Settings for AIF File Adapter
/AIF/POC	Configuration for POC Integration
/AIF/VC_TJ_CONF	Configure Data Transfer
/AIF/VREP_AC_ASG	Assign Automatic Reprocessing Action
/AIF/VREP_AC_DEF	Define Automatic Reprocessing Action
/AIF/V_ALRT_USR2	Define Recipients of Other Users
/AIF/V_ALRT_USR3	Define Recipients of Own User
/AIF/V_BDC_IF	Assign Batch Input Session and Creator
/AIF/V_FINF_TL	Define Trace Level
/AIF/V_HINTS	Define Custom Hints
/AIF/V_PERS_RTCG	Define Runtime Configuration Group

12.9.2.1.2.2 AIF All Authorizations

This role template contains all SAP Application Interface Framework authorization objects with all activities and also all SAP Application Interface Framework transactions. It should only be used for test purposes.

12.9.2.1.2.3 AIF Architect

An *AIF Architect* is responsible for planning and coordinating the development of interfaces.

For these tasks, an *AIF Architect* is provided with the following authorizations:

Authorization Object	Activity	Activity Description
/AIF/CFUNC	1	Create or generate
/AIF/CFUNC	2	Change
/AIF/CFUNC	3	Display
/AIF/CFUNC	6	Delete
/AIF/CFUNC	16	Execute
/AIF/CLINK	1	Create or generate
/AIF/CLINK	2	Change
/AIF/CLINK	3	Display
/AIF/CLINK	6	Delete
/AIF/CTEXT	1	Create or generate
/AIF/CTEXT	2	Change
/AIF/CTEXT	3	Display
/AIF/CTEXT	6	Delete
/AIF/CUST	2	Change
/AIF/CUST	3	Display
/AIF/ERR	16	Execute
/AIF/ERR	33	Read
/AIF/ERR	34	Write
/AIF/ERR	70	Administer
/AIF/ERR	71	Analyze
/AIF/ERR	75	Remove
/AIF/ERR	A4	Resubmit
/AIF/ERR	GL	General overview

Authorization Object	Activity	Activity Description
/AIF/HINTS	1	Create or generate
/AIF/HINTS	2	Change
/AIF/HINTS	3	Display
/AIF/HINTS	6	Delete
/AIF/IFDET	1	Create or generate
/AIF/IFDET	2	Change
/AIF/IFDET	3	Display
/AIF/IFDET	6	Delete
/AIF/LFA	3	Display
/AIF/LFA	6	Delete
/AIF/LFA	33	Read
/AIF/LFA	34	Write
/AIF/LFA	71	Analyze
/AIF/PROC	60	Import
/AIF/PROC	61	Export
/AIF/PROC	A4	Resubmit
/AIF/SER	2	Change
/AIF/SER	3	Display
/AIF/TECH	63	Activate
/AIF/VMAP	2	Change
/AIF/VMAP	3	Display

In addition, an *AIF Architect* is provided with the authorization to the following transaction codes:

Transaction Code	Description
/AIF/BDC_GEN	Batch Input Structure Generator
/AIF/CORRECTIONS	Correction Report

Transaction Code	Description
/AIF/CUST	Customizing
/AIF/CUST_COPY	AIF Customizing Copy
/AIF/CUST_FUNC	Define Custom Functions
/AIF/CUST_HINTS	Define Custom Hints
/AIF/CUST_LINK	Define Custom Data Link
/AIF/CUST_SMAP_COPY	Copy Customizing
/AIF/CUST_TEXT	Define Custom Message Texts
/AIF/DEL_STRUC_CACHE	Delete Structure Cache
/AIF/DISPMSGSNAP	AIF Display Snapshot
/AIF/DOCU	Interface Documentation Tool
/AIF/EDCHANGES	Error Handling Changes Log
/AIF/ERR	Monitoring and Error Handling
/AIF/ERR_BASE	Error Handling Base
/AIF/GENMSGSNAP	AIF Generate Snapshot
/AIF/IDOC_GEN	IDoc Structure Generator
/AIF/IDOC_IMPORT	AIF IDOC Import
/AIF/IDOC_TEST	Generate Test IDocs
/AIF/IDXTBL	Index Table Overview
/AIF/IF_TRACE	AIF Interface Trace Level
/AIF/IFB	Interface Builder
/AIF/IFMON	Interface Monitor
/AIF/IFTEST	Interface Test Tool
/AIF/LFA_CHECK_SEND	Read Files from folder; Send to AIF
/AIF/LFA_UPLOAD_FILE	Upload File to AIF
/AIF/LOG	Interface Logs
/AIF/MSGNOTI	Message Overview Notification

Transaction Code	Description
/AIF/MYRECIPIENTS	Recipients of Current User
/AIF/PERFORMANCE	Performance Tracking
/AIF/PERS_CGR	Runtime Configuration Group
/AIF/PERS_TEST	Test Persistence with Flight Booking
/AIF/RECIPIENTS	Recipients of a User
/AIF/REP_AC_ASGN	AIF Reprocessing Action Assignment
/AIF/REP_AC_DEF	AIF Reprocessing Action Definition
/AIF/RFC_FUNC_GEN	RFC Function Generator
/AIF/RFC_MASS_GEN	Mass RFC Function Generator
/AIF/SERIAL_INDEX	Manual Change of External Index
/AIF/TEXT_HINTS	Transport Text of Hints
/AIF/TJ_CONFIG	Configure Data Transfer
/AIF/TRANSFER	Transfer into AIF Persistence
/AIF/VMAP	Value Mapping
/AIF/VMAP_BASE	Base Transaction for Value Mappings
/AIF/VPN	Maintain Validity Periods

In addition, an *AIF Architect* is provided with the change authorization to the following views:

View/View Cluster	Description
/AIF/ALERT	Define Recipients
/AIF/ERROR_GLB	Global Features
/AIF/ERROR_HDL	Define Applications
/AIF/V_ALRT_USR2	Define Recipients of Other Users
/AIF/V_IDOCSTAT	Mapping of IDoc Status to AIF Status
/AIF/V_NS	Define Namespace
/AIF/V_RFC_FCOL	Define RFC Function Module Collection

View/View Cluster	Description
/AIF/V_RFC_FUNCS	Assign Functions to RFC Function Module Collection
/AIF/V_SYSNAMES	Define Business Systems
/AIF/V_VALID_PER	Define Validity Period

12.9.2.1.2.4 AIF Developer

An *AIF Developer* is responsible for the development of interfaces.

For these tasks, an *AIF Developer* is provided with the following authorizations:

Authorization Object	Activity	Activity Description
/AIF/CFUNC	1	Create or generate
/AIF/CFUNC	2	Change
/AIF/CFUNC	3	Display
/AIF/CFUNC	6	Delete
/AIF/CFUNC	16	Execute
/AIF/CLINK	1	Create or generate
/AIF/CLINK	2	Change
/AIF/CLINK	3	Display
/AIF/CLINK	6	Delete
/AIF/CTEXT	1	Create or generate
/AIF/CTEXT	2	Change
/AIF/CTEXT	3	Display
/AIF/CTEXT	6	Delete
/AIF/CUST	2	Change
/AIF/CUST	3	Display
/AIF/ERR	16	Execute
/AIF/ERR	33	Read

Authorization Object	Activity	Activity Description
/AIF/ERR	34	Write
/AIF/ERR	70	Administer
/AIF/ERR	71	Analyze
/AIF/ERR	75	Remove
/AIF/ERR	A4	Resubmit
/AIF/ERR	GL	General overview
/AIF/HINTS	1	Create or generate
/AIF/HINTS	2	Change
/AIF/HINTS	3	Display
/AIF/HINTS	6	Delete
/AIF/IFDET	1	Create or generate
/AIF/IFDET	2	Change
/AIF/IFDET	3	Display
/AIF/IFDET	6	Delete
/AIF/LFA	3	Display
/AIF/LFA	6	Delete
/AIF/LFA	33	Read
/AIF/LFA	34	Write
/AIF/LFA	71	Analyze
/AIF/PROC	60	Import
/AIF/PROC	61	Export
/AIF/PROC	A4	Resubmit
/AIF/SER	2	Change
/AIF/SER	3	Display
/AIF/TECH	63	Activate
/AIF/VMAP	2	Change

Authorization Object	Activity	Activity Description
/AIF/VMAP	3	Display

In addition, an *AIF Developer* is provided with the authorization to the following transaction codes:

Transaction Code	Description
/AIF/BDC_GEN	Batch Input Structure Generator
/AIF/CUST	Customizing
/AIF/CUST_COPY	AIF Customizing Copy
/AIF/CUST_FUNC	Define Custom Functions
/AIF/CUST_HINTS	Define Custom Hints
/AIF/CUST_LINK	Define Custom Data Link
/AIF/CUST_SMAP_COPY	Copy Customizing
/AIF/CUST_TEXT	Define Custom Message Texts
/AIF/DEL_STRUC_CACHE	Delete Structure Cache
/AIF/DISPMSGSNAP	AIF Display Snapshot
/AIF/DOCU	Interface Documentation Tool
/AIF/EDCHANGES	Error Handling Changes Log
/AIF/ERR	Monitoring and Error Handling
/AIF/ERR_BASE	Error Handling Base
/AIF/GENMSGSNAP	AIF Generate Snapshot
/AIF/IDOC_GEN	IDoc Structure Generator
/AIF/IDOC_IMPORT	AIF IDOC Import
/AIF/IDOC_TEST	Generate Test IDOCs
/AIF/IDXTBL	Index Table Overview
/AIF/IF_TRACE	AIF Interface Trace Level
/AIF/IFB	Interface Builder
/AIF/IFMON	Interface Monitor

Transaction Code	Description
/AIF/IFTEST	Interface Test Tool
/AIF/LFA_CHECK_SEND	Read Files from folder; Send to AIF
/AIF/LFA_UPLOAD_FILE	Upload File to AIF
/AIF/LOG	Interface Logs
/AIF/MYRECIPIENTS	Recipients of Current User
/AIF/PERFORMANCE	Performance Tracking
/AIF/PERS_CGR	Runtime Configuration Group
/AIF/PERS_TEST	Test Persistence with Flight Booking
/AIF/REP_AC_ASGN	AIF Reprocessing Action Assignment
/AIF/REP_AC_DEF	AIF Reprocessing Action Definition
/AIF/RFC_FUNC_GEN	RFC Function Generator
/AIF/RFC_MASS_GEN	Mass RFC Function Generator
/AIF/SERIAL_INDEX	Manual Change of External Index
/AIF/TJ_CONFIG	Configure Data Transfer
/AIF/TRANSFER	Transfer into AIF persistence
/AIF/VMAP	Value Mapping
/AIF/VMAP_BASE	Base Transaction for Value Mappings

In addition, an *AIF Developer* is provided with the change authorization to the following views:

View/View Cluster	Description
/AIF/ACTIONS	Define Actions
/AIF/BDC_V_CONF	Define Pre-Interface Determination for Batch Input
/AIF/CHECKS	Define Checks
/AIF/ERROR_IF	Define Interface-Specific features
/AIF/ERROR_NS	Define Namespace-Specific features
/AIF/FIXVALUES	Define Fix Values

View/View Cluster	Description
/AIF/LFA_SETTINGS	Settings for AIF File Adapter
/AIF/POC	Configuration for POC Integration
/AIF/SMAP	Define Structure Mapping
/AIF/VALMAPS	Define Value Mappings
/AIF/VARIANT_MAPPINGS_ALL	Define Variant Mappings
/AIF/VC_SERIAL	Define Serialization Settings
/AIF/VC_TJ_CONF	Configure Data Transfer
/AIF/VREP_AC_ASG	Assign Automatic Reprocessing Action
/AIF/VREP_AC_DEF	Define Automatic Reprocessing Action
/AIF/V_ALRT_USR3	Define Recipients of Own User
/AIF/V_BDC_IF	Assign Batch Input Session and Creator
/AIF/V_ENGINES	Define Custom-Specfic Engines
/AIF/V_FINF	Define Interfaces
/AIF/V_FINF_ENG	Define Interfaces (Engine Fields)
/AIF/V_FINF_IDOC	Define Interfaces (IDOC fields)
/AIF/V_FINF_TL	Define Trace Level
/AIF/V_IFKEY	Define Interface Key Fields for Variants
/AIF/V_PERS_RTCG	Define Runtime Configuration Group

12.9.2.1.2.5 AIF Business User

An *AIF Business User* is responsible for monitoring interfaces and error handling. This includes editing fields (if allowed in the Customizing of the interface), restarting and canceling data messages, and so on.

For these tasks, an *AIF Business User* is provided with the following authorizations:

Authorization Object	Activity	Activity Description
/AIF/CFUNC	1	Create or generate

Authorization Object	Activity	Activity Description
/AIF/CFUNC	2	Change
/AIF/CFUNC	3	Display
/AIF/CFUNC	6	Delete
/AIF/CFUNC	16	Execute
/AIF/CLINK	1	Create or generate
/AIF/CLINK	2	Change
/AIF/CLINK	3	Display
/AIF/CLINK	6	Delete
/AIF/CTEXT	1	Create or generate
/AIF/CTEXT	2	Change
/AIF/CTEXT	3	Display
/AIF/CTEXT	6	Delete
/AIF/CUST	3	Display
/AIF/ERR	16	Execute
/AIF/ERR	33	Read
/AIF/ERR	34	Write
/AIF/ERR	71	Analyze
/AIF/ERR	75	Remove
/AIF/ERR	A4	Resubmit
/AIF/HINTS	1	Create or generate
/AIF/HINTS	2	Change
/AIF/HINTS	3	Display
/AIF/HINTS	6	Delete
/AIF/LFA	6	Delete
/AIF/LFA	33	Read
/AIF/LFA	34	Write

Authorization Object	Activity	Activity Description
/AIF/LFA	71	Analyze
/AIF/PROC	60	Import
/AIF/PROC	61	Export
/AIF/PROC	A4	Resubmit
/AIF/SER	3	Display
/AIF/VMAP	2	Change
/AIF/VMAP	3	Display

In addition, an *AIF Business User* is provided with the authorization to the following transaction codes:

Transaction Code	Description
/AIF/ERR	Monitoring and Error Handling
/AIF/ERR_BASE	Error Handling Base
/AIF/IFMON	Interface Monitor
/AIF/LFA_UPLOAD_FILE	Upload File to AIF
/AIF/VMAP	Value Mapping

In addition, an *AIF Business User* is provided with the change authorization to the following views:

View/View Cluster	Description
/AIF/V_ALRT_USR3	Define Recipients of Own User

12.9.2.1.2.6 AIF Power User

An *AIF Power User* is responsible not only for monitoring and error handling but also for advanced functions, for example, archiving, correction reports, message snapshots, scheduling file uploads from application server, performance tracking, runtime configuration groups, defining automatic reprocessing, and configuring data transfer (for example, qRFC interfaces).

For these tasks, an *AIF Power User* is provided with the following authorizations:

Authorization Object	Activity	Activity Description
/AIF/CFUNC	1	Create or generate
/AIF/CFUNC	2	Change
/AIF/CFUNC	3	Display
/AIF/CFUNC	6	Delete
/AIF/CFUNC	16	Execute
/AIF/CLINK	1	Create or generate
/AIF/CLINK	2	Change
/AIF/CLINK	3	Display
/AIF/CLINK	6	Delete
/AIF/CTEXT	1	Create or generate
/AIF/CTEXT	2	Change
/AIF/CTEXT	3	Display
/AIF/CTEXT	6	Delete
/AIF/CUST	3	Display
/AIF/ERR	16	Execute
/AIF/ERR	33	Read
/AIF/ERR	34	Write
/AIF/ERR	56	Display archive
/AIF/ERR	70	Administer
/AIF/ERR	71	Analyze
/AIF/ERR	75	Remove
/AIF/ERR	A4	Resubmit
/AIF/ERR	GL	General overview
/AIF/HINTS	1	Create or generate
/AIF/HINTS	2	Change

Authorization Object	Activity	Activity Description
/AIF/HINTS	3	Display
/AIF/HINTS	6	Delete
/AIF/LFA	3	Display
/AIF/LFA	6	Delete
/AIF/LFA	33	Read
/AIF/LFA	34	Write
/AIF/LFA	71	Analyze
/AIF/PROC	60	Import
/AIF/PROC	61	Export
/AIF/PROC	A4	Resubmit
/AIF/SER	2	Change
/AIF/SER	3	Display
/AIF/TECH	63	Activate
/AIF/VMAP	2	Change
/AIF/VMAP	3	Display

In addition, an *AIF Power User* is provided with the authorization to the following transaction codes:

Transaction Code	Description
/AIF/CORRECTIONS	Correction Report
/AIF/CUST	Customizing
/AIF/CUST_FUNC	Define Custom Functions
/AIF/CUST_HINTS	Define Custom Hints
/AIF/CUST_LINK	Define Custom Data Link
/AIF/CUST_TEXT	Define Custom Message Texts
/AIF/DISPMSGSNAP	AIF Display Snapshot
/AIF/DOCU	Interface Documentation Tool

Transaction Code	Description
/AIF/EDCHANGES	Error Handling Changes Log
/AIF/ERR	Monitoring and Error Handling
/AIF/ERR_BASE	Error Handling Base
/AIF/GENMSGSNAP	AIF Generate Snapshot
/AIF/IF_TRACE	AIF Interface Trace Level
/AIF/IFMON	Interface Monitor
/AIF/LFA_CHECK_SEND	Read Files from folder; Send to AIF
/AIF/LFA_UPLOAD_FILE	Upload File to AIF
/AIF/LOG	Interface Logs
/AIF/MYRECIPIENTS	Recipients of Current User
/AIF/PERFORMANCE	Performance Tracking
/AIF/PERS_CGR	Runtime Configuration Group
/AIF/REP_AC_ASGN	AIF Reprocessing Action Assignment
/AIF/REP_AC_DEF	AIF Reprocessing Action Definition
/AIF/SERIAL_INDEX	Manual Change of External Index
/AIF/TJ_CONFIG	Configure Data Transfer
/AIF/TRANSFER	Transfer into AIF Persistence
/AIF/VMAP	Value Mapping
/AIF/VPN	Maintain Validity Periods

In addition, an *AIF Power User* is provided with the change authorization to the following views:

View/View Cluster	Description
/AIF/BDC_V_CONF	Define Pre-Interface Determination for Batch Input
/AIF/CFUNC	Define Custom Functions
/AIF/CLINK	Define Custom Data Link
/AIF/CTEXT	Define Custom Message Text

View/View Cluster	Description
/AIF/LFA_SETTINGS	Settings for AIF File Adapter
/AIF/POC	Configuration for POC Integration
/AIF/VC_TJ_CONF	Configure Data Transfer
/AIF/VREP_AC_ASG	Assign Automatic Reprocessing Action
/AIF/VREP_AC_DEF	Define Automatic Reprocessing Action
/AIF/V_ALRT_USR2	Define Recipients of Other Users
/AIF/V_ALRT_USR3	Define Recipients of Own User
/AIF/V_BDC_IF	Assign Batch Input Session and Creator
/AIF/V_FINF_TL	Define Trace Level
/AIF/V_HINTS	Define Custom Hints
/AIF/V_PERS_RTCG	Define Runtime Configuration Group
/AIF/V_VALID_PER	Define Validity Period

12.9.2.1.2.7 AIF Processing

This template contains the minimal authorization for processing SAP Application Interface Framework messages (for example, for system users). It contains the following authorizations:

Authorization Object	Activity	Activity Description
/AIF/LFA	6	Delete
/AIF/LFA	33	Read
/AIF/LFA	34	Write
/AIF/PROC	60	Import
/AIF/PROC	61	Export
/AIF/PROC	A4	Resubmit

12.9.2.1.2.8 AIF Test Template (Non-Productive)

This role template contains not only SAP Application Interface Framework authorizations and transactions but also several other authorizations and transactions that are needed for some test scenarios.

> → Recommendation
>
> Do not use this template in a productive or a “real” development environment.

12.9.2.1.3 Set Up Interface-Specific and Key Field-Specific Authorizations

Use

In the SAP Application Interface Framework, you can set up interface-specific and key-field-specific authorizations in Customizing for the *SAP Application Interface Framework* (transaction code `AIF/CUST`). This enables you to specify authorizations on the basis of a single message’s content. You can assign interface-specific authorizations that allow or deny users certain activities depending on data received by the interface.

> ✤ Example
>
> A data message includes a plant and a business system identifier. A business user is responsible only for a specific combination of a plant and a business system. You should only authorize them to display and change messages for the specific combination that is relevant to them.

Process

1. You specify the fields that are relevant for authorizations as key fields and include them in a custom single index table. You do this in Customizing for the *SAP Application Interface Framework* under *Error Handling* ▸ *Interface-Specific Features*.
2. You create a custom authorization object in *Maintain the Authorization Objects* (transaction code `SU21`). The authorization object needs to fulfill the following requirements:
   - It requires a field called `ACTVT`.
   - The available activities in the `ACTVT` field must be the same as for the `/AIF/ERR` authorization object (see *Authorization Objects*).
   - It requires one field for each key field that serves as the basis for the authorization.
3. In Customizing for the *SAP Application Interface Framework* under *Error Handling* ▸ *Interface-Specific Features*, you assign the authorization object to an interface, you specify a field sequence number, and you link the key fields to the fields of the authorization object.

> **i Note**
>
> When entering a field sequence number, you must enter the corresponding field sequence number from the definition of the key fields.

Result

You have defined the key fields, created the authorization object, assigned the authorization object to an interface, and linked the key fields to the fields of the authorization object.

Example

Interface-Specific Authorizations

The interface-specific authorization can be used, for example, if you want to specify that users are only able to display or change data if the data was received from a particular business system.

- Interface
  `INTERFACE01`
- Users
  `USER01` and `USER02`
- Systems
  `SYSTEM01` and `SYSTEM02`

The `INTERFACE01` interface can receive data from either `SYSTEM01` or `SYSTEM02`. `USER01` is only responsible for data received from `SYSTEM01` and `USER02` is only responsible for data received form `SYSTEM02`. The interface-specific authorization is used, for example, to ensure that `USER01` is not able to change data received from `SYSTEM02`.

12.9.3 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.

The supplier master data display and maintain 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 chapter.

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.

12.9.4 Agent Framework

12.9.4.1 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 http://help.sap.com/s4hana_op_1610_001 and go to

- *Cross Components* > *Data Protection*.

13 SAP S/4HANA LoB Products for specific Industries

13.1 Automotive

13.1.1 Vehicle processes for Wholesale and Retail

13.1.1.1 Authorizations

Vehicle Processes for Wholesale and Retail uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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

13.1.1.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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*.

13.2 Banking

13.2.1 SAP Financial Customer Information Management (FS-BP)

The security policy with *SAP Financial Customer Information Management* (FS-BP) is very similar to the security policy with the central *SAP Business Partner* (SAP BP).

For more information about authorizations and data storage security in the *SAP Business Partner* , see the 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* > *Security Aspects When Using Business Objects* > *SAP Business Partner Security.*

13.2.1.1 Authorizations

You can create roles in the *SAP Customizing Implementation Guide* (IMG) 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 two 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).

13.2.1.2 Network and Communication Security

When processing total commitment, the communication with other SAP systems (such as Account Management) takes place via Remote Function Call (RFC).

13.2.1.2.1 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).

13.2.1.3 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 http://help.sap.com/s4hana_op_1610_001 and go to

- *Cross Components* > *Data Protection* .

13.2.1.4 Data Storage Security

Authorization object B_CCARD can be used to control access to credit card information that is stored in the business partner. This control falls in the area of responsibility of central *SAP Business Partner* .

You can protect employee data by using authorization groups (authorization object B_BUPA_GRP).

13.2.2 Bank Customer Accounts (BCA)

13.2.2.1 Authorizations

The following standard roles are available in *Bank Customer Accounts (BCA)*:

Role	Name
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

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*, and its subtopic *Authorization Objects*.

Bank Customer Accounts (BCA) also contains the following business transaction events on the subject of authorizations:

Business Transaction Event	Name
SAMPLE_INTERFACE_00011040	AUTH1 account
SAMPLE_INTERFACE_00011700	Authorization checks/authorization type
SAMPLE_INTERFACE_00010950	Check management
SAMPLE_INTERFACE_00010210	Payment item dialog
SAMPLE_INTERFACE_00010410	Payment order dialog
SAMPLE_INTERFACE_00010411	Standing order dialog

13.2.2.2 Network and Communication Security

Bank Customer Accounts (BCA) communicates with the following external systems:

- Payment transaction systems
- *Interest income tax*
- *Financial Accounting (FI)* , if *Financial Accounting (FI)* runs on another system

Encrypt communication with external systems in accordance with the SAP standards.

Communication with all external systems is performed via Remote Function Call (RFC).

13.2.2.3 Data Storage Security

The security of sensitive objects such as savings accounts and checking accounts is guaranteed by the general authorization concept of *Bank Customer Accounts (BCA)*.

For employee accounts, the following security mechanisms are available in addition to the general authorization concept:

The following special authorization objects

F_EMAC_MTH

F_EMAC_TRN

The following special field modification criterion of the Business Data Toolset (BDT)

FMOD1

This criterion is applied to employee accounts.

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

The *Bank Customer Accounts (BCA)* 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 and error message.

The following lists the logical file names and paths used by *Bank Customer Accounts (BCA)* 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:

BKK_PAYMEX_DE_DTA_FILE

Program using this logical file name:

RFBKPAYMEX_DE_DTA

Parameters used in this context: None

BKK_PAYMIN_DE_DTA_FILE

Program using this logical file name:

RFBKPAYMIN_DE_DTA

RFBKPAYMINREST_DE_DTA

RFBKPAYMINREV_DE_DTA

Parameters used in this context: None

Logical File Paths Used in This Application

The logical file name BKK_PAYMEX_DE_DTA_FILE uses the logical file path BKK_PAYMEX_DE_DTA.

The logical file name BKK_PAYMIN_DE_DTA_FILE uses the logical file path BKK_PAYMIN_DE_DTA.

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:

13.2.2.4 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 http://help.sap.com/s4hana_op_1610_001 *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: • BKKPRENOTE • FIBA_ACCNT • FIBA_EFTEX • FIBA_EFTIN • FIBA_ENRCH • FIBA_EVLIM • FIBA_HIERA • FIBA_HOLD • FIBA_ITEM • FIBA_ORDER • FIBA_STORD • FIBA_TERM

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`.

13.2.2.5 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.

The scenario *Payment Document Display/Change/Create* (Tx WZR(1/2/3)) in *Agency Business* (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 30] 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

13.2.3 Loans Management (FS-CML)

13.2.3.1 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	Name	Scope
Loans Officer	SAP_CML_LOANS_OFFICER	• 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, payoff)
Credit Analyst	SAP_CML_CREDIT_ANALYST	• 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	• Loan rollover (individual and mass) • Process correspondence • Management of rollover file • Maintain condition tables
Staff Accountant for Loans	SAP_CML_STAFF_ACCOUNTANT	• Post transactions • Clearing • Create payments • Post and monitor incoming payments • Process waivers and write-offs • Cancellation • Accrual/deferral • Valuation • Generating accounting reports

Role	Name	Scope
Manager of Loans Department	SAP_CML_DEPARTM_MANAGER	• 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	• Update reference interest rates • Maintain condition tables • Maintain new business tables
Technical Administrator	SAP_CML_TECHNICAL_ADMIN	• 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 Maintenance* > *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.

13.2.3.2 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.

13.2.3.3 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 in *SAP Business Partner*, 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* > *Security Aspects When Using Business Objects* > *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 and 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
- RFVOBJ01_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.

For more information, see:

- *Logical File Names*
- *Protecting Access to the File System*
- *Security Audit Logs*

13.2.3.4 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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_DE-STRUCTION

Application Object	Detailed Description	Provided Deletion Functionality
CMLINTPAR	Interested Party	Destruction object CML_INTEREST-PARTY_DESTRUCTION ILM object CML_INTERESTPARTY_DE-STRUCTION
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 Pur-pose 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
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`.

13.2.4 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 SAP *Netweaver Application Server* security guide (**service.sap.com**) that describes the basic security aspects and measures for SAP systems.

13.2.4.1 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 *CM* .
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)

Technical name	Name
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.

13.2.4.2 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	

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
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 andcalculations 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

BAPIs 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. BAPIs 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.

BAPIs 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 BAPIs in *CM* caters mainly to the migration scenarios. Hence these BAPIs are not protected by special authorizations. Authorization checks for BAPIs 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* .

13.2.5 Reserve for Bad Debt (FS-RBD)

13.2.5.1 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:

- Activities
  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

Role	Description
S_A.ADMIN	Access authorizations for administration of the operational SAP system, but **without** access authorization for the following areas: • 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 *Activity*	Authorization Field *RBD Area*	Authorization Field *Organizational Unit*
RBD_CUST	RBD: Customizing	16 *(Execute)*	Not relevant	Not relevant
RBD_EDIT	RBD: Dialog & Batch	01 *(Add or Create)* 02 *(Change)* 03 *(Display)* 05 *(Lock)* 10 *(Post)* 66 *(Update)* 85 *(Reverse)* 86 *(Transfer Post)* 91 *(Reactivate)* 95 *(Unlock)* H1 *(Deactivate)*	According to Customizing (table /IBS/CRB_RBD_P)	According to Customizing (table /IBS/CRB_ORGEIN)

Object	Description	Authorization Field *Activity*	Authorization Field *RBD Area*	Authorization Field *Organizational Unit*
RBD_REPO	RBD: Reporting	Not relevant	According to Customizing (table /IBS/CRB_RBD_P)	According to Customizing (table /IBS/CRB_ORGEIN)
/IBX/EDIT	IPX: Dialog & Batch	02 *(Change)* 03 *(Display)* 06 *(Delete)* 10 *(Post)* 21 *(Transfer Valuation)* 23 *(Maintain)* 41 *(Delete on Database)* 43 *(Release)* 46 *(Aggregate Valuation)* 60 *(Import)* 69 *(Delete Valuation)* 71 *(Analyze)* 78 *(Assign)* 85 *(Reverse)* 93 *(Calculate)* 94 *(Override)*	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 gives the user authorization to use the function *RBD Tool Customizing: Duplicate 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 the 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 "Tokyo".
- 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 in 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`)	Relevant + 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 Management `/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
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
• Drilldown Reporting with References /IBS/RB_REF • IRP: Filling Report for ECF Gate /IBS/RB_ECF_FILL • 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

Transaction	Object (Activity)	RBD Area + Organizational Unit
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
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
• 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
• 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
• IRP: Filling Report for ECF Gate /IBS/RB_ECF_FILL	RBD_EDIT (02)	Not relevant+Not relevant
• IRP: Deletion Report for ECF Gate /IBS/RB_ECF_CLEAR	Not relevant	Not relevant+Not relevant
• IRP: ECF Update Run /IBS/RB_ECF_UPDATE • IRP: ECF Update Run (PPF) /IBS/RB_ECF_UPD_PPF • IRP: ECF Unwinding Run /IBS/RB_ECF_UPD_UNW • IRP: ECF Unwinding Run (PPF) /IBS/RB_UNW_PPF	RBD_EDIT (02, 10)	Relevant +Not relevant

Transaction	Object (Activity)	RBD Area + Organizational Unit
IRP: ECF Creation Process /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 Creation /IBS/RB_ACC_CREATION	RBD_REPO (Not relevant)	Relevant +Not relevant
IVA: Initialization - Future Analysis /IBS/RB_IAS_UPD_INIT	RBD_EDIT (02)	Relevant + Relevant
IRP: ECF Initialization Run /IBS/RB_ECF_UPD_INIT	RBD_EDIT (02, 10)	Relevant +Not relevant
IRP: ECF Initialization (PPF) /IBS/RB_ECF_INIT_PPF	RBD_EDIT (02, 10)	Relevant +Not relevant

RBD Area Menu, Impairment Processing Extension - Environment Folder

Transaction	Object (Activity)	RBD Area
Upload Files /IBX/FILE_UPLOAD	/IBX/EDIT (60)	Not relevant
Maintain Import Data /IBX/IMP_CHNG	/IBX/EDIT (43, 60)	Not relevant
Main Dialog /IBX/MAIN	/IBX/EDIT (03, 10, 94)	Not relevant
Restrict Data Selection /IBX/SELECTION	Not relevant	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
Import CSV Files /IBX/IMPORT	/IBX/EDIT (60)	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 Impairment Categorization /IBX/IC_ASSIGN	/IBX/EDIT (78)	Not relevant

Transaction	Object (Activity)	RBD Area
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
Display Logs /IBX/COCKPIT	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.

13.2.5.2 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).

13.2.5.2.1 Communication Destinations

For Remote Function Call (RCF) 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.

13.2.5.3 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.

13.3 Higher Education and Research

13.3.1 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 SAP NetWeaver Security Guides also apply to the SAP ECC Industry Extension Higher Education & Research component. The SAP NetWeaver 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 SAP NetWeaver 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	

Role	Description
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	
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)

Role	Description
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 `Academic Advisor`
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 `Student`

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 more information, see application help for Business Rule Framework plus (BRFplus) in SAP Library for SAP NetWeaver on SAP Help Portal at *http://help.sap.com/netweaver* > *SAP NetWeaver 7.0 (2004s)* > *SAP Netweaver 7.0 including Enhancement Package 3* > *SAP NetWeaver* > *SAP NetWeaver by Key Capability* > *Application Platform by Key Capability* > *Business Services* > *Business Rule Framework plus (BRFplus)* > *Concepts* > *Authorizations*

13.3.2 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 a 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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

Application	Detailed Description	Provided Deletion Functionality
PSCM	Student Lifecycle Management: Public Sector Campus Management	`HRIQ_ATTDN`Data Destruction in Student Lifecycle Management

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 ERP (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 ERP .

4. Business users can request unblocking of blocked data for customers, vendors and central business partners by using the transaction `BUP_REQ_UNBLK`.
5. 5.If you have the necessary authorizations, you can unblock data by running the transaction `BUPA_PRE_EOP` and `CVP_UNBLOCK_MD`.
6. 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 Managemen* . 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*

13.3.3 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 SAP NetWeaver Security Guide.

13.3.4 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 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, see the product assistance for SAP NetWeaver on SAP Help Portal at Start of the navigation path *http://help.sap.com/netweaverInformation* > *SAP NetWeaver Library* > *Function-Oriented View* > *System Security for SAP NetWeaver AS for ABAP Only*

13.4 Professional Services

13.5 Commercial Project Inception and Lean Staffing

The following guide covers the information that you require to operate Commercial Project Inception and Lean Staffing securely.

13.5.1 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 .

13.5.2 Before You Start

It is important that you read and understand the information contained in the Authorizations [page 302] 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	*SAP NetWeaver Security Guide - All sections*
SAP ECC	*SAP ERP Central Component Security Guide - All sections*

For a complete list of the available SAP Security Guides, see **service.sap.com/securityguide** on the SAP Service Marketplace.

13.5.3 User Management and Authentication

SAP ECC Industry Extension Professional Services uses the user management and authentication mechanisms provided with the *SAP NetWeaver* platform, particularly the *SAP NetWeaver Application Server ABAP* . Consequently, the security recommendations and guidelines for user management and authentication that are described in the *SAP NetWeaver 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.

13.5.4 Authorizations

Use

The business function *Commercial Project Inception and Lean Staffing* uses the authorization concept provided by the SAP NetWeaver AS for 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 SAP NetWeaver 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 infotypes)	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	

Authorization Object	Field	Value	Description
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 VTWEG SPART KDGRP KOSTL ACTVT	VBAK-VKORG VBAK-VTWEG VBAK-SPART KNVV-KDGRP VBAK-KOSTL 02, 03, 06	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.
V_PRS_LS_I (new)	PRCTR ACTVT	VBAP-PRCTR 02, 03, 06	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.
C_PRPS_LS (new)	PS_FKOKR PS_FKSTL PRCTR ACTVT	PRPS-FKOKR PRPS-FKSTL PRPS-PRCTR 02, 03, 06	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.
K_PRS_LS	PRCTR ACTVT	AUFK-PRCTR 02, 03, 06	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.
PRS_LS_FC	EMP_LEVEL ACTVT	Level 1, 2 or 3 02, 03, 06	See description below.

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.

13.5.5 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 information about access to this data, see Authorization [page 302] .

For information about deletion and archiving of this data, see *Archiving* .

13.6 Public Sector

13.6.1 Finance

13.6.1.1 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 SF01 (client-specific). To determine which paths are used by your system, you can activate the relevant settings in the Security Audit Log.

13.6.1.1.1 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
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

Role	Name
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

Authorization Object	Name
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

13.6.1.1.2 Grants Management

Standard roles for Grants Management (PSM-GM)

Function	Name	Function
SAP_FI_GM_GRANT_ANALYST	Grants Management: Grant Analyst	M aster 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

Function	Name	Function
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
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 the *SAP Help Portal* at *help.sap.com* > *SAP ERP Central Component* > *Accounting* > *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

13.6.1.1.3 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* on SAP Service Marketplace at *service.sap.com/securityguide* > *SAP NetWeaver Security Guide* > *Security Aspects for Connectivity and Interoperability.*

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.

13.6.1.1.4 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 the implementation guide of *Public Sector Management:*

- *Funds Management-Specific Postings* > *Earmarked Funds and Funds Transfers* > *Field Control for Earmarked Funds and Funds Transfers* > *DefineField Status Variant* /Assign *Field Status Variant to Company Code* / *Define Field Status Groups*
- *Actual and Commitment Update/Integration* > *Integration* > *MaintainField Status for Assigning FM Account Assignments*

For more information, see the documentation on *Funds Management* on the SAP *Help Portal* at *help.sap.com* > *ERP Central Component* > *Accounting* > *Public Sector Management*.

For Grants Management, note the following system settings in the implementation guide of *Public Sector Management,underFunds Management Government* > *Master Data* > *Grant*

- *GM Grant Control: Field Group for Authorizations*
- *Maintain Grant Authorization Types*
- *Maintain Grant Authorization Groups*

13.6.2 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).

13.6.2.1 Authorizations

SAP Public Sector Collection and Disbursement (SAP PSCD) and SAP Tax and Revenue Management (SAP TRM) uses the authorization concept provided by the SAP NetWeaver AS for 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 SAP NetWeaver 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 SAP NetWeaver 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	AUTHTYP_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
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

Authorization Object	Field	Value	Description
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: Autorization 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
F_KKCOL	ACTVT	01 Create or Generate 02 Change 03 Display 06 Delete 16 Execute 39 Check AF Prompts	PSCD Co-Liability: Authorization for Co-Liabilities

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 02 Change 03 Display 06 Delete F1 Approve	TRM Object: Authorization for Form Handling and Form View
F_PSFH_ REV	FMCA_ABTYP	01 Create or Generate 02 Change 03 Display 06 Delete F1 Approve	TRM Object: Authorization for Form Handling and Revenue Type
F_PSFH_ACT	ACTVT	01 Create 02 Change 03 Read	TRM Object: Authorization for Form Handling
F_PSFH_FBT	FBTYP	01 Create or Generate 02 Change 03 Display 06 Delete F1 Approve	TRM Object: Authorization for Form Handling and Form Bundle Type
F_PSFH_STA	FMCA_FBSTA	01 Create or Generate 02 Change 03 Display 06 Delete F1 Approve	TRM Object: Authorization for From Handling and Status
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 02 Change 03 Display 06 Delete	TRM Object: Authorization for Master Data Relationship Category

13.6.2.2 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 SAP NetWeaver Security Guide.

13.6.3 Multichannel Foundation for Utilities and Public Sector (Public Sector)

13.6.3.1 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 SAP NetWeaver Security Guide.

13.7 Utilities

13.7.1 Authorizations

The way that authorization management is organized within a company depends on factors such as the size of the company and its organizational structure, amongst others. Authorization management must be tailored to each company's specific requirements and processes. SAP Utilities uses the authorization concept provided by `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 `SAP NetWeaver` 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Authorization Objects

The following table provides an overview of the authorization objects available for SAP Utilities, sorted by component:

Component	Authorization Object	Description
Regional Structure	E_REGIOGRP	Authorization Object for Regional Structure Group
Scheduling	E_PORTION	Authorization Object for Portion
Master Data	E_CONTRACT	Authorization Object for IS-U Contract
	E_CUST_CHG	Authorization Object for Maintaining Sample Customers in IS-U
	E_GRID	Authorization Object for Grid.
	E_INSTLN	Authorization object for utility installation.

Component	Authorization Object	Description
	E_INSTLN2	Authorization Object for Utility Installation – IDEX
	E_INSTFACT	Installation Facts
	E_LOYALACC	Authorization Object for Loyalty Account
	E_NBSERVI2	Authorization Object for Point of Delivery Service – IDEX
	E_NBSERVIC	Authorization Object for Point of Delivery Service
	E_POD	Authorization Object for Point of Delivery
	E_POD2	Authorization Object for Point of Delivery Transaction – IDEX
	E_PREMISE	Authorization Object for Premise
	E_PROPERTY	Authorization object for owner allocation.
Device Management	E_CERTIFCT	Authorization Object for Device Certification
	E_CONNOBJ	Authorization Object for Connection Object
	E_CRFC_CHG	Authorization Object for Changing Certification in Device Category
	E_DEV_CHNG	Authorization Object for Device Modification
	E_DEV_PREL	Authorization Object for Changing Validation Relevance of Devices
	E_DEV_REL	Authorization Object for Device Relationships
	E_DEVGRP	Authorization Object for Device Group
	E_DEVLOC	Authorization Object for Device Locations
	E_INST_REM	Authorization Object for Installation, Removal, and Replacement

Component	Authorization Object	Description
	E_LOG_REG	Authorization Object for Logical Registers
	E_METER_RR	Authorization Object for Meter Reading Results
	E_MR_DOC	Authorization Object for Meter Reading Documents and Orders
	E_MR_DOC1	Authorization Object for Meter Reading Documents and Orders
	E_MR_DOC2	Authorization Object for Meter Reading Documents w.r.t. Company Code
	E_MRD_UNIT	Authorization Object for Meter Reading Unit
	E_REG_REL	Authorization Object for Register Relationships
	E_SAMP_LOT	Authorization Object for Sample Lot
	E_SEAL_IN	Authorization Object for Seal Management
Energy Data Management	E_EDM_PRF2	Authorization Object for Processing EDM Profiles – IDEX
	E_EDM_PROF	Authorization Object for Processing EDM Profiles
	E_EDM_SETT	EDM Settlement
	E_INSTLN3	Authorization Object for Profile Allocation in Utility Installation
	E_PROF_IMP	Authorization Object for Profile Import to IS-U EDM
Billing	E_B_BIL_PL	Authorization Object for Budget Billing Plan
	E_BILL_CL	Authorization Object for Billing Class
	E_DEV_RATE	Authorization Object for Rate Data
	E_DISCOUNT	Authorization Object for Discount/ Surcharge

Component	Authorization Object	Description
	E_INSTCALC	Authorization Object for Asynchronous Formula Instance Calculation
	E_OPERAND	Authorization Object for Operands
	E_PRESCL	Authorization Object for Price Adjustment Clause
	E_PRICE1	Authorization Object for Price
	E_PRICEUPL	Authorization Object for Importing Prices from Excel
	E_RATE	Authorization Object for Rate
	E_RATE_CAT	Authorization Object for Rate Category
	E_RATE_DET	Authorization Object for Rate Determination
	E_SCHEMA	Authorization Object for Schema
	E_TRIGGER	Authorization Object for Billing Order
	E_VARIANT	Authorization Object for Variants
Invoicing	E_INVOICE	Authorization Object for Invoicing Contract Accounts
Contract Accounts Receivable and Payable	E_DEREG_WO	Authorization Object for Write-Off in Deregulation Scenarios
Customer Service	E_DISC_DOC	Authorization Object for Disconnection Document for Installation
	E_ISUEBPP	Authorization Object for Activities (ISU_ABPP)
	E_MOVE_IN	Authorization Object for Move-In
	E_MOVE_OUT	Authorization Object for Move-Out
	E_PRDOC	Authorization Object for Parked Document
	E_REDEMPTN	Authorization Object for Redemption
Intercompany Data Exchange	E_DRGSCEN	Authorization Object for Supply Scenario

Component	Authorization Object	Description
	E_DTX_TASK	Authorization Object for Processing Data Exchange Tasks
	E_IDE_CHKT	Authorization Object for IDE Check Framework Tool for Deregulation
	E_INV_DOC	Authorization Object for Bill Receipt Document or Payment Advice Note
	E_INV_ETHI	Authorization Object for Aggregated Posting to Contract Account of Service Provider
	E_SERVPROV	Authorization Object for Service Provider
	E_SWTDOC	Authorization Object for Switch Document
Advanced Metering Infrastructure	E_AMI_EM	Authorization Object for IS-U Event Management
	E_AMI_IN	Authorization Object for AMI Inbound Confirmation Methods
	E_AMI_MON	Authorization Object for AMI Monitoring
	E_AMI_MSG	Authorization Object for Sending Messages
	E_AMI_OPST	Authorization Object for Operational State of Advanced Meter
	E_AMI_SMDS	Authorization Object for AMI Simplified Master Data Synchronization
	E_DISC_AMI	Authorization Object for Remote Disconnection
	E_MDUSCONF	Authorization Object for MDUS Configuration
	E_TSCALC	Authorization Object for Time Series Calculation
	EAMI_CO_IN	Authorization Object for Inbound Confirmation

Component	Authorization Object	Description
	ETOUEXCEPT	Authorization Object for TOU Exceptions
	ETOUEXRESP	Authorization Object for TOU Exception Responses

To display the standard authorization objects for SAP Utilities in your system, proceed as follows:

1. In the SAP menu, choose *Tools* > *Administration* > *User Maintenance* > *Authorizations and Profiles* > *Edit Authorizations Manually* (transaction `SU03`).
2. Select object class `IS_U` (Industry Solutions – Utilities) and choose *List* > *Authorizations.*

13.7.2 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.

13.7.3 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.

13.7.4 Deletion of Personal Data

SAP Utilities 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 Utilities uses SAP ILM to support the deletion of personal data. SAP delivers end of purpose checks for SAP Utilities-specific objects.

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

The end of purpose checks for SAP Utilities are based on those of 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 for which business partners 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 ERP) and in SAP CRM, the end of purpose checks cover both applications so 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 business partner is used in a franchise fee contract
- Check if business partner is used in a loyalty account
- Check if business partner is used as a service provider
- Check if business partner is used as an owner
- Check for open disconnection documents for business partner
- Check if business partner is used in role `ISUI` (installer)
- Check for open error messages for 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.

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: `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 ERP.
   - 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 SAP Utilities.

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*

13.7.5 Multichannel Foundation for Utilities and Public Sector

13.7.5.1 Authorizations

The Multichannel Foundation for Utilities and Public Sector solution uses the authorization concept provided by the SAP NetWeaver Application Server for ABAP.

Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to the Multichannel Foundation for Utilities and Public Sector solution. The SAP NetWeaver 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, see the SAP Help Portal at:http://help.sap.com/nwgateway ▶ *SAP Gateway Security Guide* ▶ *Authorizations in the SAP System* ▶ *Roles in the SAP Gateway Landscape* ▶.

Service Roles and Authorizations in SAP S/4HANA

For SAP 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` `/IWBEP/RT_USS_SRVUSR`	`SAP_ISU_UMC_SRV` `/IWBEP/RT_USS_SRVUSR`	`/IWFND/RT_GW_USR` `/IWBEP/RT_USS_SRVUSR`
`UMC_REF_USR`	`SAP_CRM_UMC_ODATA` `/IWBEP/RT_USS_INTUSR`	`SAP_ISU_UMC_ODATA` `/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 ERP 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

Gateway Security Guide

See http://help.sap.com/nwgateway

User and Role Administration for SAP NetWeaver AS for ABAP

See http://help.sap.com/netweaver under *Identity Management*

Authorization Templates

See http://help.sap.com/netweaver, under *System Administration Tasks* > *Authorizations* > *Maintaining Authorizations*

Setting up Authorizations with Role Maintenance

See http://help.sap.com/netweaver, under *System Administration TasksAuthorizationsMaintaining Authorizations*

13.7.5.2 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 ERP 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

RFC/ICF Security Guide

See http://help.sap.com/netweaver under *SAP NetWeaver 7.0 Including Enhancement Package 1* > *SAP NetWeaver Security Guide* > *Security Guides for Connectivity and Interoperability*.

13.8 Oil and Gas

13.8.1 Authorizations

SAP Oil & Gas uses the authorization concept provided by the SAP NetWeaver AS for 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 SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

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:

Role	Description
SAP_BR_SHIPPING_SPECIALIST_IOG	This role is enhanced to support IS-OIL business processes and must be used along with other roles delivered by SAP. For example, SAP_BR_SHIPPING_SPECIALIST. This role includes Transportation and Distribution shipment processing, master data maintenance for shipment, shipment processing and Transportation Scheduler Workbench operations.
SAP_BR_INVENTORY_MANAGER_IOG	This role is enhanced to support IS-OIL business processes and must be used along with other roles delivered by SAP. For example, SAP_BR_INVENTORY_MANAGER. This role manages inventory with respect to quantity and value. It also includes IS-OIL specific Quantity Conversion Interface (QCI) and tank management related tasks.
SAP_BR_BILLING_CLERK_IOG	This role is enhanced to support IS-OIL business processes and must be used along with other roles delivered by SAP. For example, SAP_BR_BILLING_CLERK.. This role is used mostly for IS-OIL specific exchanges netting related tasks.
SAP_BR_SUPPLYCHAIN_MANAGER_IOG	This role is enhanced to support IS-OIL business processes and must be used along with other roles delivered by SAP. For example, SAP_BR_PURCHASING_MANAGER, SAP_BR_PURCHASER, SAP_BR_INTERNAL_SALES_REP.The Supply Chain Manager role is primarily responsible for ensuring proper supply of hydrocarbons downstream of the Oil & Gas value chain. This role is also responsible for handling the exchange business for refined products with exchange partners.
SAP_BR_TRANSP_SCHDLR_IOG	This role is enhanced to support IS-OIL business processes and must be used along with other roles delivered by SAP. For example, SAP_BR_PURCHASING_MANAGER, SAP_BR_SALES_MANAGER, SAP_BR_CONTRACT_MANAGER_CC . The transportation scheduler schedules as well as execute hydrocarbon logistics movements along the supply chain. The scheduler is responsible for multiple terminals and/or transport systems as well as multiple crude or finished products. As part of the job, the scheduler schedules primarily bulk shipments, usually in planning cycles like weekly/monthly cycles. The scheduling includes vessels, barges, rail, truck, and pipeline for crude, feed stocks and refined products.

SAP_BR_PRICING_SPECIALIST_IOG	This is an IS-OIL role for pricing. The pricing specialist is responsible to Create Price, Change Price, Mass change of prices, and Mass Creation of prices. Sets up the price lists for preparation and issue the price lists for execution. Keeps the prices consistent across different channels. Checks compliance of prices according to guidelines e.g. discount policy. Receives price data from stakeholders for example, for a campaign or from product or marketing manager. Views global market price quotes for oil products in the system and can also modify these price quotes in system based on prior approvals. Is responsible for creation of F&A pricing based on the price quotes that are available in system, Requests price data from business units and provides information for the (customer) data specialist. Also gives the proposal for relevant product. In addition to that, also triggers configuration changes (for example, collaborate with IT), trigger creation/completion/correction of material master data, and trigger price approval. And also gives the notification to purchaser/production planner in case of poor availability.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used.

Authorization Object	Field	Value	Description
O_OIJ_NOM	OIJ_NOMTYP OIJ_TSYST OIJ_SHPR OIJ_CARR OIJ_LOC	Display	If you are authorized for a particular transport system, , location only then the you can view/change the event data in Mass Change Event Fiori App.
O_OIJ_NOM	OIJ_NOMTYP OIJ_TSYST OIJ_SHPR OIJ_CARR OIJ_LOC	Change	If you are authorized for a particular nomination type, transport system, shipper, carrier and location only then the you can view/change the nomination data in the Nomination Fiori app.

Authorization Object	Field	Value	Description
O_OIJ6_INV	OIJ_LOC MATNR BWTAR	Display	If you are authorized for particular location and material for which you are running the regional inventory only then data/inventory data is displayed in the Regional Inventory Fiori app.
O_O3DEFA	WERKS		Determines which activities are allowed for O3DEFAULTS
O_OI0_TCD	TCD		This object controls which Oil downstream transactions the user may access. The field values are identical to the transaction code.
O_OIA_EXG	OIA_EXGTYP BUKRS	Create or generate Change Display Print Edit messages	Determines which activities are allowed for maintenance of Exchange Headers and assignment of sales and purchasing contracts.
O_OIA_LIA	OIA_UPEDOC BUKRS Create or generate Display	Create Display	Determines which activities are allowed for maintenance of Exchange Logical Inventory Adjustments.
O_OIA_NDOC	BUKRS	Create or generate Change Display Print, edit messages Lock	Determines which activities are allowed for maintenance of the Exchange Netting document.
O_OIF_PBL	OIF_PBLTYP OIRB_AUTGR	Create or generate Change Display	Determines which activities are allowed for maintenance of Business Locations.

Authorization Object	Field	Value	Description
O_OIG_SHP	BETRVORG TPLST OIG_SHTYPE		Determines which activities are allowed for maintenance of certain shipments. The shipments are determined by shipment type and transportation planning point.
O_OIG_SPT	VSTEL		Determines if: The assignment of deliveries to TD shipments according to the shipping point of the deliveries is allowed or not. The user can change deliveries when in the TD shipments function, according to the shipping point of the deliveries, or whether this is not allowed.
O_OIJ_3WP	OIJ_3WPACT	Create Change Display	This authorization object is checked whenever a user tries to access the 3WP transaction.
O_OIJ_LOCN	OIJ_LOCTYP	Create or generate Change Display	This authorization object is used to authorize maintaining locations in Trader's and Schedulers Workbench. The locations are determined by the location type.
O_OIJ_NMST	OIJ_NOMTYP	Activate/Deactivate Display	This authorization object is checked whenever a status code is activated or deactivated.
O_OIJ_NOM	OIJ_NOMST	Create or generate Change Display Print, edit messages Lock	

Authorization Object	Field	Value	Description
O_OIJ_NOMA	OIJ_NOMTYP OIJ_NOMST	Create or generate Change Display	This authorization object is checked whenever a user tries to access the nomination data.
O_OIJ_NOMI	VSART WERKS	Create or generate Change Display	This authorization object is used to authorize maintenance of nominations in Trader's and Schedulers Workbench. The nominations are created with reference to a transport system.
O_OIJ_PROL	KTOKD KTOKK WERKS LGORT	Create or generate Change Display Print, edit messages Lock	This authorization object is used to authorize maintaining partner role assignments in Trader's and Schedulers Workbench. The TSW partner roles are determined by the vendor grp, cust. grp. and the plant and storage location attached to a role type at a location or transport system.
O_OIJ_SPTP	OIJ_SPTYPE OIJ_SIMTYP	Change Display	Determines which activities (Display or Change) are allowed for different Stock Projection Types (SP types).
O_OIJ_TCKT	OIJ_NOMTYP OIJ_TSYST OIJ_SHPR OIJ_CARR OIJ_LOC	Create or generate Change Display Print, edit messages Lock	

Authorization Object	Field	Value	Description
O_OIJ_TKT	OIJ_TKTTYP	Create Change Display Delete Retrieve from archive Rebook Reverse	This authorization object is checked whenever a user tries to access the Ticket Data
O_OIJ_TSYS	VSART WERKS	Create Change Display	This authorization object is used to authorize maintaining transport system in Trader's and Schedulers Workbench. The transport systems are determined by the shipping type
O_OIR_PBLD	OIF_PBLTYP OIRA_RNBT OIF_DTSECT	Create or generate Change Display	Determines whether a user is authorized to view a specific business location master data section on a detailed business type level.
O_OIR_PBLG	OIF_PBLTYP OIF_DTSECT	Create or generate Change Display Print, edit messages Lock	Determines whether a user is authorized to view a specific business location master data section on a detailed business type level.
O_OIRB_PBL	OIF_PBLTYP OIRB_AUTGR OIRA_RNBT	Create or generate Change Display	

13.8.2 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 My Nominations , Regional Inventory View and Mass Change Events in the TSW area, following services are needed:

- TSW_MYNOMINATIONS_SRV_01

- TSW_REGIONAL_INVENTORY_SRV_01
- TSW_MYEVENTS_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 SAP NetWeaver Security Guide.

13.8.3 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:

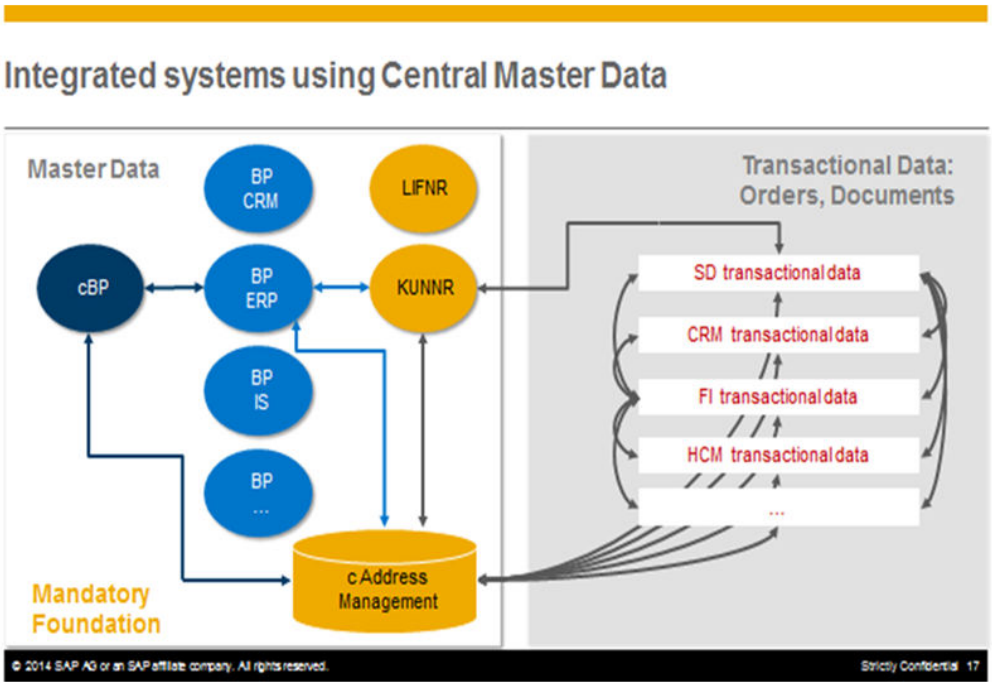
- **Display**: The system does not display blocked data.
- **Change**: It is not possible to change a business object that contains blocked data
- **Create**: It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up**: It is not possible to copy a business object 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.

Integration with Other Solutions

In the majority of cases, different installed applications run interdependently as shown in following graphic.



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 Deletion Functionality

Application	*Detailed Description*	*Provided Deletion Functionality*

IS-OIL Downstream	The customer/vendor blocking report will check the consuming application to determine end of purpose of the customer/vendor.
	
	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 *IS-OIL Downstream* application has to be made.
	
	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 `CVP_OIL_EOP_CHECK`.
		ILM Enabled Archiving objects:
		`OIG_DRIVER`
		`OIG_VEHCLE`
		`OIG_TPUNIT`
		`OIJ_NOMIN`
		`OIJ_TICKET`
		`IS_OIFSPBL`
		Data Destruction objects:
		`OIJ_SCHED_DESTRUCTION`
		`OIJ_PARTNER_DESTRUCTION`
		`OIA_EXGDOCU_DESTRUCTION`
		`OIL_TAS_TPI_DESTRUCTION`

Decoupled TSW `TSW_ECC`	The customer/vendor blocking report will check the consuming application to determine end of purpose of the customer/vendor.
	
	In a Decoupled TSW scenario , the checks for usage of customer/vendor in TSW application specific documents like nomination is made.
	
	The `TSW_ECC` 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 `TSW_ECC` will be delivered in the class `CVP_TSW_ECC_CHECK`.
		ILM Enabled Archiving objects:
		`OIG_VEHCLE`
		`OIG_TPUNIT`
		`OIJ_NOMIN`
		`OIJ_TICKET`
		`IS_OIFSPBL`
		Data Destruction objects:
		`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 ERP (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 ERP.
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 ERP.
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*

13.8.4 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, see *Read Access Logging* in the documentation for *SAP NetWeaver* on the SAP Help Portal under http://help.sap.com.

13.9 SAP for Insurance

Note that the following security information applies to SAP Claims Management (FS-CM) only and not to other SAP for Insurance solutions.

13.9.1 Authorizations

SAP Claims Management 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 for Application Server ABAP` also apply.

The SAP NetWeaver 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 SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP Claims Management uses the following PFCG roles:

PFCG Role	Description
`SAP_ICL_CLAIM_HANDLER`	Role for claim handling
`SAP_ICL_CLAIM_VIEWER`	Role for claim display
`SAP_ICL_CLAIM_CUSTOMIZING`	Role for customizing
`SAP_ICL_CLAIM_AUTHORIZATION`	Role for payments, reserves, subrogation
`SAP_ICL_CLAIM_PROCUREMENT`	Role for procurement
`SAP_ICL_CLAIM_BATCH`	Role for background processing

SAP Claims Management uses the following portal roles:

Portal Role	Description
Claim Center Agent (Insurance) (`com.sap.pct.isins.ccagent.claim_center_agent`)	The portal role is delivered in Business Package for Center Agent (Insurance) 1.30.
Claim Handler (Insurance) (`com.sap.pct.isins.clmhandl.claim_handler`)	This portal role has the additional authorization to create and release payments up to a specific amount. The amount is defined in Customizing of the backend system. The portal role is delivered in Business Package for Claim Handler (Insurance) 1.30.

Portal Role	Description
The following Web Dynpro ABAP applications are embedded in these portal roles: • Claims Search: `icl_wd_claimsearchapp_ui` • Claims Summary: `icl_wd_claimsummary_ui` • Post Proc FROI (Post Processing of First Report of Injury): `icl_wd_postprocfroi_ui`	

Standard Authorization Objects

General List

You can find a list with all standard authorization objects in the SAP Help Portal at **`http://help.sap.com/insurance-cm`** under *Application Help* > *Claims Management* > *Claim* > *Administration of the Claims Management System* > *Authorizations in the Claims Management System*.

Authorization Objects for Use of Enterprise Search

You can find the relevant authorization objects in the in the SAP Help Portal at **`http://help.sap.com/insurance-cm`** under *Application Help* > *Claims Management* > *Claim* > *Administration of the Claims Management System* > *Search Using Enterprise Search*, chapter *Integration*.

Authorization Objects for Use of BRFplus

You can find the relevant authorization objects in the in the SAP Help Portal at **`http://help.sap.com/insurance-cm`** under *Application Help* > *Claims Management* > *Claim* > *Structuring Business Processes* > *Business Rule Framework plus (BRFplus)* > *Authorizations for Using BRFplus*.

13.9.2 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.

13.9.3 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 http://help.sap.com/s4hana_op_1610_001 > *Product Assistance* > *Cross Components* > *Data Protection*.

Relevant Application Objects and Available Deletion Functionality

Application	Detailed Description	Provided Deletion Functionality
Archiving of Claims (Archiving Object `ICLCLAIM`)	For more information, see `Archiving of Claims`.	ILM Object `ICLCLAIM` (see SAP Note 1976123)
Archiving of Claim Bundles (Archiving Object `ICLECCEVT`)	For more information, see `Archiving of Claim Bundles`.	ILM Object `ICLECCEVT` (see SAP Note 1976123)

Relevant Application Objects and Available EoP/WUC functionality

Application	Implemented Solution (EoP or WUC)	Further Information
Archiving of Claims (Archiving Object `ICLCLAIM`)	EoP	See SAP Note 1976123
Archiving of Claim Bundles (Archiving Object `ICLECCEVT`)	EoP	See SAP Note 1976123

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 and vendor master data in Customizing for *SAP Insurance* under *Claims Management* > *Claim* > *Technical Settings* > *Lock Claims*.

13.9.4 Read Access Logging

In Read Access Logging (RAL), 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 ZIP attachments from the following SAPNote: 2369248.

Extract these ZIP files, and import the RAL configurations using the Import function for configurations using transaction `SRALMANAGER`.

SAP Claims Management logs health data, bank account, and social security number. You can find the configurations as described in the Read Access Logging [page 30] chapter.

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

Configuration	Fields Logged	Business Context
`ICL_SSN`	• `ICLC_ICL_BP_MINI_SCREEN-TAXTYPE` (Tax Number Category) • `ICLC_ICL_BP_MINI_SCREEN-TAXNUM` (Business Partner Tax Number)	In the Mini Business Partner the tax number is only logged if the user has selected the tax number category **`US1`**.

14 SAP S/4HANA LOB Products

14.1 Asset Management

14.1.1 Maintenance Operations

14.1.1.1 Authorizations in Plant Maintenance

Plant Maintenance uses the authorization concept provided by the SAP 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Roles for Plant Maintenance

Role	Description
SAP_COCKPIT_EAMS_MAINT_WORKER2	*Maintenance Worker 2* This role contains all the functions that a maintenance worker requires to carry out their work effectively and safely. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.
SAP_COCKPIT_EAMS_GENERIC_FUNC2	*Generic EAM Functions 2* The purpose of this role is to provide the maintenance planner with a broad range of functions necessary for planning and executing maintenance activities. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.

14.1.2 Environment, Health and Safety

14.1.2.1 User Administration and Authentication

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

The SAP NetWeaver 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 12] in the *Introduction* section.

14.1.2.1.1 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 12] in the *Introduction* section.

User ID	Type	Password	Description
Business processing user	Dialog user	To be entered	Business user of *EHS*

User ID	Type	Password	Description
E-mail inbound processing user	Communication user	Not needed	User to process the incoming e-mails of *EHS*
Workflow engine batch user	Background user	Not needed	User for the background processing of workflows in *EHS*

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).

14.1.2.1.2 Standard Roles

In *Environment, Health, and Safety* (EHS), you use specific roles in the application to access content. These roles are designed to support your EHS business processes.

The following roles are delivered:

- Roles for Foundation Processes [page 349]
- Roles for Managing Incidents [page 350]
- Roles for Managing Health and Safety Processes [page 350]
- Roles for Managing Environmental Data [page 351]

Unless shown in the tables below, the roles are delivered without authorization profiles. The authorization profiles are then generated from these roles.

> **i Note**
>
> The EHS roles that are delivered contain specific configuration such as object-based navigation (OBN). In consequence, customizing these roles has a certain level of complexity. Custom roles can be created as follows without losing their specific configuration:
>
> 1. Create your custom PFCG role.
> 2. Copy the menu structure from the SAP_EHSM_MASTER role or from the other roles that are delivered.
> 3. Generate the authorization profile.
> 4. Assign the custom role to end users.

For more information about roles for EHS, go to http://help.sap.com/s4hana_op_1610_001, enter *Foundation for EHS* into the search bar, press `Enter`, and open the search result with that title.

14.1.2.1.2.1 Roles for Foundation Processes

Role	Description
SAP_EHSM_MASTER	Master PFCG role for all EHS functionalities.
SAP_EHSM_PROCESS_ADMIN	End user role for the person who is technically responsible for the workflow-based processes of EHS. This role assigns the necessary authorizations in the SAP S/4HANA system. This role can receive workflow items.
SAP_EHSM_FND_WF_PERMISSION	System user role for the Workflow Engine. This role contains the additional authorization profiles needed to process the workflows in the background. The users who process workflows in the background should, in addition to this role, be assigned the SAP_BC_BMT_WFM_SERV_USER role. For processing incident management workflows, the users should also receive the same authorizations as the SAP_EHSM_HSS_INCIDENT_MANAGER role. For processing risk assessment workflows, the users should also receive the same authorizations as the SAP_EHSM_HSS_ENVMGR, SAP_EHSM_HSS_HYGIENIST, and SAP_EHSM_HSS_SAFEMGR roles.
SAP_EHSM_HSS_EML_REC	System user role for the e-mail recipient. This role contains the authorization profiles needed to receive and process e-mails.
SAP_EHSM_FND_MIGRATION	End user role for the migration. You use this role to access the *Legacy System Migration Workbench*. Depending on the content you want to migrate, you still need to configure and assign the corresponding business role (including the profiles). For example, to access the incident business object and migrate the incident content, you also need the SAP_EHSM_HSS_INCIDENT_MANAGER role assigned (along with the corresponding profiles).

14.1.2.1.2.2 Roles for Managing Incidents

Back End Roles for Incident Management

Role	Description
SAP_EHSM_HSS_INCIDENT_MANAGER	End user role for the incident manager. This role can receive workflow items.
SAP_EHSM_HSS_INCIDENT_REPORTER	End user role for the incident reporter.
SAP_EHSM_HSS_INCIDENT_NOTIFIED	End user role for a person who is notified during the processing of an incident. This role can receive workflow items.
SAP_EHS_INC_INJRSILLNESSES_APP	End user role for the users of the app *Injuries and Illnesses - Detailed Analysis*.
SAP_EHS_INC_REPORINCIDENT_APP	End user role for the users of the app *Report Incident*.
SAP_EHS_INC_DETAILEDANALYS_APP	End user role for the users of the app *Incidents - Detailed Analysis*.

Front End Roles for Incident Management

Role	Description
SAP_BR_INDUSTRIAL_HYGIENIST	End user role for the users of the SAP Fiori launchpad. This role contains the *Health and Safety – Incident Management* business catalog and the *Incident Management* tile group.

14.1.2.1.2.3 Roles for Managing Health and Safety Processes

Back End Roles for Managing Health and Safety Processes

Role	Description
SAP_EHSM_HSS_CHEMAPPR	End user role for the chemical approver.
SAP_EHSM_HSS_CHEMREQ	End user role for the chemical requestor.
SAP_EHSM_HSS_HSMGRCORP	End user role for the corporate health and safety manager.
SAP_EHSM_HSS_ENVMGR	End user role for the environmental manager.
SAP_EHSM_HSS_HAZSUBMGR	End user role for the hazardous substance manager.
SAP_EHSM_HSS_HYGIENIST	End user role for the industrial hygienist.

Role	Description
SAP_EHSM_HSS_LINEMGR	End user role for the line manager.
SAP_EHSM_HSS_SAFEMGR	End user role for the safety manager.
SAP_EHSM_HSS_SDSCLERK	End user role for the safety data sheet clerk.
SAP_EHSM_HSS_SMPLTECH	End user role for the sampling technician.

Front End Roles for Managing Health and Safety Processes

Role	Description
SAP_BR_HAZMAT_MANAGER	End user role for the users of the SAP Fiori launchpad. This role contains the *Health and Safety – Hazardous Materials Management* business catalog and the *Hazardous Materials Management* tile group.
SAP_BR_INDUSTRIAL_HYGIENIST	End user role for the users of the SAP Fiori launchpad. This role contains the *Health and Safety – Incident Management* business catalog and the *Incident Management* tile group.

14.1.2.1.2.4 Roles for Managing Environmental Data

Back End Roles for Managing Environmental Data

Role	Description
SAP_EHSM_HSS_ENVMGR	End user role for the environmental manager. This role can receive workflow items.
SAP_EHSM_ENV_TECHNICIAN	End user role for the environmental technician. This role can receive workflow items.

Front End Roles for Managing Environmental Data

Role	Description
SAP_BR_ENVIRONMENTAL_MANAGER	End user role for the users of the SAP Fiori launchpad. This role contains the *Health and Safety – Environment Management* business catalog and the *Environment Management* tile group.
SAP_BR_PRODN_OPTR_EHS_INFO	End user role for the users of the SAP Fiori launchpad. This role contains the *Health and Safety – Production Operator* business catalog and the *Production Operator* tile group.

14.1.2.1.3 Standard Authorization Objects

The following security-relevant authorization objects are used in *Environment, Health, and Safety*:

- Authorization Objects for Foundation Processes [page 352]
- Authorization Objects for Managing Incidents [page 356]
- Authorization Objects for Managing Health and Safety Processes [page 359]
- Authorization Objects for Managing Environmental Data [page 363]
- Authorization Objects for Integration [page 364]

14.1.2.1.3.1 Authorization Objects for Foundation Processes

Authorization Object	Field	Value	Description
EHFND_CHDC (Change Document)	ACTVT	03 (Display)	Activity
	BO_NAME	EHFND_LOCATION (Location)	Business Object Name
		EHHSS_INCIDENT (Incident)	
		EHHSS_INCIDENT_ACTION (Incident Action)	
		EHHSS_RISK_ASSESSMENT (Risk Assessment)	
		EHHSS_RAS_ACTION (Risk Assessment Action)	
		EHHSS_RISK (Risk)	
		EHHSS_AGENT (Agent)	
		EHHSS_JOB (Job)	
		EHFND_DATA_AMOUNT (Amount)	
		EHFND_CHEMICAL (Chemical)	
EHFND_LOC (Location)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
		A3 (Change status)	

Authorization Object	Field	Value	Description
	LOCAUTHGRP		Location Authorization Group
	LOCBUSAREA		Business Area
	LOCCOMP		Company Code
	LOCCOST		Cost Center
	LOCPLANT		Plant ID
	LOCSTATUS	01 (New) 02 (Active) 03 (Inactive) 04 (Historic)	Location Status
	LOCTYPE		Location Type
EHFND_DCTR (Default Controls)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
S_PB_CHIP (Chips for side panel)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete) 16 (Execute)	Activity (03 and 16 are needed for displaying the information in the side panel)

Authorization Object	Field	Value	Description
	CHIP_NAME	X-SAP-WDY-CHIP:EHFNDWD-CHIP_LOC_STRUCT	Web Dynpro ABAP: CHIP ID
		X-SAP-WDY-CHIP:EHHSSWD-CHIP_ASSWRKF_LOC_LIST	
		X-SAP-WDY-CHIP:EHHSSWD-CHIP_INC_LOC_LIST	
		X-SAP-WDY-CHIP:EHHSSWD-CHIP_RSK_LOC_LIST	
		X-SAP-WDY-CHIP:EHHSSWD-CHIP_RSK_LOC	
		X-SAP-WDY-CHIP:EHHS-SUCWCHP_ASSWRKF	
		X-SAP-WDY-CHIP:EHHS-SUCWCHP_INC_LOC	
		X-SAP-WDY-CHIP:EHHS-SUCWCHP_APPRCHEM	
		X-SAP-WDY-CHIP:EHFN-DUCWCHP_EASYWORKLIST	
		X-SAP-WDY-CHIP:EHFN-DUCWCHP_LAUNCHPAD	
		X-SAP-WDY-CHIP:FND_UI_CHM_SAFETY_INSTR_CHIP	
		X-SAP-WDY-CHIP:BSSP_SW_FEEDS	
		X-SAP-WDY-CHIP:BSSP_SW_ACTIVITIES	
		X-SAP-WDY-CHIP:BSSP_NOTES	
		X-SAP-WDY-CHIP:EHFND_UI_CHM_OVP_ALOC_VB_CHIP	

Authorization Object	Field	Value	Description
		X-SAP-WDY-CHIP: EHFND_UI_CHM_OVP_APPR_LOC_CHIP	
		X-SAP-WDY-CHIP: EHFND_UI_CHM_SAFETY_INSTR_CHIP	
		X-SAP-WDY-CHIP: EHHS-SUCWCHP_SPLCP	
		X-SAP-WDY-CHIP: EHHS-SUCWCHP_SPLCP_HEAT-MAP	
		X-SAP-WDY-CHIP:EHHS-SUCWCHP_SPLPH	
S_PB_PAGE (Configuration for side panel and home pages)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
	CONFIG_ID	EHFND_LOC_OIF_SIDE_PANEL	Configuration Identification
		EHFND_CHM_SIDE_PANEL	
		EHHSS_HAZ-SUBMGR_HOMEPAGE	
		EHHSS_HYGIENIST_HOME-PAGE	
		EHHSS_INC_MANAGER_HOMEPAGE	
		EHHSS_HSMGRCORP_HOMEPAGE	
		EHHSS_SMPLTECH_HOME-PAGE	
	PERS_SCOPE	0 (No Personalization	Web Dynpro: Personalization
		1 (User)	
		2 (View Handle)	
		4 (All)	
		5 (Configuration)	

Authorization Object	Field	Value	Description
EHFND_WFT (Workflow Tools)	ACTVT	16 (Execute)	Activity
	TCD	All transactions of workflow tools	Transaction Code
EHFND_WFF (Workflow and Processes)	EHSM_COMP	HSS (Health and Safety)	Component of EHS
	PURPOSE	Process Purpose (see Customizing activity Specify Process Definitions)	Process Purpose
	EHSM_PVAR	Process Variant (see Customizing activity Specify Process Definitions)	Name of Process Variant
	EHSM_PCACT	CANCELPROC (Cancel Process)	Activity of Task or Process
EHFND_EXPP (Export Profile)	ACTVT	01 (Create, Generate)	Activity
	EHFND_EXPP		Configured Export Profile
EHFND_CHM (Chemical)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHFND_REGL (Regulatory List Content)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity

14.1.2.1.3.2 Authorization Objects for Managing Incidents

Authorization Object	Field	Value	Description
EHHSS_INC2 (Incident Report)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity

Authorization Object	Field	Value	Description
	ORGUNIT_ID		Organizational Unit ID
	PLANT_ID		Plant ID
	FORM_NAME		Form Name
EHHSS_INC6 (Incident)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete) 60 (Import) C5 (Re-open)	Activity
	INC_CATEG	001 (Incident) 002 (Near Miss) 003 (Safety Observation)	Incident Category
	INC_STATUS	00 (Void) 01 (New) 02 (In Progress) 03 (Closed) 04 (Re-opened)	Incident Record Status
	ORGUNIT_ID		Organizational Unit ID
	PLANT_ID		Plant ID
	LOC_ID		Location ID
	COUNTRY		Country Key
	REGION		Region (State, Province, County)

Authorization Object	Field	Value	Description
	ACCESS_LEV	000 (Basic Information / Standard Data) 001 (Person Involved Access) 002 (Injury / Illness Access) 003 (Confidential Access) 004 (Date of Birth Access)	Incident Access Level For more information about creating and assigning access levels to tabs, see the following Customizing activities for *Environment, Health, and Safety* under *Incident Management* > *General Information*: • *Create Incident Access Levels* • *Assign Access Levels to Tabs*
EHHSS_INC7 (Incident Group)	ACTVT	02 (Change) 03 (Display) 06 (Delete)	Activity
	NM_GROUP	Entries in Customizing activity *Specify Near Miss Groups* under *Environment, Health, and Safety* > *Incident Management* > *Incident Recording*	Near Miss Group
	SO_GROUP	Entries in Customizing activity *Specify Near Miss Groups* under *Environment, Health, and Safety* > *Incident Management* > *Incident Recording*	Safety Observation Group
	INC_GROUP	Entries in Customizing activity *Specify Near Miss Groups* under *Environment, Health, and Safety* > *Incident Management* > *Incident Recording*	Incident Group
S_TABU_DIS	DICBERCL	EHMI (Incident) EHMF (Foundation)	Authorization Group

Authorization Object	Field	Value	Description
	ACTVT		Activity
S_PROGRAM	P_GROUP	EHINCXML (XML reports) EHFNDPRG (Foundation program authorization) EHFNDWFT (Workflow tools) EHHSSINC (Incident management)	Authorization group ABAP/4 program
	P_ACTION	SUBMIT	User action ABAP/4 program

14.1.2.1.3.3 Authorization Objects for Managing Health and Safety Processes

Authorization Object	Field	Value	Description
EHHSS_AGT (Agent)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHFND_CTRL (Control Master Data)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHHSS_JOB (Job)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHHSS_PEP (Personal Exposure Profile)	ACTVT	03 (Display)	Activity
	PERSA		Personnel Area
	BTRTL		Personnel Subarea

Authorization Object	Field	Value	Description
EHHSS_RAS (Risk Assessment, Risks, Controls on Risks and Control Inspections)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete) A8 (Process mass data)	Activity
	RAS_TYPE	EHHSS_RAT_ENV (Environment) EHHSS_RAT_HEA (Health) EHHSS_RAT_JHA (Job Hazard Analysis) EHHSS_RAT_SAF (Safety)	Risk Assessment Type
	LOCAUTHGRP		Location Authorization Group
	LOCPLANT		Plant ID
	LOCCOST		Cost Center
	LOCCOMP		Company Code
	LOCBUSAREA		Business Area
EHHSS_RASP (Proposal of Health Surveillance Protocol)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
	HSP_TYPE		Health Surveillance Protocol Type
EHHSS_HSP (Health Surveillance Protocol Master Data)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
	HSP_TYPE		Health Surveillance Protocol Type
	COUNTRY		Country Key

Authorization Object	Field	Value	Description
	REGIO		Region (State, Province, County)
EHFND_CHM (Chemical)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHFND_CHA (Chemical Approval)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHFND_DCTR (Default Controls)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHFND_DSC (Dynamic Statement Creation)	EHFND_DSCC	Entries in Customizing activity *Enable BO Fields for Dynamic Creation of Statements* under *Environment, Health, and Safety* > *Foundation for EHS* > *General Configuration*	Dynamic Statement Creation enabled fields
EHFND_RCH (Request Chemical)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity (01 and 02 are needed for using the service "request chemical approval")
EHFND_VEN (Vendor)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity

Authorization Object	Field	Value	Description
EHHSS_SI (Safety Instruction)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
EHFND_SPL (Sample Management)	ACTVT	03 (Display) 16 (Execute) 23 (Maintain)	Activity
	EHSM_COMP	HSS	Component
	LOCAUTHGRP		Location Authorization Group
	LOCPLANT		Plant ID
	LOCCOST		Cost Center
	LOCCOMP		Company Code
	LOCBUSAREA		Business Area
EHFND_SPLM (Sampling Method)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
S_TABU_DIS	DICBERCL	EHMR (Risk Assessment)	Authorization Group
S_PROGRAM	P_GROUP	EHFNDPRG (Foundation program authorization) EHFNDWFT (Workflow tools) EHHSSRAS (Risk Assessment)	Authorization group ABAP/4 program
	P_ACTION	SUBMIT	User action ABAP/4 program

14.1.2.1.3.4 Authorization Objects for Managing Environmental Data

Authorization Object	Field	Value	Description
EHFND_REQ (Compliance Requirement)	ACTVT	03 (Display) 23 (Maintain)	Activity
	REQDOMAIN		Compliance Requirement Domain
	LOCCOUNTRY		Country
	LOCREGION		Region
EHENV_SCEN (Compliance Scenario)	ACTVT	03 (Display) 06 (Delete) 23 (Maintain) 76 (Enter)	Activity
	LOCTYPE		Location Type
	LOCSTATUS		Location Status
	LOCAUTHGRP		Location Authorization Group
	LOCPLANT		Plant ID
	LOCCOST		Cost Center
	LOCCOMP		Company Code
	LOCBUSAREA		Business Area
	LOCCOUNTRY		Country
	LOCREGION		Region
S_PB_CHIP (Environment Management Chips)	CHIP_NAME	X-SAP-WDY-CHIP:EHENV_CHIP_ENTER_VALUES X-SAP-WDY-CHIP:EHENVUCWCHP_ISSUESWORKLIST	Web Dynpro ABAP: CHIP ID

14.1.2.1.3.5 Authorization Objects for Integration

The table below shows the security-relevant authorization objects that are used by *Environment, Health, and Safety* (EHS) if you integrate the system with other SAP components.

Authorization Object	General Settings	Further Information
P_ORGIN (HR: Master data)	Display authorizations are required for specific infotypes.	See Customizing for *Environment, Health, and Safety* under *Foundation for EHS* > *Integration* > *Human Resources Integration* > *Check Authorizations for Person Information*
P_ORGXX (HR: Master data - extended check)	Activation of the check by this authorization object is required. P_ORGXX can be used in addition to or instead of the check by the authorization object HR: Master Data.	
P_APPL (HR: Applicants)	Display authorizations are required for specific infotypes.	
B_BUPA_RLT (Business partner: BP roles)	Authorizations are required for the following BP roles: CBIH10 - External person HEA010 - Physician HEA030 - Health center (hospital)	
B_BUPA_FDG (Business partner: field groups)	Special authorization check for individual field groups in the business partner dialog box.	

14.1.2.1.4 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
<MOC system>	No	RFC (3, H)	Connection to the *SAP Management of Change* system (ABAP/3- and HTTP/H-Connection)

Destination	Delivered	Type	Description
<OH system>	No	RFC	Connection to the *Occupational Health* application of *SAP EHS Management* as part of the *SAP ERP* system
<EWM system>	No	RFC	Connection to the *Extended Warehouse Management* system

> **i Note**
>
> EHS does not provide any authorizations for:
>
> - *SAP Management of Change*
> - *Occupational Health* of *SAP EHS Management* as part of *SAP ERP*

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

14.1.2.2 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 19] 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:
  - `repincidents1` (*Report Incident*)
  - `injillanalyss1` (*Injuries and Illnesses - Detailed Analysis*)
  - `incdntanalyss1` (*Incidents - Detailed Analysis*)
- 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_mycs1` (*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 back-end system, open transaction `SICF`. Under `/default_host/sap/bc/webdynpro/sap/`, activate all Web Dynpro services that start with `ehenv` and `ehfnd`.

14.1.2.3 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:

- EHHSS_INCIDENTS_XML

- Program R_EHHSS_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 EHHSS_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 SAP NetWeaver Security Guide.

14.1.2.4 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 of category *Action*, 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 28] in the *Introduction* section.

14.1.2.4.1 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 http://help.sap.com/s4hana_op_1610_001 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
Incidents	Archiving object `EHHSS_INC`
Incident Summary Reports	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 http://help.sap.com/s4hana_op_1610_001 under *Product Assistance* > *Enterprise Business Applications* > *Asset Management* > *Environment, Health, and Safety* > *Incident Management (EHS-MGM-INC)* > *Data Archiving in Incident Management*.

Application Objects and Available Deletion Functionality in Health and Safety Management

Application Objects	Provided Deletion Functionality
Risk Revisions	Archiving object `EHHSS_RSV`
Risks	Archiving object `EHHSS_RSK`
Risk Assessments	Archiving object `EHHSS_RAS`
Safety Instructions	Archiving object `EHHSS_SI`
Control Evaluations	Archiving object `EHHSS_CEVL`
Control Inspections	Archiving object `EHHSS_CINS`
Control Replacements	Archiving object `EHHSS_CRPL`
Sampling Campaigns	Archiving object `EHHSS_SPLC`
Samplings	Archiving object `EHFND_SPLG`
Chemical Approvals	Archiving object `EHFND_CHA`
Assignment of Person to Locations	Archiving object `EHFND_LOCP`

Application Objects	Provided Deletion Functionality
Assignment of Person to Jobs	Archiving object `EHFND_JOBP`
Sampled Person	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 http://help.sap.com/s4hana_op_1610_001 under *Product Assistance* > *Enterprise Business Applications* > *Asset Management* > *Environment, Health, and Safety* > *Health and Safety Management (EHS-MGM-RAS)* > *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 Environmental Management

Application Objects	Provided Deletion Functionality
Compliance Scenario Actions	Archiving object `EHENV_SAC`

For more information about application objects and deletion functionality, see the product assistance for SAP S/4HANA on the SAP Help Portal at http://help.sap.com/s4hana_op_1610_001 under *Product Assistance* > *Enterprise Business Applications* > *Asset Management* > *Environment, Health, and Safety* > *Environment Management (EHS-MGM-ENV)* > *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
Incident Management (`EHS_INC`)	`EHHSS_INC_EOP_CHECK_BP`	The check determines whether the business partner is used in: • Incidents • Tasks in incidents

Application	End of Purpose Check	Further Information
Health and Safety (EHS_HS)	EHHSS_HS_EOP_CHECK_BP	The check determines whether the business partner is used in: • Risk assessment projects • Tasks in risk assessment projects • Risks • Control inspections • Control evaluations • Control replacements
Health and Safety (EHS_HS_EXPOSURE)	EHHSS_EXP_EOP_CHECK_BP	The check determines whether the business partner is assigned to: • Job positions • Location positions • Samplings as sampled person
Environment Management (EHS_ENV)	EHENV_EOP_CHECK_BP	The check determines whether the business partner is used in tasks of category *Action*.

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*.

14.1.2.4.2 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 application 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
Involved Person - Basic Information	<concatenate name> • *Injured Person Name* • *Phone Number* • *Email* *Role(s)* *Incident Type* *Privacy Case* *Injured on Site* *Injured on Duty* *Additional Criteria* *Fatality* *Location of Death* *Cause of Death* *Statement of Involved Person*	Logs basic information of the person who is involved in the incident.
Involved Person - Injury-Illness Information	<concatenate name> • *Injured Person Name* • *Phone Number* • *Email* *Classification* *Injury/Illness Type* *Injury/Illness Description* *Body Part* *Body Part Description* *Body Side*	Logs information on the injuries or the illness of the person who is involved in the incident.

Configuration	Fields Logged	Business Context
Involved Person - Treatment Information	<concatenate name> • *Injured Person Name* • *Phone Number* • *Email* *First Physician* *Further Treatment Provider* *Treatment Beyond First Aid* *Emergency Room* *Inpatient Overnight* *Unconsciousness* *Immediate Resuscitation* *Comment* *To First Aid* *To Further Treatment*	Logs information on the treatment of the person who is involved in the incident.
Involved Person - Reports and Documents	<concatenate name> • *Injured Person Name* • *Phone Number* • *Email* *File Name* (of report forms) *File Name* (of documents)	Logs the files of reports and documents that are assigned to the involved person.
Incident - Reports and Documents	*File Name* (of report forms) *Reference* (Report forms of person references) *File Name* (of documents) *Reference* (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 30] chapter.

14.1.2.5 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 22] in the *Introduction* section.

14.1.2.6 Other Security-Relevant Information

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

14.1.2.6.1 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 HR Absences from the incident. For all actions, HR authorizations are checked.

14.1.2.6.2 Security Settings for the Report Incident App

You use the *SAP Cloud Platform, mobile service for SAP Fiori* to implement the app *Report Incident*. For more information on the security settings of the *SAP Cloud Platform, mobile service for SAP Fiori*, see the SAP Help Portal at https://help.sap.com. There, search for **`SAP Cloud Platform, mobile service for SAP Fiori User Guide`**.

14.1.3 Resource Scheduling

14.1.3.1 Authorizations for Resource Scheduling

The SAP S/4HANA Asset Management solution for resource scheduling uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 SAP NetWeaver Security Guide under *User Administration and Authentication*.

Standard Roles

The table below shows the standard roles that are used.

Role	Description
SAP_BR_MAINTENANCE_PLANNER_RSH	*Maintenance Planner - Resource Scheduling* You can use this role as a template for creating your own role. Please note that this business role must be created in the front-end system.

SAP does not deliver a back-end role for resource scheduling for asset management. You must create your own role in the back-end system using transaction **PFCG**. To this role, you must assign the authorization objects listed in the table below.

Standard Authorization Objects

The following table below shows the security-relevant authorization objects that are used:

Authorization Object	Fields	Values	Description
I_TCODE	TCD	**IW38**	*PM: Transaction Code*
I_AUART	IWERKAUFART	Enter the relevant plants and maintenance order types.	*PM: Order Type*
I_BEGRP	BEGRP	Enter the relevant technical object authorization group.	*PM: Authorization Group*
I_IWERK	IWERK	Enter the relevant plant.	*PM: Maintenance Planning Plant*
I_INGRP	IWERK INGRP	Enter the relevant planning plants and maintenance planner groups.	*PM: Maintenance Planner Group*
I_SWERK	SWERK	Enter the relevant maintenance plant.	*PM: Maintenance Plant*
I_KOSTL	KOKRS KOSTL	Enter the relevant controlling area and cost center.	*PM: Cost Centers*
C_ARPL_ART	AP_ART	Enter the relevant work center category.	*CIM: Work center category*

Authorization Object	Fields	Values	Description
C_ARPL_WRK	ACTVT WERKS	ACTVT: **03** (display work centers) WERKS: Enter the relevant plants for which the user may display work centers.	*CIM: Work center- plant*

14.2 Commerce

14.2.1 Commerce Management

14.2.1.1 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).

14.2.1.1.1 Authorizations

Standard Roles

SAP delivers standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles. You specify roles that are used in Contract Accounts Receivable and Payable (FI-CA) in the SAP Easy Access menu by choosing *Tools* > *Administration* > *User Maintenance* > *Information System* > *Roles* > *Roles by Complex Selection Criteria* and entering SAP_FI_CA* in the *Role* field.

Contract Accounts Receivable and Payable (FI-CA) delivers only single roles.

Before using the roles listed, you may want to check whether the standard roles delivered by SAP meet your requirements.

Standard Authorization Objects

You can easily recognize the authorization objects currently used in Contract Accounts Receivable and Payable (FI-CA) from their technical name as follows:

1. In the SAP Easy Access menu choose *Tools* > *Administration* > *User Maintenance* > *Information System* > *Authorization Objects* > *By object name*.
2. Enter `F_KK*` in the *Authorization Object* field and execute your search.

In the result list, you can display the details for each selected authorization object such as authorization fields, documentation and permitted activities, if defined.

In addition, for the Clarification Processing area, the authorization object `S_CFC_AUTH` exists; for the Correspondence area, the authorization object `P_CORR`; and for prepaid processing, authorization objects exist that follow the naming convention `F_PREP*`. You can use Customizing roles to control access to the configuration of Contract Accounts Receivable and Payable (FI-CA) in the SAP Customizing Implementation Guide (IMG).

14.2.1.1.2 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 SAP NetWeaver Security Guide.

14.2.1.1.3 Data Protection

Contract Accounts Receivable and Payable (FI-CA) might process data (personal data) that is subject to the data protection laws applicable in specific countries.

Contract Accounts Receivable and Payable (FI-CA) uses SAP ILM to support the deletion of personal data as described in the following sections. SAP delivers end of purpose checks 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 business partner.

For information about the Customizing of blocking and deletion for Contract Accounts Receivable and Payable, see *Configuration: Simplified Blocking and Deletion below. Displaying Blocked Data*.

Also, see the sections mentioned below in the Product Assistance of Contract Accounts Receivable and Payable under *Basic Functions* > *SAP Business Partner* > *Blocking and Deleting Personal Data*.

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, see Displaying Personal Data.

Relevant Application Objects and Available Deletion Functionality

For more information, see the following sections of the application documentation:

- Blocking and Deleting Personal Data
- Deleting Business Partners
- Dealing with Personal Data Outside the Business Partner

Relevant Application Objects and Available EoP functionality

For more information, see section Check for End of Purpose in Contract Accounts Receivable and Payable.

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.

14.2.1.1.4 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`.
- You create EDRs of the type `AMOUNT` using function module `FKKBI_EDR_AMOUNT_CREATE`.

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: • /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 for "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 your own IDocs containing credit card information, see the SAP NetWeaver Security Guide under *Security Guides for Connectivity and Interoperability Technologies* > *Security Guide ALE (ALE Applications) in SAP NetWeaver Release 7.30*.
>
> 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	*BAPI - FI-CA Prepaid Account: Create*
BAPI	BAPI_CTRACPREPAIDACCOUNT_CHNG	*BAPI - FI-CA Prepaid Account: Change*
BAPI	BAPI_CTRACPREPAIDACCOUNT_GETD	*BAPI - FI-CA Prepaid Account: Read Detail Data*
BAPI	BAPI_CTRACDOCUMENT_CREATE	*BAPI: FI-CA Post Document*

RFC	`FKK_PREP_PCARD_STORE`	*Prepaid: Store Payment Data in DFKK_PCARD*
RFC	Event 1421 (function module `FKK_SAMPLE_1421`)	*Parallel Billing: Call Settlement*
RFC	`FKK_BUPA_MAINTAIN_SINGLE`	*Maintain Business Partner*
RFC	`/1FE/`<billable item class_`BIT_CREATE_API`	Generated RFC interfaces for transferring billable items with payment information
Enterprise Service	`CashPointPaymentCreateNotification_In`	*External Cash Point Payment*
Web Service	`ECC_CASHPOINTPAYMENTCRTNO`	*External Cash Point Payment*
File	Report `RFKKPCDS`	*Payment Cards: Execute Billing*
ALE/IDoc	`ALE_CTRACDOCUMENT_CREATE`	*BAPI -> IDoc: ALE_CTRACDOCUMENT_CREATE(FI-CA Post document)*

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.
>
> Please 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.

14.2.1.1.5 Other Security-Relevant Information

In Contract Accounts Receivable and Payable (FI-CA), some objects and special activities are protected by special authorizations. The associated authorization object is `F_KK_SOND`. See table `TFKAUTH` (use transaction `SM30` to display) for information on all activities that you can protect with this authorization object.

14.3 Finance

14.3.1 Treasury and Financial Risk Management

14.3.1.1 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* .

14.3.1.1.1 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 *SAP NetWeaver Security Guide (Complete)* on *SAP Service Marketplace* at **http:// service.sap.com/securityguide** .

For more information about the technical system landscape, see the resources listed in the table below.

Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for SAP Bank Communication Mangement and the underlying components such as SAP NetWeaver	*Master Guide*	**http://service.sap.com/instguides**
High availability	*High Availability for SAP Solutions*	**http://sdn.sap.com/irj/sdn/ha**
Technical landscape design	See applicable documents	**http://sdn.sap.com/irj/sdn/landscapedesign**
Security	See applicable documents	**http://sdn.sap.com/irj/sdn/security**

14.3.1.1.2 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 *SAP Integration Package for SWIFT Configuration Guide* .

You need to create these users before XI configuration.

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

Creation of role SWIFT_ADMINSTRATOR is described in the *SAPIntegration Package for SWIFT Configuration Guide* .

14.3.1.1.3 Authorizations

Standard Roles

The table below shows the standard roles that are used by the SAP *Bank Communication Management*.

Role	Description
SAP_XI_IS_SERV_USER	Exchange Infrastructure: Integration Server Service User
SWIFT_ADMINSTRATOR	Operating SWIFT interface. See Integration Package for SWIFT Configuration Guide
SAP_BPR_CASH_MANAGER	Cash Manager

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP *Bank Communication Management*.

Authorization Object	Description
F_FEBB_BUK	Company Code Bank Statement
F_REGU_BUK	Automatic Payment: Activity Authorization for Company Codes

14.3.1.1.4 Communication Destinations

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

Destination	Delivered	Type	User, Authorizations	Description
INTEGRATION_SERVER	No	RFC	XIAPPLUSER Role SAP_XI_APPL_SERV_USER	*service.sap.com/instguides* > *SAP NetWeaver Configuration Guide SAP XI*
LCRSAPRFC	No	RFC		*service.sap.com/instguides* > *SAP NetWeaver Configuration Guide SAP XI*
SAPSLDAPI	No	RFC		*service.sap.com/instguides* > *SAP NetWeaver Configuration Guide SAP XI*

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

14.3.1.1.5 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_RFEBKAT0_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBKAT0
- 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_RFEBEST0_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBEST0
- 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 .

14.3.1.2 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 the *SAP ERP Central Component Security Guide* under *Accounting* → *SAP Banking* → Bank Customer Accounts (BCA) [page 269]

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 *SAP ERP Central Component Security Guide* under *Accounting* → *SAP Banking* → Bank Accounting (FI-BL) [page 67]

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

For information about the processes of *SAP In-House Cash* and about ALE Customizing, see the Configuration Guide and the business process documentation athttp://service.sap.com/ibc

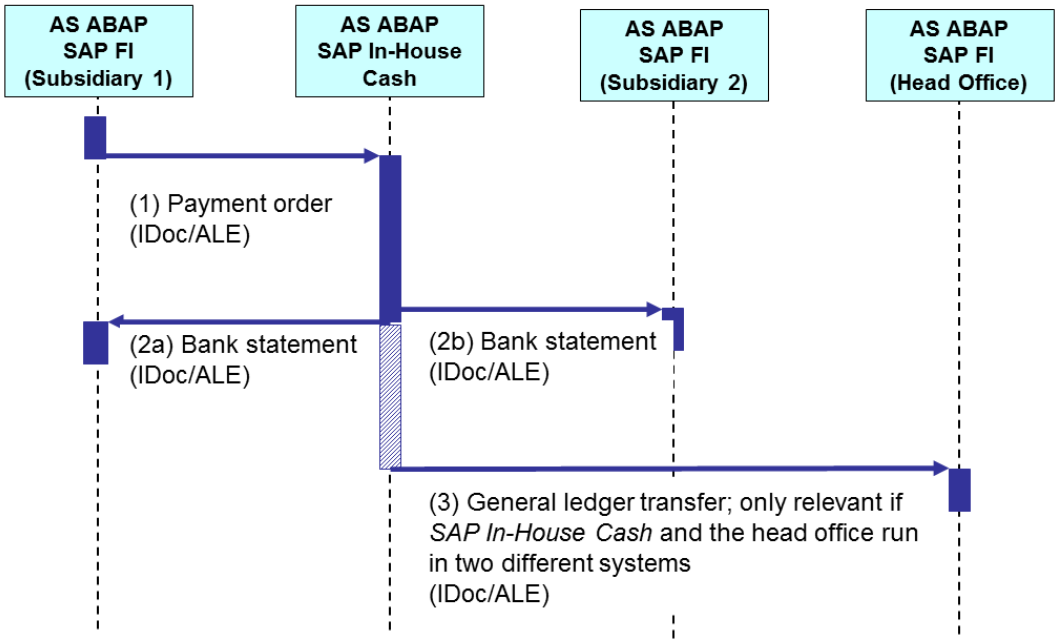
14.3.1.2.1 Security Aspects of Data, Data Flow and Processes

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

> **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.

14.3.1.2.1.1 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.

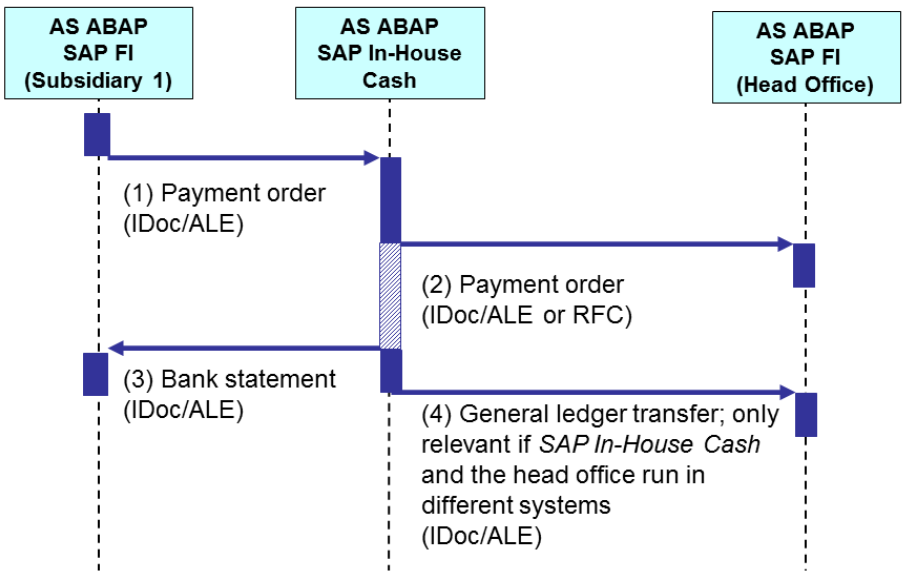


The table below shows the security aspect to be considered for the process step and what mechanism applies.

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

14.3.1.2.1.2 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.



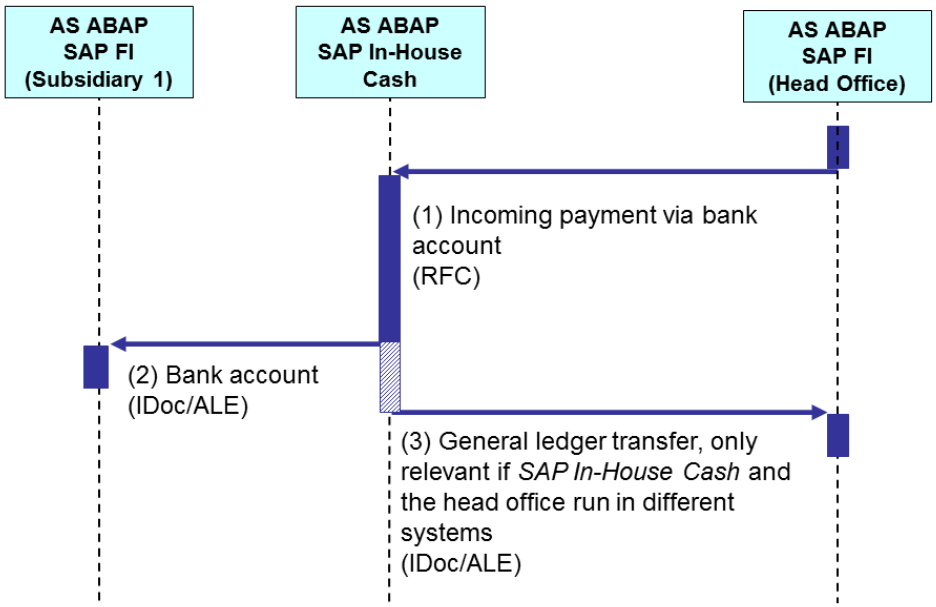
The table below shows the security aspect to be considered for the process step and what mechanism applies.

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
3	Bank statement (IDoc/ ALE)	User type: dialog user or technical user
4	General ledger transfer; only relevant if *SAP In-House Cash* 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* .

14.3.1.2.1.3 Central Incoming Payments

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



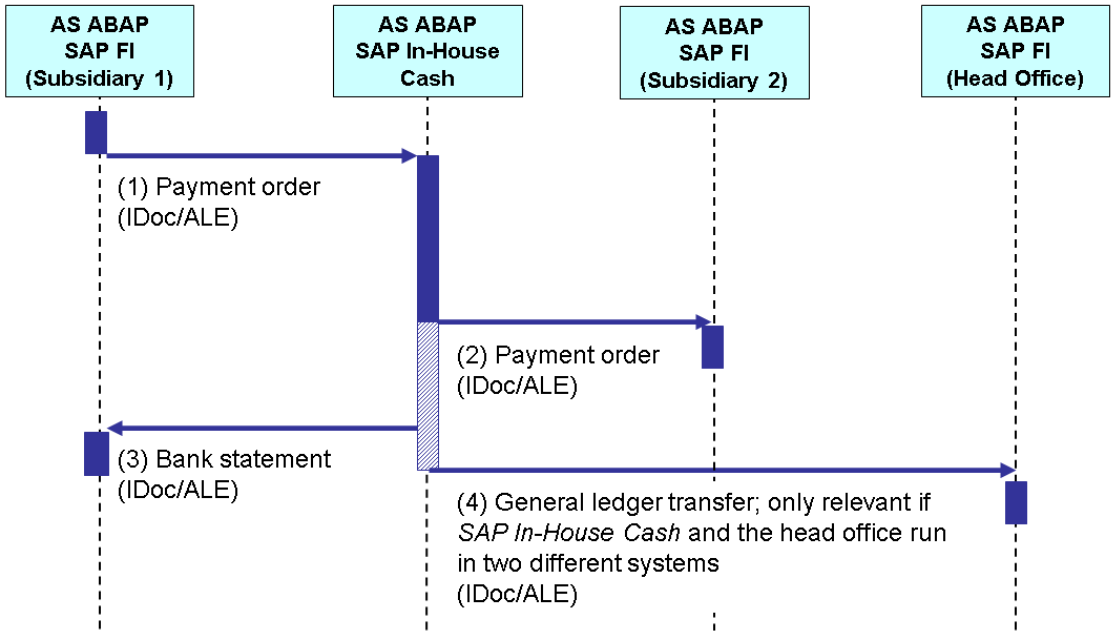
The table below shows the security aspect to be considered for the process step and what mechanism applies.

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 *SAP In-House Cash* and the head office are running in two different systems (IDoc/ALE)	User type: dialog user or technical user

14.3.1.2.1.4 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 391] .



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

Step	Description	Security Measure
3	Bank statement(IDoc/ALE)	User type: dialog user or technical user
4	General ledger transfer; only relevant if *SAPIn-House Cash* and the head office are running in two different sys-tems(IDoc/ALE)	User type: dialog user or technical user

14.3.1.2.2 Authorizations

Standard Roles

The table below shows the standard roles that are used by the SAP *In-House Cash* component. They contain the maximum values of the authorizations.

Roles	Description	Comments
SAP_CFM_IHC_SUPERVISOR	In-House Cash Supervisor	Relevant for CFM 2.0
SAP_FSCM_IHC_SUPERVISOR	FSCM In-House Cash Supervisor	EA-Finserv 200 onwards

Authorization Objects

The table below shows the security-relevant authorization objects that are used by the SAP *In-House Cash* component.

Authorization Objects	Description
IHC_ACTION	Authorizations for IHC activities
IHC_ROUTE	Authorizations in route definition
IHC_CMSTAT	Cash Management status of In-House Cash
F_PAYRQ	Authorization object for payment requests

See also the Customizing activities in the SAP Customizing Implementation Guide (IMG). To do this, choose *SAP Reference IMG* > *Financial Supply Chain Management* > *In-House Cash* > *Authorization Management.* >.

14.3.1.3 SAP Cash 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.

Authorizations

Access is protected by the authorization objects described in Authorizations [page 395].

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 411].

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 412].

14.3.1.3.1 Authorizations

SAP Cash Management uses the authorization concept delivered by SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS ABA security guide also apply to SAP Cash Management.

The SAP NetWeaver 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 Roles

The following table shows the standard role that is used in SAP Cash Management.

Role	Description
SAP_BR_CASH_MANAGER	Business catalog role for cash managers
SAP_BR_CASH_SPECIALIST	Business catalog role for cash specialists
SAP_FIN_ANALIQUIDITYPLAN_APP	Back-end role for liquidity plans
SAP_FIN_DEVLIQUIDITYPLAN_APP	Back-end role for develop liquidity plans
SAP_FIN_LF90DAYS_SMB_APP	Back-end role for liquidity forecast
SAP_FIN_ACF90DAYS_SMB_APP	Back-end role for actual cash flow

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used in SAP Cash Management.

Authorization Object	Authorization Field	Permitted Activities	Description
B_BUPA_RLT Business Partner: BP Roles	ACTVT	• 01 Create or generate • 02 Change • 03 Display	With this authorization object, you define which BP roles can be edited.
	RLTYP BP Role Type		
B_BUPR_BZT Business Partner Relationships: Relationship Categories	ACTVT	• 01 Create or generate • 02 Change • 03 Display • 06 Delete	With this authorization object, you define which BP with specific authorization groups can be displayed.
	RLTYP BP Role Type		
B_BUPR_GRP Business Partner: Authorization Groups	ACTVT	• 03 Display	With this authorization object, you establish which relationship categories can be processed.
	BERGU		

Authorization Object	Authorization Field	Permitted Activities	Description
CA_POWL Authorizations for the Personal Object Worklist (POWL) iViews.	POWL_APPID	POWL-FCLM-BAM-INBOX-WI	Application ID of POWL iView (as specified in Application Parameters in the iView properties)
	POWL_CAT	03	The user is not allowed to re-assign queries or change the query order.
	POWL_LSEL		It determines if the user is allowed to select the layout style (either one entry in a hyper-link matrix or one tab-strip per query) for the POWL iView
	POWL_QUERY	• 01 • 02 • 03	• 01 The user is allowed to create/change/delete own queries for all POWL object types assigned to him (c.f. customizing tables POWL_TYPE_USR and POWL_TYPE_ROL). • 02 the user is only allowed to create own queries on the basis of admin queries assigned to him via customizing tables POWL_TYPE_USR and POWL_TYPE_ROLrespectively. (Note: this is also subjected to the user - POWL object type assignments) • 03 (and other values): the user is only allowed to change admin queries assigned to him with respect to the select options restrictions of those admin queries (thus creating one own "derivation" per admin query transparently)

Authorization Object	Authorization Field	Permitted Activities	Description
	POWL_RA_AL		It determines if the user gains access to a "Refresh all" button, which triggers a parallelized refresh for all queries which are active on the POWL iView identified by POWL_APPLID. Note this may cause high system load on the application server group used for refreshes on this POWL iView.
	POWL_TABLE		It determines if the user is allowed to personalize the query result table settings (define column order, hide columns, etc.).
F_BNKA_MAN Banks: General Maintenance Authorization	ACTVT	• 01 Create or generate • 02 Change • 03 Display	This object controls the authorizations for maintaining bank master data.
F_CLM_BAM Authorization for Bank Account Management	ACTVT	• 01 Create or generate: Create new bank account master records • 02 Change: Change bank account master records • 03 Display: Display bank account master records • 06 Delete: Delete inactive bank account master records • 31 Confirm: Review bank account master records • 69 Discard: Close bank accounts	This authorization object is used for controlling the authorizations of Bank Account Master Data maintenance. This authorization object is assigned to the standard role Cash Manager by default.
	FCLM_ACTY Bank Account Type ID		
	FCLM_BUKRS Company Code		

Authorization Object	Authorization Field	Permitted Activities	Description
	FCLM_GSBER Business Area		
	FCLM_KOKRS Controlling Area		
	FCLM_PRCTR Profit Center		
	FCLM_SGMT Segment for Segmental Reporting		
F_CLM_BAH2 Bank Account Hierarchy	ACTVT	• 01 Create or generate • 02 Change • 03 Display • 06 Delete	This authorization object is used for controlling the authorizations of bank hierarchy and bank account group maintenance.
	HIERTYPE Hierarchy Type		
	PUBLICHIER Public Flag for Hierarchy		
F_CLM_UP Authorization for Import and Export Bank Accounts	ACTVT	01 Create or generate: Create or update bank account master data	This authorization object controls the authorization of using the *Import and Export Bank Accounts* tool to create or update bank account master data by importing bank accounts from an XML file.
F_BNKA_MAO Banks: General Maintenance Authorization by Country	ACTVT	• 01 Create or generate • 02 Change • 03 Display	This authorization object controls the authorizations for maintaining bank master data. The authorizations can be assigned according to the country.
	BBANKS Bank country		

Authorization Object	Authorization Field	Permitted Activities	Description
F_STAT_MON Bank Relationship: Status Monitor authorizations	BNK_ACT	READ Read and display batch or batch item.	This authorization object controls in the transactions to monitor and approve payment batches, which batches the user is allowed to display or to process.
	BNK_RULE Rule ID		
	BNK_ITMDET Action on item level allowed (display, reject, resubmit)	*	Display and process on item level (marked) or only on batch level (not marked) Notice that field BNK_ITMDET determines whether or not the user is authorized to display, reject, or return single payments contained in a batch.
F_BNKA_BUK Banks: Authorization for Company Codes	ACTVT	• 02 Maintain (create or change) • 03 Display	This object controls the authorizations for maintaining house banks and bank accounts in a company code.
	BUKRS Company code		
F_REGU_BUK Automatic Payment: Activity Authorization for Company Codes	BUKRSCompany Code		Using this authorization object, you determine which activities are allowed for the payment program. The object consists of the Company Code and Activity fields. You can call up the possible keys for the Activity field with the Environment menu option in the request screen of the payment program.
	FBTCH Action for Automatic Procedures in Financial Accounting	23 Maintain	
F_FEBB_BUK Company Code Bank Statement	ACTVT	• 03 Display	This authorization object controls the authorizations for maintaining bank statements in a company code. A user who would like to display Bank Statement reports
	BUKRS Company code		

Authorization Object	Authorization Field	Permitted Activities	Description
			using SAP Cash Management should have Bank Statement display authorization. This authorization object is assigned to the standard role Cash Manager by default.
F_FDES_BUK Cash Management and Forecast: Company Code Memo Records	ACTVT	• 01 Create or generate • 02 Change • 03 Display	With this authorization object, you can check the authorizations to maintain Cash Management and Forecast payment advice and planned items in a company code.
	BUKRSCompany Code	$GSBER	
F_FDES_GSB Cash Management and Forecast: Business Area Memo Records	ACTVT	• 01 Create or generate • 02 Change • 03 Display	With this authorization object, you can check the authorizations to maintain Cash Management and Forecast payment advice and planned items in a business area (not business area SPACE). At this level you define whether a user may create, change or display individual payment advice or planned items of a business area.
	GSBERBusiness Area	$GSBER	
F_FDSB_BUK Cash Position: Company Code Summary Records	ACTVT	• 01 Create or generate • 02 Change • 03 Display • 16 Execute	With this authorization object, you control the authorizations to maintain summary records for the cash management position (Cash Management) in a company code. At this level you define whether a user may create, change or display summary records of a company code. Display authorization is need to display the cash management position of a company code.
	BUKRSCompany Code	$BUKRS	

Authorization Object	Authorization Field	Permitted Activities	Description
F_FDSB_GSB Cash Position: Business Area Summary Records	ACTVT	03 Display	This object controls the authorizations to maintain the summary records for the cash management position (Cash Management) in a business area (except for business area BLANK).
	GSBERBusiness Area	$GSBER	
F_FDSR_BUK Liquidity Forecast: Company Code Summary Records	ACTVT	• 03 Display • 16 Execute	With this authorization object, you control the authorizations to maintain the liquidity forecast (Cash Forecast) summary records in a company code. At this level you define whether a user may display or execute liquidity forecast summary records of a company code. Display authorization is necessary for displaying the liquidity forecast.
	BUKRSCompany Code	$BUKRS	
F_FDSR_GSB Liquidity Forecast: Business Area Summary Records	ACTVT	• 03 Display	With this authorization object, you control the authorizations to maintain the liquidity forecast (Cash Forecast) summary records in a business area (except for business area BLANK). At this level you define whether a user may display or execute liquidity forecast summary records of a business area. Display authorization is necessary for displaying the liquidity forecast of a business area.
	GSBERBusiness Area	$GSBER	
F_BKPF_BUK Accounting Document: Authorization for Company Codes	ACTVT	• 03 Display	With this authorization object, you determine in which company codes documents can be processed. An employee can only call up the functions for posting if he/she has this authoriza-

Authorization Object	Authorization Field	Permitted Activities	Description
	BUKRSCompany Code	$BUKRS	tion in at least one company code. The object consists of the Company code and Activity fields. You take the possible input values for the Activity field from table TACTZ.
F_KNA1_GEN Customer: Central Data	ACTVT	03 Display	This authorization object controls which activities are permitted for the general data. The general data consists of the fields that are independent of the company code and the sales organization.
F_LFA1_GEN Vendor: Central Data	ACTVT	03 Display	This authorization object controls which activities are permitted for the general data. The general data consists of the fields that are independent of the company code and the sales organization.
F_PAYRQ Authorization Object for Payment Requests	ACTVT	• 01 Create or generate • 02 Change • 03 Display • 43 Release The Release (43) activity is also checked after corresponding activation according to SAP Note 2150759. • 85 Reverse	This authorization is used when payment requests are created, displayed, and reversed.
	BUKRS Company Code	$BUKRS	
	ORIGIN Origin Indicator	TR-CM-BT	
F_REGU_KOA	KOARTAccount type	$KOART	Using this authorization object, you determine which

Authorization Object	Authorization Field	Permitted Activities	Description
Automatic Payment: Activity Authorization for Account Types	FBTCHAction for Automatic Procedures in Financial Accounting		activities are allowed for the payment program for which account types (D for customer, K for vendor, and S for G/L accounts). The object consists of the Account type and Activity fields. You can call up the possible keys for the Activity field with the Environment menu option in the request screen of the payment program.
FQM_FLOW Financial Quantity Management	ACTVT	• 01 Create or generate • 03 Display • 06 Delete • 25 Reload	With this authorization object, you can control the access to the data stored in the One Exposure from Operations hub.
	BUKRS Company Code		
	FQM_ORIGAP Source Application		
S_RS_COMP Business Explorer - Components	ACTVT	• 16 Execute	With this authorization object, you can restrict the components that you work with in the Business Explorer query definition.
	RSINFOAREA	2O-FI	InfoArea: Determines which InfoAreas a given user is allowed to process.
	RSINFOCUBE	2CILFOBALWLIBAL	InfoCube: Determines which InfoCubes a given user is allowed to process.
	RSZCOMPTP	REP	Component type: Determines which components a given user is allowed to process.
	RSZCOMPID	2CCLFCASTANLYTS	Name (ID) of a reporting component: Determines which components (according to name) a given user is allowed process.

Authorization Object	Authorization Field	Permitted Activities	Description
S_RS_COMP1 Business Explorer - Components: Enhancements to the Owner	ACTVT	• 16 Execute	With this authorization object, you can restrict query component authorization with regards to the owner. This authorization object is checked in conjunction with the authorization object S_RS_COMP.
	RSZCOMPID	2CCLFCASTANLYTS	Name (ID) of a reporting component: Determines which components (according to name) a given user is allowed process.
	RSZCOMPTP	REP	Type of reporting component: determines which component types are allowed to be edited by the user.
	RSZOWNER	*	Reporting component owner: determines whose components are allowed to be edited by the user.
S_SERVICE Check at Start of External Services	ACTVT	• 16 Execute	This authorization object is automatically checked when external services are started (not yet for all service types). The Profile Generator automatically assigns authorizations if an external service is entered in a role menu.
	SRV_NAME Hash value of the external service	• 84A2886C6DA699EF0F0F4083ADC455 • C_LFCASTANALYTICS_CDS 0001 • AB088B10113EAC3BC6349F4E933053 • /SSB/SMART_BUSINESS_RUNTIME_SRV 0001	
	SRV_TYPE	TADIR OBJECT	Type of the external service

Authorization Object	Authorization Field	Permitted Activities	Description
S_RS_AUTH BI Analysis Authorizations in Role	BIAUTH	0F_AUTH_RP1	This authorization object is used to make analysis authorizations available in the SAP NetWeaver standard roles. The values in field BIAUTH are authorization names from the analysis authorizations. They can be selected using input help (F4).
S_RS_ZEN Design Studio: Authority Object	ACTVT	• 03 Display • 16 Execute	With this authorization object, you can restrict working with Design Studio objects, such as analysis applications or SDK extensions.
	RSAO_OBJID Technical name of the object	• 0ANALYSIS • 0FCLM_ALP_ACUR • 0FCLM_ALP_BY_ALERT_OVERVIEW • 0FCLM_ALP_BY_LQITEM_ACUR • 0FCLM_ALP_BY_LQITEM_PCUR • 0FCLM_ALP_PCUR	With this authorization field, you can restrict the access to a specific analysis application.
	RSAO_OBJTY Object Type	10	For analysis applications, you need to enter 10 as the correct object value.
	RSZOWNER Owner of the object	*	With this authorization field, you can restrict the access to Design Studio objects created by a specific owner.
RSBPC_BBPF Manage and use BPF	ACTVT	• 03 Display • 16 Execute • 23 Maintain • 16 Execute	With this authorization object, you can define the authorizations of business process flow.
	RSBPC_APPS Environment ID	0FCLM_LP_ENV	

Authorization Object	Authorization Field	Permitted Activities	Description
	RSBPC_TMPL BPF Template ID	FCLM_LP_PROCESS	
RSBPC_ENVM Manage environment	ACTVT	• 03 Display • 23 Maintain	Authorization object that is checked when an environment is viewed or maintained.
	RSBPC_APPS Environment ID	0FCLM_LP_ENV	
RSBPC_ID Grant user access to a BPC environment	RSBPC_APPS Environment ID	0FCLM_LP_ENV	Authorization object that is checked when it is necessary to find out whether a user is assigned to an environment.
RSBPC_MODL Manage model	ACTVT	• 03 Display • 23 Maintain • A3 Change status	Authorization object that is checked when a model is viewed or maintained.
	RSBPC_APPS Environment ID	0FCLM_LP_ENV	
	RSBPC_APPL Model ID	FCLM_LP_PROCESS	
RSBPC_TEAM Manage team	ACTVT	• 03 Display • 23 Maintain	Authorization object that is checked when a team is viewed or maintained.
	RSBPC_APPS Environment ID	0FCLM_LP_ENV	
	RSBPC_TEAM Team ID	*	
RSBPC_USER Manage and use User	ACTVT	• 03 Display • 23 Maintain	Authorization object that is checked when a user is viewed or maintained.
	RSBPC_APPS Environment ID	0FCLM_LP_ENV	
	RSBPC_USER User ID	*	

Authorization Object	Authorization Field	Permitted Activities	Description
RSBPC_WKSP Manage resource	ACTVT	• 03 Display • 23 Maintain	With this authorization object, you can define the authorizations of resources, including reports, input forms, work spaces and so on.
	RSBPC_APPS BPC: Environment ID	0FCLM_LP_ENV	
	RSBPC_FLDR BPC: Folder authorization	*	Possible values: • PUBLIC: Live report • NON_PUBLIC: Input form

Authorization Object	Authorization Field	Permitted Activities	Description
	RSBPC_RSTY BPC: Resource Type	*	Possible values: • LIVE_REPORT: Live report • INPUT_FORM: Input form • SUB_FOLDER: Subfolder • EXCEL_INPUT_FORM: Input form in Microsoft Excel • EXCEL_REPORT: Report in Microsoft Excel • ACTIVITY_WORKSPACE: Workspace • LINK: Link • DASHBOARD: Dashboard • WORKBOOK: Workbook • BOOKS: Published books • DOCUMENT: Assign the user the authorization to upload files • DISTRIBUTION: "Distribution" folder under team folder • EEXCEL: "EExcel" folder under public folder for EPM add-in • PUBLICATION: "Publication" folder under team folder • XLTX: Book template
S_BTCH_JOB Background Processing: Operations on Background Jobs	JOBGROUP Summary of jobs for a group	$JOBGROUP	The authorization object consists of the authorization fields JOBACTION and JOBGROUP. JOBGROUP must always have the value *. Each of these permits the user to perform different operations on jobs. A user WITHOUT ANY specific au-

Authorization Object	Authorization Field	Permitted Activities	Description
	JOBACTION Job Operations	• DELE Delete other users' background jobs. • LIST Not used • MODI Modify other users' jobs. • PLAN Copy or repeat other users' jobs • PROT (No check) • RELE Release jobs (including your own) • SHOW Display definitions of other users' jobs	thorization for jobs may perform the following actions: • Schedule jobs for which the job class is C and cannot be changed. • View and change steps of his or her own jobs. • Delete his or her own jobs. • View the job details of his or her own jobs. If a user has an authorization for the object S_BTCH_ADM, he or she has full authorization for all jobs of all users.
S_PROGNAM Generic Program Start	P_ACTION User Action in ABAP Program	BTCSUBMIT	The object is used to supplement the start authorization check for programs. Authorizations for this object are checked exclusively with method CL_SABE=>AUTH_CHECK_PROGNAM() in the context of scenarios for switchable authorizations (maintenance transaction SACF). The check does not take place with each submit command, but only if is explicitly called. If the associated scenario is activated, all programs are checked in addition to the existing authorization checks (for example, with authorization groups). You can assign authorizations for the following activities: • Starting a program

Authorization Object	Authorization Field	Permitted Activities	Description
	P_PROGNAM Program Name with Search Help	• /ATL/F110_SCHEDULE_AFTER_RUN • RBNK_PAYM_GRP_N_BATCH • SAPF111S SAPFPAYM_MERGE • SAPFPAYM_SCHEDULE	• Scheduling a program to run as a background job. • Delete his or her own jobs. • Defining variants

14.3.1.3.2 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For SAP Cash Management powered by SAP HANA, 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 SAP NetWeaver Security Guide.

14.3.1.1.3.3 Data Storage Security

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

SAP Cash 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 SAP Cash 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 SAP Cash 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.

14.3.1.3.4 Data Protection

14.3.1.3.4.1 Deletion of Personal Data

Use

One Exposure from Operations in SAP S/4HANA Finance for cash 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.

SAP S/4HANA Finance for cash management delivers a where-used check (WUC) for *One Exposure from Operations*.

For information about the Customizing of blocking and deletion for *One Exposure from Operations*, see *Configuration: Simplified Blocking and Deletion*.

Relevant Application Objects and Available Deletion Functionality

One Exposure itself does not directly use SAP ILM. But the integrated source applications, which have to comply with retention periods, use SAP ILM to support the deletion of personal data.

One Exposure, however, provides the program *Aggregate Flows*, which helps to reduce the data volume in database table `FQM_FLOW`.

Application	Detailed Description	Provided Deletion Functionality
One Exposure from Operations	You use this transaction to delete flows with certainty level `ACTUAL` in One Exposure and substitute them with aggregation flows. They then no longer contain any person-related information. For more information, see the corresponding program documentation.	`FQM_AGGREGATE_FLOWS`

Where-Used Check (WUC)

A where-used check is a simple check to ensure data integrity in case of potential blocking. The WUC in *SAP S/4HANA Finance for cash management* checks whether any dependent data for a certain business partner, customer, or vendor exists in the related table for *One Exposure from Operations*:

- Affected table in *One Exposure from Operations*:
  - `FQM_FLOW`

If dependent data exists, that is, if the data is still required for business activities, the system does not block a certain BP. 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.

Relevant Application Objects and Available EoP/WUC functionality

For the following application object, a where-used check (WUC) supporting the blocking of business partner master data is available:

Application	Implemented Solution (EoP or WUC)	Further Information
One Exposure from Operations	WUC with function module `FQM_BUPA_WUC_CHECK`	

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*.
  - Under *Register Application Names for EoP Check* (view `V_BUTEOPAPP`) you find *One Exposure from Operations*(`FQM`).
  - Under *Define Application Function Modules Registered for EoP Check* (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`

For more information about configuration, see the Customizing documentation.

14.3.1.3.5 Country Specifics

14.3.1.3.5.1 China

14.3.1.3.5.1.1 Cash Budgeting

14.3.1.3.5.1.1.1 Authorizations

Cash Budgeting uses the authorization concept provided by the SAP Net Weaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to *Cash Budgeting*.

The SAP NetWeaver 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 *Role Administration*.

Standard Roles

The following table shows the standard roles that are used by *Cash Budgeting*:

Role	Description
FUCN_TREASURY_MANAGER	Treasury Manager
FUCN_PLANNER	Planner
FUCN_BUSINESS_MANAGER	Business Manager

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by *Cash Budgeting*.

Authorization Object	Description
F_CYC_DSVC	You use this authorization object to determine who has authorization to start/void/ complete a cycle.
F_CYC_CRUD	You use this authorization object to determine who has authorization to create/edit/view/ save a cycle.
F_ORG_LOAD	You use this authorization object to determine who has authorization to view/upload an organizational hierarchy.
F_PRO_RULE	You use this authorization object to determine who has authorization to view/edit an approval process rule
F_APR_DATA	You use this authorization object to determine who has authorization to approve budget data.
F_LIQ_LAYO	You use this authorization object to determine who has authorization to create/view/edit a planning layout.

14.3.1.3.5.1.1.2 Internet Communication Framework Service

You should only activate the services needed for the applications running in your system. In the SAP Business Client, the following services, which you can find under the path `default_host/sap/bc/webdynpro/sap`, are needed.

For application from WD ABAP Page Builder (`BC-WD-ABA-PB`):

- `WDR_CHIP_PAGE`

Cash Budgeting ICF Configuration

The `SICF` services should be activated in `sap/bc/webdynpro/sap`

- `CMCB_APPROVAL_PROCESS`
- `CMCB_CONSM_ASSIGNMENT`
- `CMCB_CONSM_STATUS`
- `CMCB_CYCLE_APPROVE`
- `CMCB_CYCLE_FORM`
- `CMCB_CYCLE_SEARCH`
- `CMCB_ORG_HIERARCHY`
- `CMCB_PLANNING`
- `CMCB_PLANNING_LAYOUT`
- `CMCB_PLANNING_LAYOUT_OWL`
- `CMCB_UPLOAD_FORM`

- CMCB_WORKING_CONTEXT
- CMCB_WORKLIST
- CMCB_CONSM_ASSIGN_ALV_APP
- CMCB_CONSM_STATUS_ALV_APP
- CMCB_CYC_PLANNING_REPORT
- CMCB_REPORTS
- CMCB_CNSUM_ACT_PAY
- CMCB_CYC_ORG_SEARCH
- CMCB_CYC_PLANNING_REPORT
- CMCB_DOC_SEARCH
- CMCB_MANUAL_TRANSFER
- CMCB_ORGQUERY_SEARCH
- CMCB_PMT_CTRL_RULE
- CMCB_SUPPLEMENTARTY_BUDGET
- WDA_FCLM_LQH

Features

Use the transaction SICF to activate these services.

If your firewalls use URL filtering, take note of 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*.

14.3.1.4 SAP Treasury and Risk Management

- **Network and Communication Security**
  Communication with external systems is possible using standard interfaces via BAPI, IDoc, XI and BAdIs.
- **Communication Destinations**
  In certain cases a technical user may be required for applying BAPIs.
- **Data Storage Security**
  - *SAP Treasury and Risk Management* accesses financial transaction data that can be particularly sensitive. Access is protected by the authorization objects described in the Authorizations [page 418]section.
  - Using Logical Path and Filenames to Protect Access to the File System [page 437]
- **Additional Security-Relevant Information**

All authorizations are managed by means of roles and profiles.
In addition you can further increase the system security by making a number of Customizing settings such as trader authorizations, posting release settings and a lot of other release workflows for objects like hedging relationships, correspondence objects or exposure positions. However, the authorization check itself must always be run on the basis of roles and profiles.

14.3.1.4.1 Authorizations

Standard Roles

The table below shows the standard roles that are used by the *SAP Treasury and Risk Management*.

Role	Description
SAP_BR_TREASURY_RISK_MANAGER	Treasury Risk Manager
SAP_TRM_ADMINISTRATOR	Treasury Administrator
SAP_TRM_DEALER	Trader
SAP_TRM_LIMIT_MANAGER	Limit Manager
SAP_TRM_RISK_CONTROLLER	Risk Controller
SAP_TRM_TM_BACKOFFICE_PROCES	Back Office Processor
SAP_TRM_TM_FUND_MANAGER	Fund Manager
SAP_TRM_TM_STAFF_ACCOUNTANT	Staff Accountant
SAP_TRM_TM_TRADE_CONTROLLER	Trade Controller
SAP_TRM_TREASURY_MANAGER	Treasury Manager

Transaction Roles

Role	Description
SAP_AUDITOR_BA_CFM (AIS – Audit Information System)	Allows evaluations in *Treasury* to be collected, structured and preset. The required menu forms part of this role. The relevant authorization role is SAP_AUDITOR_BA_CFM_A (AIS – Authorizations for SAP Applications (Excluding HR)).

Role	Description
SAP_AUDITOR_TAX_TR (AIS – Audit Information System Transaction Role)	Provides the collection, structuring, and presetting of evaluations in *Treasury* for tax auditing purposes. The required menu forms part of this role. The relevant authorization roles are SAP_AUDITOR_TAX_TR_A (AIS – Tax Auditor TR (Authorizations)) and SAP_AUDITOR_TAX_A (AIS – Tax Auditor Central Functions (Authorizations)).

Authorization Roles

Role	Description
SAP_AUDITOR_BA_CFM_A (AIS – Audit Information System)	Allows read-only access for the business audit in Treasury The relevant transaction role is SAP_AUDITOR_BA_CFM (AIS – Transactions for SAP Applications (Excluding HR)).
SAP_AUDITOR_TAX_TR_A (AIS – Audit Information System)	Grants read-only access to tax auditors. The relevant transaction role is SAP_AUDITOR_TAX_TR (AIS – Tax Audit Treasury)

An extended authorization check is performed with the roles SAP_AUDITOR_TAX_TR and SAP_AUDITOR_TAX_TR_A.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by the *SAP Treasury and Risk Management* (class TRTM *Treasury Management*).

Standard Authorization Objects

Authorization Object	Permitted Activities	Description
CMM_ESTIME	01 Create or Generate 02 Change 03 Display 06 Delete	This authorization object enables you to restrict who can create, edit, delete, or display exception end-of-day snapshot definitions.

Authorization Object	Permitted Activities	Description
CMM_STIME	01 Create or Generate 02 Change 03 Display 06 Delete	This authorization object enables you to restrict who can create, edit, delete, or display end-of-day snapshot definitions.
T_ASGTTMPL Acct Assignment Templates	02 Change	
IDCFM_FRAM Amortized Costs	01 Display 03 Update	Authorization object for amortized cost function.
T_RMOB_AUG Application Objects for CFM/Banking Analysis	01 Create or generate 02 Change 03 Display 06 Delete 21 Transport	This authorization object controls authorization for editing and using different settings within CFM/Banking Analysis (e.g. evaluation type, scenario, portfolio hierarchy).
T_POS_ASS Assign Attributes to Positions	01 Create or generate 02 Change 03 Display	This object checks if the user is allowed to create, change (delete), or display position attributes. These attributes are the position's account assignment reference and the position management procedure. You can control the authorization for each Accounting code, valuation area, and product type. The check for assignment of the position management procedure is carried out when a position is created either manually or automatically. The check for assignment of the account assignment reference is carried out with the first posting to the position or when the account assignment reference is manually assigned to the position.

Authorization Object	Permitted Activities	Description
T_TLR_REP Authorization for Legal Report Type	02 Change 03 Display 70 Administer	With this authorization object, you define user-specific authorizations for activities concerning trade repository objects. Use in function: • Trade Repository Monitor (transaction FTR_TARO_MONITOR) • Update Trade Repository Objects (transaction FTR_TARO_PROCESS) • Send Trade Repository Objects (transaction FTR_TARO_SEND) • Import Incoming Messages (transaction FTR_TARO_IMPORT) • Report R_TLR_TARO_STATUS_REMARK *Update the Status or the Text in the Field Remark of TAROs*
T_DEAL_PD Authorization for Product/Transaction Types	01 Create or generate 02 Change 03 Display 06 Delete 16 Execute 38 Perform 43 Release 48 Simulate 83 Counterconfirm 85 Reverse AB Settle KI Knock In KO Knock Out KU Give notice PR Process Correspondence PS VF Expired	With this authorization object, you determine for a user which functions and activities he is allowed to execute for a product and transaction type within a company code. Use in functions: All transaction of the Transaction Management (Trade, Back Office) of the *Transaction Manager* (FSCM-TRM-TM) which create or maintain financial transactions including the BAPIs.

Authorization Object	Permitted Activities	Description
T_IGT_DEAL Authorization for Product/Transaction Types for IGT	01 Create or generate 02 Change 03 Display 06 Delete 10 Post	With this authorization object, you determine which functions and activities are allowed for a product and transaction type in a company code for Intragroup transactions [within *Edit Intragroup Transactions* (transaction TRIG_IGT)].
T_DEAL_DP Authorization for Securities Account	01 Create or generate 02 Change 03 Display 06 Delete 16 Execute 43 Release 48 Simulate 85Reverse PR Process Correspondence PS	With this authorization object, you determine which functions and activities are allowed for a securities account in a company code. Use in functions: • TRS_SEC_ACC – Edit Securities Account • FWDP – Securities Account List • TS09 – Define Default Values
T_DEAL_AG Authorization for an Authorization Group	01 Create or generate 02 Change 03 Display 06 Delete 16 Execute 43 Release 48 Simulate 85 Reverse PR Process Correspondence PS	With this authorization object, customer specific authorization checks can be carried out if necessary in addition to the objects • T_DEAL_DP • T_DEAL_PF • T_DEAL_PD Application examples: • A trader should only be allowed to display/process department-related orders. • A clerk should not be allowed to display/process an employee loan.
T_EXT_SEC Authorization for external security account	01 Create or generate 02 Change 03 Display 06 Delete	Authorization object for maintaining external securities account statements

Authorization Object	Permitted Activities	Description
T_RIGHTS Authorization to Exercise Options	03 Display 38 Perform 48 Simulate 85 Reverse	The authorization object T_RIGHTS is required for exercising security rights in the securities area of the Transaction Manager. The system checks the object T_RIGHTS in the application function for exercising security rights (path: *Transaction Manager* > *Securities* > *Trading* > *Security Right* > *Exercise / Reverse* >).
T_BP_USED Business Partner: Authorization for Where-Used List		Prior to calling up the where-used list of the business partner from dialog maintenance, or with incoming telephone calls, a check is made as to whether the user has the authorization to display the use of a business partner in a particular application. If this is not the case, the user is not offered the corresponding application to see how the business partner is used. The partner number and assignment category fields are requested. The assignment category defines the application being used by the business partner (for example, Real Estate, Money Market, Loans). The assignment categories can be displayed with the V_TPR1 view.
T_BP_USEDT Business Partner: Where-Used List Authorization (Decoupling)		
T_FTI_LDB CFM Position Management Reporting Using Logical Databases		You use this authorization object to assign authorizations for CFM position management reporting using logical databases.

Authorization Object	Permitted Activities	Description
T_CML_ARCH CML: Authorization in Loans Archiving Area	03 Display 24 Archive 25 Reload 33 Read 56 Display archive 57 Save archive	When you select a transaction, the system checks whether the function may be executed and in which company codes the system is permitted to process documents.
T_RMCHAR_V Characteristic Values in Risk Management Reports		You can use this authorization object to define for which financial objects a user can run particular evaluations. The authorization is based on characteristic values. Defined fields • Report Category The report category describes the business purpose of the analysis (for example, NPV analysis, gap analysis). The possible values can be taken from the fixed values for domain RMRPTYPE. • Characteristic • Value Note: The checking of the characteristics is based on an AND link. This means that if an entry for the field Characteristic is not equal to *, then an additional entry with the value * has to be defined for each characteristic for which all values are permitted. No hierarchy can be defined with this authorization object. For example, this means that is not possible to give a user authorization for all product types in company code 001, but then to restrict the authorization to certain product types in company code 002. Any restriction of the authorization to certain product types would apply automatically to company code 001.

Authorization Object	Permitted Activities	Description
T_KAPM_1 Corporate Actions I	01 Create or generate 02 Change 03 Display 63 Activate	You use this object to define the user authorizations for: • Corporate action types • Activities Use in functions The object T_KAPM_1 is checked in the following application functions: *Securities* > *Back Office* > *Corporate Actions* for *Corporate action category*: Manually generated
T_KAPM_2 Corporate Actions II	10 Post 48 Simulate 85 Reverse	With this authorization object, you define at the company code level, for which corporate actions postings or simulation runs may be carried out. Use in functions Object T_KAPM_2 is checked in the following application function: Securities – Processing: Post other corporate actions
T_THXE_ET Effectiveness Tests	01 Create or generate 02 Change 03 Display 06 Delete 94 Override	You can use this authorization object to manage the access in the effectiveness test part of the *Hedge Accounting for Positions*. Use in functions: The system checks whether the user is authorized to execute the function based on *Company Code*, *Valuation Area*, *Hedging Relationship Category*, *Hedging Relationship Profile* and *Activity*within the following functions: • *Manage Hedging Relationships* (transaction TPM100) • *Run Effectiveness Test* (transaction TPM110

Authorization Object	Permitted Activities	Description
T_TREA_EVA Execute or Display Evaluation Data on External Accounts	01 Create or generate 03 Display	With this authorization object, you determine which activities for evaluations on external accounts can be performed by which users. Use in functions: • NPV Calculation for External Account Transactions (transaction: TREA_EVAL) • Show Results of Key Figure calculation for External Accounts (transaction: TREA_EVAL_SHOW)
T_RIGHTS_D Exercise Rights for Listed Options or Futures	03 Display 38 Perform 48 Simulate 85 Reverse	
T_TEX_POS Exposure Position	02 Change (Change attributes of the exposure position) 03 Display (Display exposure position) 59 Distribute (Update exposure position in the Hedge Accounting for Exposures) 61 Export (Export exposure position to market place or other function covered by BAdI)	The authorization object controls which activities are allowed for exposure positions within *Exposure Management 2.0*.
T_TREA_CA External Account	01 Create 02 Change 03 Display 06 Delete NP Net Payment	With this authorization object, you determine for users which activities they are allowed to execute for an external account. Used in functions: • Maintain External Accounts (transaction TREA_ACC_MNT) • Create Net Payment (transaction TREA_PAY)

Authorization Object	Permitted Activities	Description
T_TREA_STA External Account Statement	Create or generate Change Display Delete Release	With this authorization object, you determine for users which activities for an external account statement they are allowed to execute. Used in functions: • Maintain External Account Statements (transaction TREA_STA_MNT) • Upload External Account Statements (transaction TREA_STA_UPL) • Release Line Items (transaction TREA_RELEASE)
T_BP_DEAL FS Business Partner: Standing Instructions	01 Create or generate 02 Change 03 Display	The system checks against the authorization object *Treasury Business Partner: Standing Instructions* when the user calls up the standing instructions function. The system only displays the standing instructions for which the user is authorized. Examples: • If a user is not authorized to use the standing instructions function, this user is unable to branch to the standing instructions from the business partner master data screen. • If a user is only authorized to maintain transaction authorizations, the system only displays the corresponding tab for transaction authorizations when this user calls up the standing instructions.

Authorization Object	Permitted Activities	Description
T_FGDT_ART Generic Transaction: Authorization Types	01 Create or generate 02 Change 03 Display	You can use this authorization object to define authorizations for the input fields of the generic transaction. Based on the field values, you define which generic transactions the user is allowed to maintain. To do this, you have to define an authorization type and the names of the fields to be checked in the Customizing settings for generic transactions. Note: This authorization is optional. You do not need to assign authorizations if you do not want to give special protection to a particular field group, and have not therefore stored field groups for authorization in your Customizing settings. Procedure If you want to use this authorization object, proceed as follows: • Decide for which fields in the generic transaction you want to assign authorizations. • In the Customizing for the generic transaction, create an authorization type for these fields. • Define the authorizations you want to assign to selected employees. Use the authorization type you have created and define the corresponding values for the activity and the selected fields of the generic transaction. • Assign the authorizations you have created to the selected employees by using the relevant profile.
T_HM_BUK Hedge Accounting (E-HA) in Company Code	01 Create or generate 02 Change 03 Display 06 Delete	Authorization object for the functions of hedge accounting (E-HA) in the company code.

Authorization Object	Permitted Activities	Description
IDCFM_FRIM Impairment Authorization Object	01 Display 02 Create 03 Update	Authorization object for impairment function.
F_T_VTBLV Limit	02 Change 03 Display 05 Lock 43 Release 98 Mark for release	With this authorization object, you define which limits can be edited. The object consists of the fields Limit type and Activity.
F_T_VTBLR Limit Reservations	01 Create or generate 02 Change 03 Display	This authorization object determines which activities a user can perform for a limit reservation.
F_T_VTBLL Limit Transfers	01 Create or generate 02 Change 03 Display	
T_STAM_GAT Master Data: Class Category	01 Create or generate 02 Change 03 Display 06 Delete 43 Release 56 Display archive 57 Save archive	This authorization object enables you to control the various activities that can be executed with a security class. You can also control the activities according to the product type. You can set up your system, for example, so that a certain employee can change stocks, but can only display bonds. Use in function: Class Data (transaction FWZZ)

Authorization Object	Permitted Activities	Description
T_DEAL_PF Portfolio Authorization	01 Create or generate 02 Change 03 Display 06 Delete 16 Execute 38 Perform 43 Release 48 Simulate 85 Reverse AB Settle KI Knock In KO Knock Out KS Reverse notice KU Give notice PR Process Correspondence PS VF Expired	With this authorization object, you determine which functions and activities are allowed for a portfolio in a company code.

Authorization Object	Permitted Activities	Description
T_PACC_POS Position in Futures Account	10 Post 85 Reverse	You use this authorization object to determine the company code, product type, and futures account for which activities can be executed that affect the position. You use the authorization object for the following transactions or functions: • Post Variation Margin: Function A, Activity 10 • Post Close Margin: Function A, Activity 10 • Reverse Margin Flows: Function A, Activity 85 • Manual Posting: Function B, Activity 10 • Reverse Manual Posting: Function B, Activity 85 • Execute Matching: Function C, Activity 10 • Reverse Matching: Function C, Activity 85
T_TEX_REXP Raw Exposure	01 Create or generate Create raw exposure 02 Change Change attributes of the raw exposure 03 Display Display raw exposure 06 Delete Delete a raw exposure (Only if it is unreleased) 43 Release Release the raw exposure to exposure positions	The authorization object controls, which activities are allowed for raw exposures within *Exposure Management 2.0*.

Authorization Object	Permitted Activities	Description
T_RDB_CVKF Results Database: Characteristic Value and Key Figure		With the help of this authorization object you can specify for which values of a characteristic a user may display the values of a key figure. The system checks the values of all defining characteristics for a certain review unit (for example, a portfolio hierarchy node). Authorization for the value * is required for characteristics with no restrictions (for example, those that do not appear in a portfolio hierarchy or only appear at a lower level).
T_RDB_RDEL Results Database: Delete Single Records		This authorization enables you to delete single records from the results database by restricting the deletion to a particular application. For example, if you want to delete single records in Market Risk only, but not those in the Portfolio Analyzer, you specify the application RA here.
F_TR_MRM_S Scenario Maintenance	01 Create or generate 02 Change 03 Display 06 Delete	Object F_TR_MRM_S (*Scenario maintenance*) controls the authorizations for maintaining scenarios in Market Risk Management. On this level you define whether a user is authorized to create, change or display a scenario of a certain scenario type.

Authorization Object	Permitted Activities	Description

T_DEPOT
Securities Account Position
	01 Create or generate
	02 Change
	03 Display
	06 Delete
		With this authorization object, you define which position-changing measures may be carried out for the following:
		• company code
		• product category
		• securities account
		Defined fields
		• Company code
		• Product type
		• Function (D4= Disposition block, D5= securities account transfer, D6= securities account cash flow)
		• Securities account
		• Activity (create, change, display, delete, reverse)
		i Note
		• Necessary authorization for *Unblock*: 06 (delete)
		• Necessary authorization for *Manual posting or debit position*:
		  ○ Function: Securities account cash flow (D6)
		  ○ Activity: change (02)
		• Necessary authorization for *Update securities account position*
		  ○ Function: Securities account cash flow (D6)
		  ○ Activity: change (02)
		Use in functions
		Object T_DEPOT is checked in the following functions:
		• Securities account transfer
		• Securities account position overview
		• Manual posting
		• Debit position
		• Reversal of debit position / manual posting

Authorization Object	Permitted Activities	Description
		• Update securities account position • Posting journal
T_SEC_PRIC Security Price Maintenance – Price Type	• 03 Display Display Security Price • 23 Maintain Create/Change/Delete Security Prices	With this authorization object you can control, for which price types a user has the authorization to display or maintain security prices. Defined fields The authorization object has the following fields: • S_KURSART Rate/Price Type – Treasury Instruments • ACTVT Activity (Display, Maintain) Use When you have activated the security price check in the customizing under *Treasury and Risk Management* > *Transaction Manager* > *General Settings* > *Organization* > *Activate Authority Check for Security Price Type* the authorization object T_SEC_PRIC is checked in the following functions: ○ Display security price (transaction FW17) ○ Maintain security price (transaction FW18) ○ Class Master Data (transaction FWZZ)
F_T_FBNAME Treasury: Authorization for Asynchronous Datafeed	01 Create or generate	Treasury: Authorization to call up a function module.
T_TRADER Treasury: Trader Authorization	02 Change 03 Display	Treasury: Authorization for trader

Authorization Object	Permitted Activities	Description
F_T_TRANSB Treasury: Transaction Authorization		When a transaction is chosen, the system checks whether the user is authorized to execute the function. The authorization object is used within nearly all transactions of the *SAP Treasury and Risk Management*.
T_TREA_CA External Account	01 Create 02 Change 03 Display 06 Delete NP Net Payment	With this authorization object, you determine for users which activities they are allowed to execute for an external account. Used in functions: • Maintain External Accounts (transaction TREA_ACC_MNT) • Create Net Payment (transaction TREA_PAY)
T_TREA_STA External Account Statement	Create or generate Change Display Delete Release	With this authorization object, you determine for users which activities for an external account statement they are allowed to execute. Used in functions: • Maintain External Account Statements (transaction TREA_STA_MNT) • Upload External Account Statements (transaction TREA_STA_UPL) • Release Line Items (transaction TREA_RELEASE)
T_DEAL_LC	• LC_ACTVT: 01 Presentation 02 Document • LC_FNCTN: 01 Create 02 Change 03 Display 04 Reverse 05 Accept/Reject 06 Pre-check 07 Send to Bank 08 Settle	With this authorization object, you determine for users which activities they are allowed to execute for a letters of credit.

Authorization Object	Permitted Activities	Description
T_HDG_AREA Hedging Area	• 02 Change • 03 Display	This authorization object enables you to restrict who can display or change hedging areas using function *Define Hedging Area* (transaction TOE_HEDGING_AREA).
T_HREL_AUT	The authorization object consists of the following fields: • Company Code • Valuation Area • Activity	With this authorization object, you determine which activities are allowed for a hedging relationship within*Hedge Accounting for Positions* (P-HA) in a company code and valuation area. Use in function: *Manage Hedging Relationships* (transaction TPM100) The hedge risk category and hedging relationship category are not used at the moment. (The class of a hedging relationship is obsolete but cannot be deleted for technical reasons.)
T_TIME_GRI Time Pattern	Activities 02 Change 03 Display	This authorization object enables you to restrict who can display or change time patterns using function *Define Time Pattern* (transaction TOE_TIME_PATTERN).
T_TOE Hedge Management: Snapshot	The authorization object consists of the following fields: BUKRS Company Code CURRENCY Currency ACTVT Activity	With this authorization object, you can restrict who can display snapshots within Hedge Management

The table below shows the security-relevant authorization objects that are used by the *SAP Treasury and Risk Management* (class *FIFinancial Accounting*).

Standard Authorization Objects

Authorization Object	Permitted Activities	Description
F_RPCODE Repetitive Code	• Create and change to bring the data into the system, • Lock and release, to control usability, • Display, to enable the user to use the function, • Display change documents, to enable you to display the master data changes.	Repetitive codes are used to simplify processing of recurring payments. Such usage is agreed between the user and the bank. You should only use the delete function once you have carefully checked and agreed with the bank that it is clear that a repetitive code is no longer being used and may be deleted. A check is made of the authorization object during among other things repetitive code maintenance (OT81), with their use in vendor payment requests (RVND) and in the fast entry of repetitive payments (FRFT). The company code controls the organizational unit in which the activities named can be carried out. The partner type restricts the activities to those repetitive codes for which the payee has the specified type (house bank, vendor or Treasury business partner are examples). When you display change documents you can only restrict to company code.

14.3.1.4.2 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 MJBEHF01
    - 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 SAP NetWeaver Security Guide.

14.3.2 Financial Operations

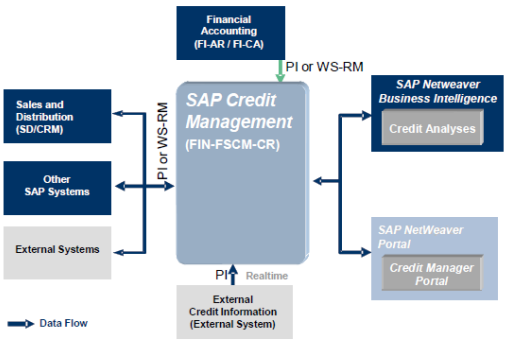
14.3.2.1 Receivables Management

14.3.2.1.1 SAP Credit Management

14.3.2.1.1.1 Technical System Landscape

Use

This figure shows an overview of the technical system landscape for *SAP Credit Management*.



Technical System Landscape

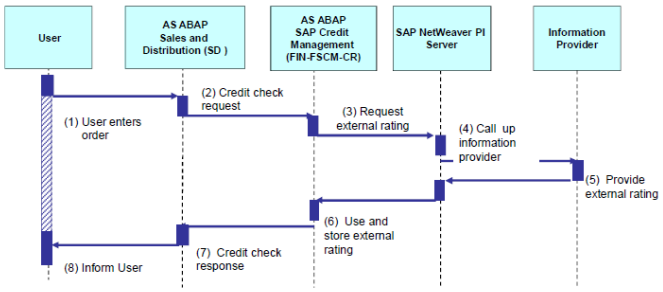
To exchange messages with external information providers, you have to use the Integration Server. For accounting systems as well as Sales and Distribution (SD) systems, you can configure the communication either via the Integration Server or via a point to point connection using Web Services Reliable Messaging (WSRM). The SAP Business Information Warehouse is connected via Remote Function Call (RFC).

For more information about recommended security zone settings, see *SAP NetWeaver Security Guide (Complete)*.

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 *SAP NetWeaver Security Guide* for the usage types Enterprise Portal Core (EPC) and SAP Enterprise Portal (EP) in the portal security guide.

14.3.2.1.1.2 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

14.3.2.1.1.3 User Management

Standard Users

This table shows the standard users that are necessary for operating *SAP Credit Management*.

System	User ID	Type	Password	Description
SAP Credit Management, client systems	For example, `CREDITXIUSER`	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 *SAP Credit Management* 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.

14.3.2.1.1.4 Authorizations

Standard Roles

This table shows the standard roles that are used by *SAP Credit Management*.

Role	Description
`SAP_FIN_FSCM_CR_USER`	SAP Credit Management - Credit Analyst
`SAP_XI_IS_SERV_USER`	SAP Process Integration: Integration Server Service User

The authorization objects for role `SAP_FIN_FSCM_CR_USER` are described in the following section.

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:

- Credit Segment

- Activity, with the following definitions:
  - 01 Add or Create
  - 02 Change
  - 03 Display
  - 06 Delete
  - 08 Display Change Documents
  - 43 Release

The role `SAP_FIN_FSCM_CR_USER` is delivered with all authorizations to this authorization object.

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`. The fields of this authorization object are:

- Application Log Object Name
- Application Log Subobject
- Activity, with the definitions
  - 03 Display
  - 06 Delete

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
`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

Object Name	Subobject	Meaning
FIN-FSCM-CR-MASS	ERROR ERROR_BIG ERROR_PROG ERROR_UPD INFO STATISTICS SUCCESS WARNING	Logs of mass changes, can be differentiated by the severity of the error

Procedure

You can organize the authorizations of your users as follows:

Activities	Authorization	Activity
Restrict access to one or more credit segments	F_UKM_SGMT with specified credit segment	
Edit master data	F_UKM_SGMT	01 02 03
Display master data	F_UKM_SGMT	03
Delete master data	F_UKM_SGMT	06
Display change documents for master data changes	F_UKM_SGMT	08
Release and reject credit limit changes/ increases requested (dual control principle)	F_UKM_SGMT	43
Edit and display master data of *SAP Credit Management*	B_BUPA_RLT with the business partner role UKM000	
Display and/or delete application logs of *SAP Credit Management*	S_APPL_LOG with the object names and subobjects listed above	03 06

14.3.2.1.1.5 Communication Destinations

Use

This table shows an overview of the communication destinations used by *SAP Credit Management*.

Connection Destinations when Using the Integration Server

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 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.

14.3.2.1.1.6 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.

14.3.2.1.1.7 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.

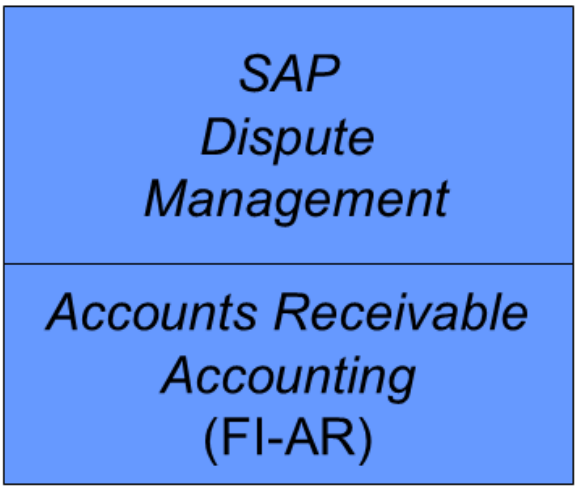
14.3.2.1.2 SAP Dispute Management

14.3.2.1.2.1 Technical System Landscape

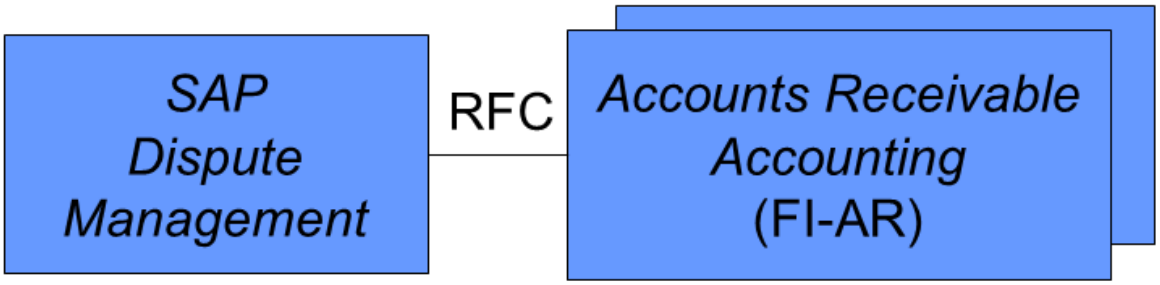
Use

You can use *SAPDisputeManagement* as a **one-system** or as a **multiple-system scenario** . If you use *SAPDisputeManagement* 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 *SAPDisputeManagement* 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 *SAPDisputeManagement* in a one-system scenario.



The figure below shows an overview of the technical system landscape of *SAPDisputeManagement* in a multiple-system scenario.



For more information about the technical system landscape, see the resources listed in the table below.

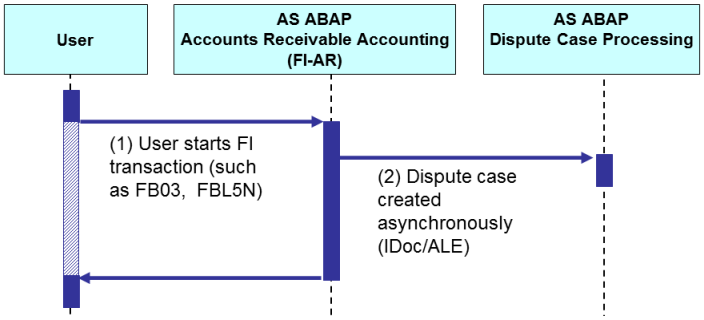
Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for *SAP Dispute Management* and the underlying components such as *SAP NetWeaver*	*Master Guide*	http://service.sap.com/instguides
High Availability	*High Availability for SAP Solutions*	http://sdn.sap.com/irj/sdn/ha

Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Design of the technical landscape	See applicable documents	http://sdn.sap.com/irj/sdn/landscape-design
Security	See applicable documents	http://sdn.sap.com/irj/sdn/security

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 *SAP NetWeaver Security Guide* for the usage types Enterprise Portal Core (EPC) and Enterprise Portal (EP) in the Portal security guide.

14.3.2.1.2.2 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 orFBL5N for line item list)	User type: dialog user
2	Dispute case is created asynchronously (IDoc/ALE)	User type: technical user or in the case of use of the Trusted/Trusting connection, dialog user (see also User Management [page 450])

As already mentioned under Technical System Landscape [page 447] , *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.

14.3.2.1.2.3 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 *SAPNetWeaver AS ABAP* (transactions SU01 and PFCG)	For more information, see User and Role Administration of Application Server ABAP in the SAP NetWeaver 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 *SAP NetWeaver 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: ALEREMOTE1_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: ALEREMOTE1_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: ALEREMOTE2_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:ALEREMOTE2_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.

14.3.2.1.2.4 Authorizations

Standard Roles:

The table below shows the standard roles used by *SAP Dispute Management* .

Role	Description
SAP_FIN_FSCM_DM_USER • One-system and multiple-system scenario	*FSCM Dispute Management - Processor* Contains the authorizations that an end user requires in Dispute Case Processing.
SAP_FIN_FSCM_DM_RFC_COMM • Multiple-system scenario	*RFC user (communication) in Dispute Case Processing* 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. Examples of such methods are creating dispute cases from Accounts Receivable and automatically changing dispute cases using clearing transactions in Accounts Receivable.

Role	Description
SAP_FIN_FSCM_DM_RFC_DIALOG • Multiple-system scenario	*RFC user (dialog) in Dispute Case Processing* 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.
SAP_FIN_FSCM_DM_AR_DIALOG • One-system scenario	*Role for Functions of Accounts Receivable* Contains authorizations required by end users in Dispute Case Processing so that they can call Accounts Receivable functions in Dispute Case Processing. Examples of such functions are including open items in a dispute case and navigating from a dispute case to a linked line item.
SAP_FIN_FSCM_DM_AR_RFC_DIALOG • Multiple-system scenario	*RFC user (dialog) in Accounts Receivable* 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. Examples of such methods are including open items in a dispute case and navigating from a dispute case to a linked line item.
SAP_FIN_FSCM_DM_AR_RFC_COMM • Multiple-system scenario	*RFC user (communication) in Accounts Receivable* Contains the authorizations required by a user to call *SAP Dispute Management* synchronous and asynchronous BAPI methods from the Dispute Case Processing system in the Accounts Receivable system. Examples of such methods are the automatic write off of dispute cases and automatic notification of Accounts Receivable when confirming and voiding cases.
SAP_FIN_FSCM_DM_DIALOG • One-system scenario	*Role for functions of Dispute Case Processing* Contains authorizations required by end users in Accounts Receivable so that they can call Dispute Case Processing functions in Accounts Receivable. Examples of such functions are creating/displaying dispute cases from transactions in Accounts Receivable and automatically changing dispute cases using clearing transactions in Accounts Receivable.

Role	Description
SAP_BC_CM_ADMINISTRATOR • One-system and multiple-system scenario	*Administrator in Case Management* Since the component *Case Management* represents the basis of *SAP Dispute Management*, you also require special *Case Management* authorizations when setting up *SAP Dispute Management*. These are included in this role.

14.3.2.1.2.5 Communication Destinations

Use

The following table shows an overview of the communication destinations used by *SAP Dispute Management* .

Destination	Delivered	Type	User, Authorizations	Description
Example: DM2FIN_DIAG	No	RFC	Under Authorizations [page 452] , you can see the roles for dialog users that you need for dialog calls that take place from the Dispute Case Processing system to the Accounts Receivable system.	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.
Example: DM2FIN_COMM	No	RFC	Under Authorizations [page 452] , you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Dispute Case Processing system to the Accounts Receivable system.	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.

Destination	Delivered	Type	User, Authorizations	Description
Example: FIN2DM_DIAG	No	RFC	Under Authorizations [page 452] , you can see the roles for dialog users that you need for dialog calls that take place from the Accounts Receivable system to the Dispute Case Processing system.	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.
Example: FIN2COL_COMM	No	RFC	Under Authorizations [page 452] , you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Accounts Receivable system to the Dispute Case Processing system.	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.

You can assign names for your RFC destinations as required. The names of the RFC destinations used above are merely examples.

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 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 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 clearings, reversals of clearings, or partial payments in the Accounts Receivable system, and therefore affect dispute cases, in the Dispute Case Processing system.

14.3.2.1.2.6 Data Storage Security

Use

Master data, transaction data, and Customizing data of *SAP Dispute Management* is stored in the database of the SAP system.

Access to the database is restricted by the authorization objects of *SAP Dispute Management* . To see the authorization objects relevant in *SAP Dispute Management* , see the roles listed under Authorizations [page 452] .

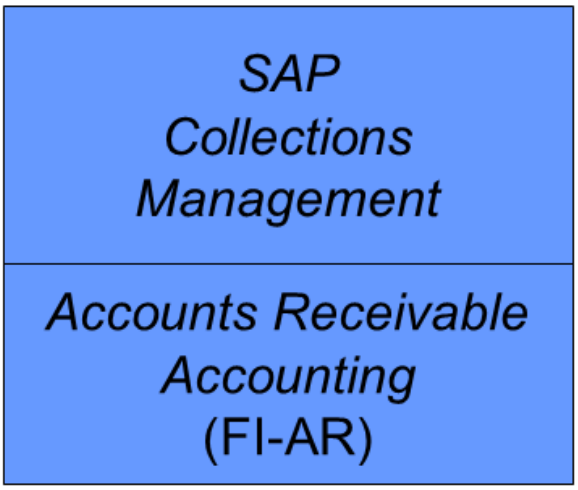
14.3.2.1.3 SAP Collections Management

14.3.2.1.3.1 Technical System Landscape

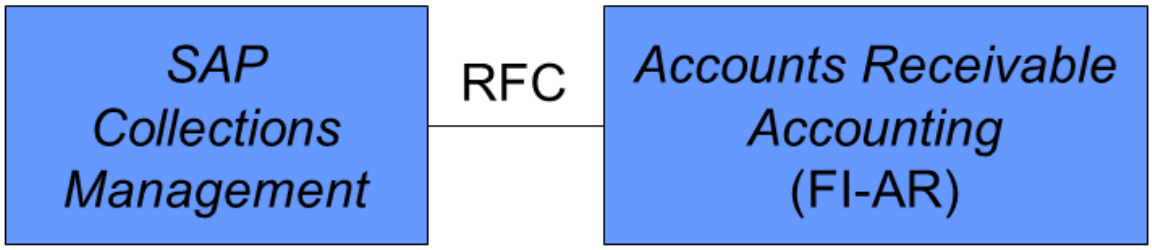
Use

You can use *SAP Collections Management* as a **one-system** or as 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** :

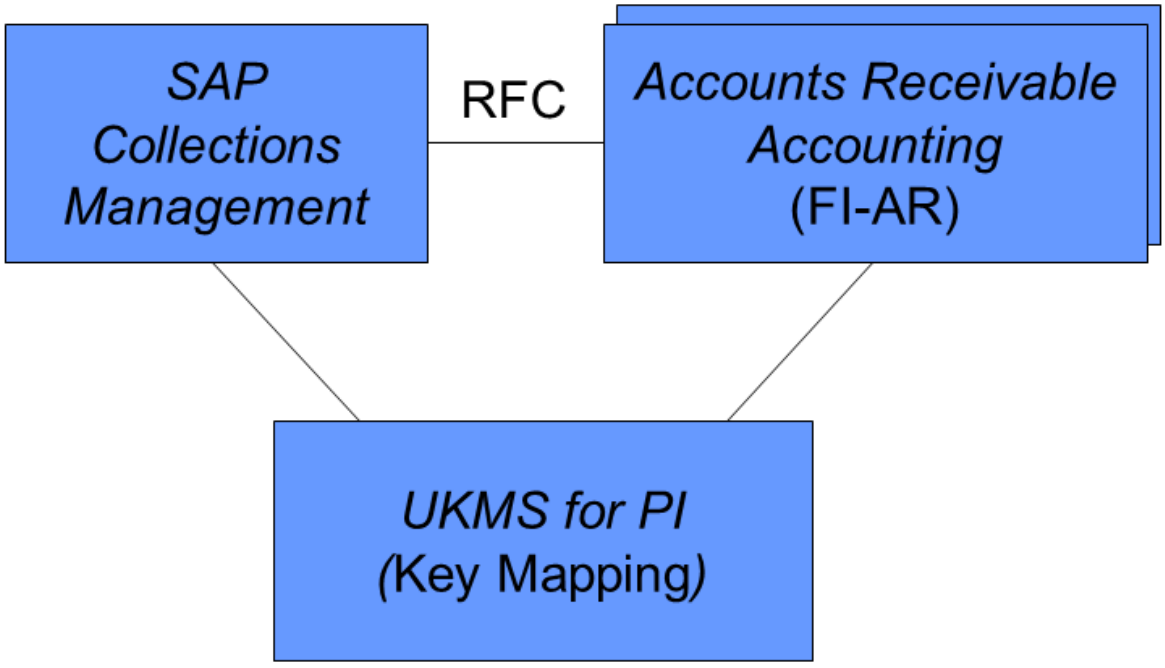


The following figure shows the technical system landscape in a **multiple-system scenario** :



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 NetWeaver Process Integration* (UKMS connection to *SAP NetWeaver PI*).

The figure below shows the technical system landscape in a **multiple-system scenario with several FI systems** :



For additional information, see theSAPNetWeaver library under *Business Services* > *Unified Key Mapping Service* > *Connection to SAP NetWeaver Process Integration* .

For more information about the technical system landscape, see the resources listed in the table below.

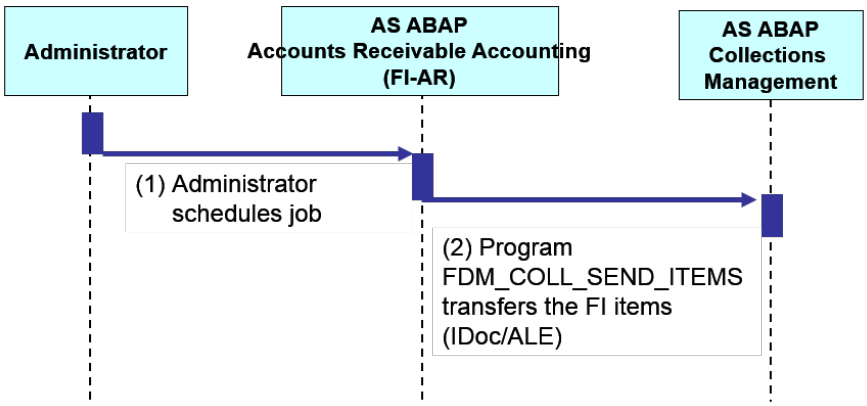
Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for *SAP Collections Management* and the underlying components such as *SAP NetWeaver*	*Master Guide*	http://service.sap.com/instguides
High Availability	*High Availability for SAP Solutions*	http://sdn.sap.com/irj/sdn/ha
Design of the technical landscape	See applicable documents	http://sdn.sap.com/irj/sdn/landscape-design
Security	See applicable documents	http://sdn.sap.com/irj/sdn/security

14.3.2.1.3.2 Security Aspects of Data, Data Flow and Processes

The following sections show an overview of the data flow in a multiple-system scenario.

14.3.2.1.3.2.1 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.

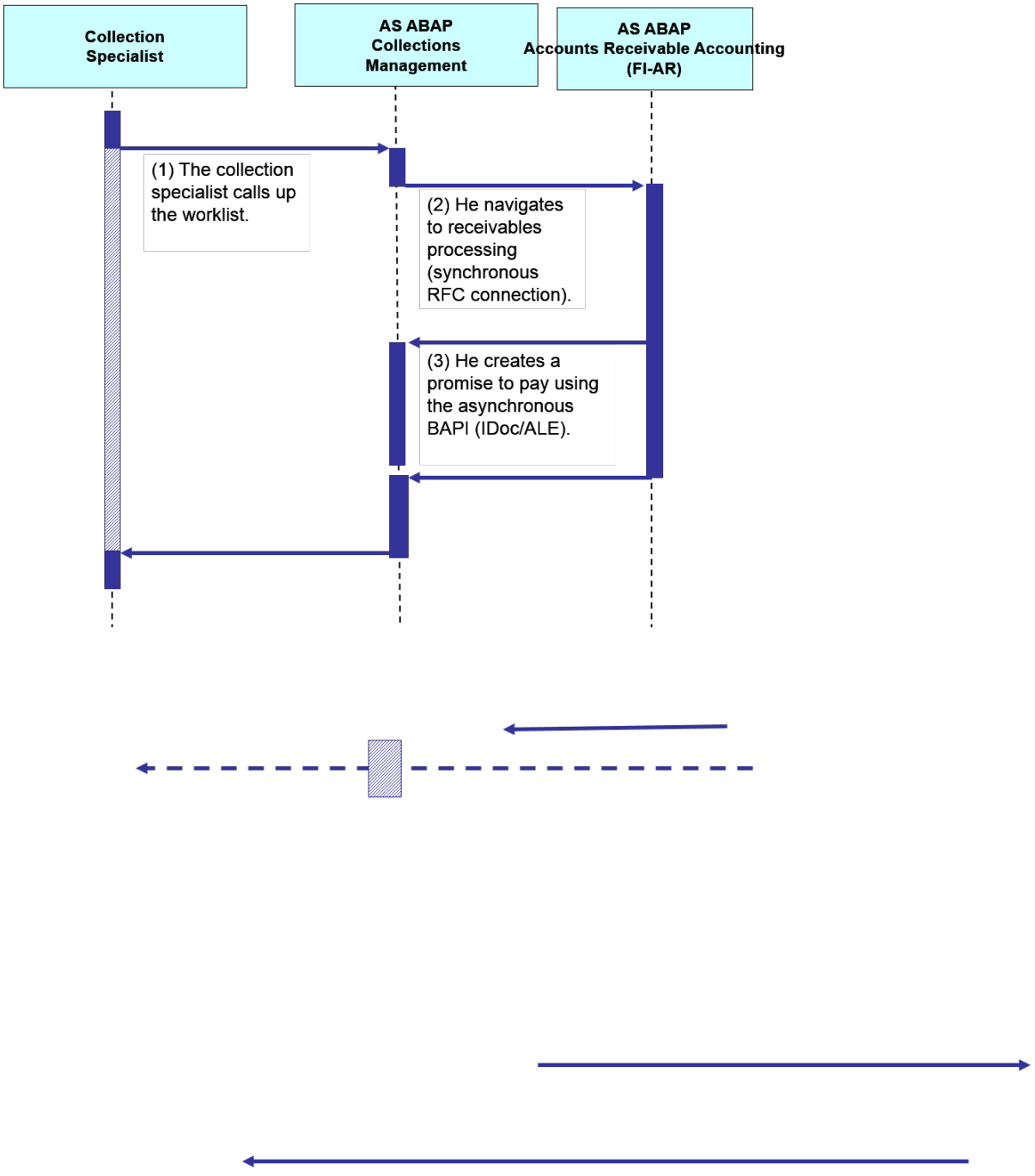


The table below shows the security aspect to be considered for the process step and what mechanism applies.

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)

14.3.2.1.3.2.2 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_SPECIAL-IST)	User type: Dialog user

Step	Description	Security Measure
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

14.3.2.1.3.3 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.

14.3.2.1.3.4 Authorizations

SAP Collections Management uses the authorization concept provided by *SAPNetWeaver*. Therefore, the security guidelines and recommendations as described in the *SAP NetWeaver AS Security Guide ABAP* also apply to *SAP Collections Management* .

The *SAPNetWeaver* authorization concept is based on assigning authorizations to users based on roles. For role maintenance in*SAP NetWeaver*, use the profile generator (transaction PFCG).

> **i Note**
>
> For more information about how to create roles, see the SAP NetWeaver Security Guide under User Administration and Authentication.

Standard Roles:

Role	Description
SAP_FIN_FSCM_COL_SPECIALIST • One-system and multiple-system scenario	*Collection Specialist* Contains the authorizations that the collection specialist needs to perform the activities in his task area. For example: • Calling the worklist • Displaying the business partner in *SAP Collections Management* • Navigating to *Process Receivables* • Creating contact persons in Collections Management • Creating promises to pay and dispute cases • Creating and changing customer contacts • Creating and changing resubmissions
SAP_FIN_FSCM_COL_MANAGER • One-system and multiple-system scenario	*Collection Manager* Contains the authorizations that the collection manager needs to perform the activities in his task area. In addition to all authorizations of the *collection specialist* (role SAP_FIN_FSCM_COLL_SPECIALIST), this covers the following actions, for example: • Definition of collection strategies • Definition of collection groups • Assignment of a strategy to a group • Change the role of the business partner specific to *SAP Collections Management* • Overview of several worklists • Distribution of worklist items to the collection specialists

Role	Description
SAP_FIN_FSCM_COL_ADMIN • One-system and multiple-system scenario	*Collections Management Administrator* Contains the authorizations that a user in the Collections Management system needs to start and monitor programs that run periodically and preferably in the background. For example: • Worklist generation • Distribution of worklist items to the collection specialists • Mass change of the role of the business partner specific to *SAP Collections Management* • Monitoring of parallel runs • Deleting Completed Resubmissions
SAP_FIN_FSCM_COL_DIALOG • One-system scenario	*Role for promise to pay functions* Contains authorizations required by end users in Accounts Receivable so that they can call promise to pay functions in Accounts Receivable. Examples are: • Creating, displaying, and changing promises to pay from receivables processing in Accounts Receivable • Automatic change of promises to pay as a result of clearing transactions in Accounts Receivable
SAP_FIN_FSCM_COL_RFC_DIALOG • Multiple-system scenario	*RFC user (dialog) for collections management functions* 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. For example, navigation from receivables processing to the detail display of the promise to pay or dispute case.
SAP_FIN_FSCM_COL_RFC_COMM • Multiple-system scenario	*RFC user (communication) for collections management* Contains authorizations for a user with which synchronous and asynchronous methods are called in the *SAP Collections Management* system from the Financial Accounting system. For example: • Posting of IDocs with data from Financial Accounting • Creation of dispute cases, promises to pay, customer contacts, and resubmissions • Reading of attributes of dispute cases, promises to pay, customer contacts, and resubmissions for display in receivables processing

Role	Description
SAP_FIN_FSCM_COL_AR_USER • One-system and multiple-system scenario	*End user in Receivables Processing* Contains the authorizations required by an end user in receivables processing in Accounts Receivable. This role is in the Accounts Receivable system.
SAP_FIN_FSCM_COL_AR_RFC_COMM • Multiple-system scenario	*RFC user (communication) in Accounts Receivable* Contains authorizations for a user with which synchronous and asynchronous methods are called from the *SAP Collections Management* system in the Financial Accounting system. An example of such a method is the automatic notification to Accounts Receivable when promises to pay are confirmed and voided.
SAP_FIN_FSCM_COL_AR_ADMIN • One-system and multiple-system scenario	*Collections Management Administrator Financial Accounting* Contains the authorizations that a user in the Accounts Receivable system needs to start and monitor programs that run periodically and preferably in the background. For example, the transfer of data relevant for *SAP Collections Management* from Accounts Receivable: • Valuating promises to pay • Automatic confirmation of promises to pay
SAP_FIN_FSCM_COL_AR_RFC_DIALOG • Multiple-system scenario	*RFC user (dialog) in Receivables Processing* 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: • Display of invoice data • Display of payment data • Display of invoice history • Creation, change, or display of a contact person

14.3.2.1.3.5 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.

Destination	Delivered	Type	User, Authorizations	Description
Example: COL2FIN_DIAG	No	RFC	Under Authorizations [page 463] , you can see the roles for dialog users that you need for dialog calls that take place from the Collections Management system to the Accounts Receivable system.	This destination is used for dialog calls that take place from the Collections Management system to the Accounts Receivable system by means of RFC.
Example: COL2FIN_COMM	No	RFC	Under Authorizations [page 463] , you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Collections Management system to the Accounts Receivable system.	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Collections Management system to the Accounts Receivable system.
Example: FIN2COL_DIAG	No	RFC	Under Authorizations [page 463] , you can see the roles for dialog users that you need for dialog calls that take place from the Accounts Receivable system to the Collections Management system.	This destination is used for dialog calls that take place from the Accounts Receivable system to the Collections Management system by means of RFC.
Example: FIN2COL_COMM	No	RFC	Under Authorizations [page 463] , you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Accounts Receivable system to the Collections Management system.	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Accounts Receivable system to the Collections Management system.

> **i Note**
>
> If you connect several FI systems in a multiple-system scenario and use the connection of *Unified Key Mapping Service* to *SAP NetWeaver Process Integration* (UKMS connection to *SAP NetWeaver PI*) 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 NetWeaver PI* (PI system)
> - Calls from the *Collections Management* system to the PI system
>
> > **i Note**
> >
> > 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* .
>
> 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).

You can assign names for your RFC destinations as required. The names of the RFC destinations used above are merely examples.

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.

14.3.3 Contract Accounting

14.3.3.1 Authorizations

Standard Roles

SAP delivers standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles. You specify roles that are used in Contract Accounts Receivable and Payable (FI-CA) in the SAP Easy Access menu by choosing *Tools* > *Administration* > *User Maintenance* > *Information System* > *Roles* > *Roles by Complex Selection Criteria* and entering `SAP_FI_CA*` in the *Role* field.

Contract Accounts Receivable and Payable (FI-CA) delivers only single roles.

Before using the roles listed, you may want to check whether the standard roles delivered by SAP meet your requirements.

Standard Authorization Objects

You can easily recognize the authorization objects currently used in Contract Accounts Receivable and Payable (FI-CA) from their technical name as follows:

1. In the SAP Easy Access menu choose *Tools* > *Administration* > *User Maintenance* > *Information System* > *Authorization Objects* > *By object name*.
2. Enter `F_KK*` in the *Authorization Object* field and execute your search.

In the result list, you can display the details for each selected authorization object such as authorization fields, documentation and permitted activities, if defined.

In addition, for the Clarification Processing area, the authorization object `S_CFC_AUTH` exists; for the Correspondence area, the authorization object `P_CORR`; and for prepaid processing, authorization objects exist that follow the naming convention `F_PREP*`. You can use Customizing roles to control access to the configuration of Contract Accounts Receivable and Payable (FI-CA) in the SAP Customizing Implementation Guide (IMG).

14.3.3.2 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 SAP NetWeaver Security Guide.

14.3.3.3 Enterprise Services Security

For general information, see the chapters on Web Services Security in the SAP NetWeaver Security Guide and in the SAP Process Integration Security Guide.

14.3.3.4 Other Security-Relevant Information

In Contract Accounts Receivable and Payable (FI-CA), some objects and special activities are protected by special authorizations. The associated authorization object is F_KK_SOND. See table TFKAUTH (use transaction SM30 to display) for information on all activities that you can protect with this authorization object.

14.3.4 Real Estate Management

14.3.4.1 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 an 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.

14.3.4.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *Product Assistance* ▶ *Cross Components* ▶ *Data Protection* ▶.

Relevant Archiving Objects

Archiving Object	Technical Name
Architectural Object	REFX_AO

Archiving Object	Technical Name
Adjustment Measure	REFX_AT
Business Entity	REFX_BE
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

Archiving Object	Technical Name
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`.

14.4 Manufacturing

14.4.1 Maintenance Operations

14.4.1.1 Authorizations in Plant Maintenance

Plant Maintenance uses the authorization concept provided by the SAP 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 SAP NetWeaver 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 NetWeaver Security Guide under User Administration and Authentication.

Standard Roles

SAP delivers the following standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles.

Roles for Plant Maintenance

Role	Description
SAP_COCKPIT_EAMS_MAINT_WORKER2	*Maintenance Worker 2* This role contains all the functions that a maintenance worker requires to carry out their work effectively and safely. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.
SAP_COCKPIT_EAMS_GENERIC_FUNC2	*Generic EAM Functions 2* The purpose of this role is to provide the maintenance planner with a broad range of functions necessary for planning and executing maintenance activities. As a pool role, it is not intended that you assign it to users as is, but that you use it as a basis for creating customer-specific roles.

14.5 Enterprise Technology

14.5.1 Geographical Enablement Framework

14.5.1.1 Authorizations

The framework uses the authorization concept provided by the SAP NetWeaver Application Server for 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
sap.gef.data::gef_user	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 SAP_GEF_USER or other reference users that are created.
sap.gef.data::gef_admin	In addition to all the authorizations provided in the gef_user 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
G_GEF_GEOM	GEF_BO_ID	Business Object ID
	GEF_CONTXT	Geometry Context ID
	ACTVT	Activity

14.5.1.2 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 SAP NetWeaver Security Guide.

14.5.1.3 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.

14.5.1.4 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.

14.6 Master Data Governance

14.6.1 Authorization Objects and Roles Used by SAP MDG, Consolidation and Mass Processing

Authorization Objects

SAP MDG, consolidation and mass processing uses the authorization objects listed below.

Authorization Object	Description
MDC_PROOT [page 481]	Consolidation Root Permissions

Authorization Object	Description
MDC_PFILT [page 483]	Consolidation Cluster Permissions
MDC_MASS [page 483]	Mass Update Permissions
MDC_ADMIN [page 484]	Administrative permissions
B_BUPA_RLT	Business Partner: BP Roles
B_BUPA_GRP	Business Partner: Authorization Groups
S_BGRFC	Authorization Object for NW bgRFC
M_MATE_MAR	Material Master: Material Types
M_MATE_MAT	Material Master: Materials
M_MATE_WGR	Material Master: Material Groups

> ⚠ Caution
>
> To use *SAP MDG, consolidation and mass processing* in combination with the functions of SAP MDG, central governance, see the required authorization objects in the documents listed below:
>
> - Authorization Objects and Roles Used by SAP MDG, Central Governance [page 485]
> - Master Data Governance for Business Partner (CA-MDG-APP-BP) [page 487]
> - Master Data Governance for Supplier (CA-MDG-APP-SUP) [page 488]
> - Master Data Governance for Customer (CA-MDG-APP-CUS) [page 490]
> - Master Data Governance for Material (CA-MDG-APP-MM) [page 493]

Standard Roles

Frontend Launchpad Role	Name
SAP_BR_BUPA_MASTER_SPECIALIST	Master Data Specialist - Business Partner Data
SAP_BR_PRODMASTER_SPECIALIST	Master Data Specialist - Product Data
SAP_BR_BPC_EXPERT	Configuration Expert - Business Process Configuration

Backend Authorization Role	Name
SAP_MD_MDC_ADMIN_APP_03	MDG, Consolidation and Mass Processing: Administrator

Backend Authorization Role	Name
SAP_MD_MDC_DISP_BP_APP_03	MDG, Consolidation and Mass Processing: Business Partner Display
SAP_MD_MDC_SPEC_BP_APP_03	MDG, Consolidation and Mass Processing: Business Partner Special
SAP_MD_MDC_DISP_BP_NOBS_APP_03	MDG, Consolidation and Mass Processing: Business Partner Non-SAP
SAP_MD_MDC_SPEC_BP_NOBS_APP_03	MDG, Consolidation and Mass Processing: Business Partner Non-SAP
SAP_MD_MDC_DISP_MM_APP_03	MDG, Consolidation and Mass Processing: Material Display
SAP_MD_MDC_SPEC_MM_APP_03	MDG, Consolidation and Mass Processing: Material Specialist
SAP_MD_MDC_ADM_CUSTOBJ_APP_03	MDG, Consolidation and Mass Processing: Custom Objects Administrator
SAP_MD_MDC_DISP_CUSTOBJ_APP_03	MDG, Consolidation and Mass Processing: Custom Objects Display
SAP_MD_MDC_SPEC_CUSTOBJ_APP_03	MDG, Consolidation and Mass Processing: Custom Objects Specialist

14.6.1.1 MDC_PROOT

Use

This document describes details of the authorization object MDC_PROOT.

Features

The activities listed below are assigned to the authorization object.

Activity	Text	Authorization
01	Create or generate	Create consolidation process

Activity	Text	Authorization
02	Change	Run consolidation process The *Start*, *Retry*, *Rollback*, and *Save* buttons become active. **i Note** Either the *Start* or the *Continue* button is displayed, depending on whether the process has started or not.
03	Display	Display consolidation process
06	Delete	Delete consolidation process The *Delete* button becomes active.
31	Confirm	Continue consolidation process after a process step has been executed • The *Continue* button becomes active. • If the process pauses at a check point, the *Continue* button stays active only if the activity 31 Confirm is permitted. **i Note** Either the *Start* or the *Continue* button is displayed, depending on whether the process has started or not.
36	Extended maintenance	Adjust configuration within the process UI for the current process The *Adjust* link is displayed.
37	Accept	Continue consolidation process after a *matching* step **that still contains open match groups** • The *Continue* button becomes active. • If the process pauses at a check point and still open match groups exist, the *Continue* button stays active only if the activity 37 Accept is permitted. **⚠ Caution** In addition, the activity 31 Confirm has to be permitted. **i Note** Either the *Start* or the *Continue* button is displayed, depending on whether the process has started or not.

14.6.1.2 MDC_PFILT

Use

This document describes details of the authorization object `MDC_PFILT`

To create a process you have to select a *Source*, which is a combination of *Source System*, *Status*, and an optional *Source Filter*.

Features

The attribute *Source Filter* `MDC_FILTER` is assigned to the authorization object: Depending on the permitted value the processes are displayed in the process list and the sources are displayed in the *Sources* dialog box during the process creation.

14.6.1.3 MDC_MASS

Use

This document describes details of the authorization object `MDC_MASS`.

Features

The activities listed below are assigned to the authorization object.

Activity	Text	Authorization
`01`	Create or generate	Create mass processes
`02`	Change	Run mass processes The *Start*, *Retry*, *Rollback* and *Save* buttons become active. **i Note** Either the *Start* or the *Continue* button is displayed, depending on whether the process has started or not.
`03`	Display	Display mass processes

Activity	Text	Authorization
06	Delete	Delete mass processes The *Delete* button becomes active.
31	Confirm	Continue or rollback mass processes after a process step has been executed. The *Continue* button and the *Rollback* button become active. **⚠ Caution** If the process pauses at a check point, the *Continue* button and the *Rollback* button stay active only if the activity 31 Confirm is permitted. **i Note** Either the *Start* or the *Continue* button is displayed, depending on whether the process has started or not.
36	Extended maintenance	Adjust configuration within the process UI for the current process The *Adjust* link is displayed.

14.6.1.4 MDC_ADMIN

Use

This document describes details of the authorization object MDC_ADMIN

Features

The activities listed below are assigned to the authorization object.

Activity	Text	Authorization
02	Change	Change process parameters in the process UI like: • *Adapter* for a process step • *Adapter Configuration* • *Check Point*

Activity	Text	Authorization
06	Delete	Delete processes with an inconsistent status - for example caused by a system error - directly in the UI. **i Note** As an alternative you can run the transaction MDC_ADMIN_DELETE in the backend system to delete processes with an inconsistent status.
60	Import	Run the report MDC_BP_TRANSFORM_SOURCE_DATA. This report transforms customer and vendor data to business partner data during the data import.

14.6.2 Authorization Objects and Roles Used by SAP MDG, Central Governance

Authorization Objects

The following authorization objects are used by all components of Master Data Governance.

i Note

To obtain more detailed information about specific authorization objects proceed as follows:

1. Choose *SAP Menu* > *Tools* > *ABAP Workbench* > *Development* > *Other Tools* > *Authorization Objects* > *Objects* (Transaction SU21).
2. Select the authorization object using and then choose .
3. On the *Display authorization object* dialog box choose *Display Object Documentation*.

Authorization Object	Description
MDG_MDF_TR	Master Data: Transport
MDG_IDM	Key Mapping
USMD_CREQ	Change Request
USMD_MDAT	Master Data
USMD_MDATH	Hierarchies
USMD_UI2	UI Configuration

Authorization Object	Description
DRF_RECEIVE	Authorization for outbound messages for receiver systems
DRF_ADM	Create Outbound Messages
CA_POWL	Authorization for iViews for personal object worklists
BCV_SPANEL	Execute Side Panel
BCV_USAGE	Usage of Business Context Viewer
MDG_DEF	Data Export
MDG_DIF	Data Import
S_DMIS	Authority object for SAP SLO Data migration server

> ⚠ Caution
>
> For information about component specific authorization objects, see the corresponding sections:
>
> - Master Data Governance for Business Partner (CA-MDG-APP-BP) [page 487]
> - Master Data Governance for Supplier (CA-MDG-APP-SUP) [page 488]
> - Master Data Governance for Customer (CA-MDG-APP-CUS) [page 490]
> - Master Data Governance for Material (CA-MDG-APP-MM) [page 493]
> - Master Data Governance for Financial (CA-MDG-APP-FIN) [page 495]
> - Master Data Governance for Custom Objects (CA-MDG-COB) [page 496]

Standard Role

Role	Name
SAP_MDG_ADMIN	Master Data Governance Administrator

This role contains authorizations needed for administrative tasks and for setting up a base configuration in all components of Master Data Governance. Some authorizations enable critical activities. If multiple users in your organization are entrusted with the administration and configuration of Master Data Governance, we recommend that you split the role into several roles, each with its own set of authorizations. The role does not contain the authorizations for the respective master data transactions.

Enterprise Search

To use the *Enterprise Search* users have to be assigned to the role SAP_ESH_SEARCH *Enterprise Search Hub (Composite): Authorizations for searching*.

14.6.2.1 Master Data Governance for Business Partner (CA-MDG-APP-BP)

Use

Authorization Objects

Master Data Governance for Business Partner mainly uses the authorization objects of the business objects Business Partner, the authorization objects of the Application Framework for Master Data Governance, and the authorization objects of the Data Replication Framework.

Authorization Object	Description
B_BUPA_GRP **i Note** This authorization object is optional. You need to assign this authorization object only if master data records are to be specifically protected.	Business Partner: Authorization Groups
B_BUPA_RLT	Business Partner: BP Roles
B_BUPR_BZT	Business Partner Relationships: Relationship Categories
B_CCARD	Payment Cards
BCV_QUILST	Overview
DC_OBJECT	Data Cleansing
BCV_PERS	Personalize BCV UI for Query View
BCV_QRYVW	Query View
BCV_QUERY	Query
BCV_QVWSNA	Query View Snapshot
S_START	Start Authorization Check for TADIR Objects
S_PB_CHIP	ABAP Page Builder: CHIP
S_PB_PAGE	ABAP Page Builder: Page Configuration

⚠ Caution

Authorization objects used by all components of Master Data Governance are listed in the document Authorization Objects and Roles Used by SAP MDG, Central Governance [page 485].

Standard Roles

Role	Name
SAP_MDGBP_MENU_04	Master Data Governance for Business Partner: Menu
SAP_MDGBP_DISP_04	Master Data Governance for Business Partner: Display
SAP_MDGBP_REQ_04	Master Data Governance for Business Partner: Requester
SAP_MDGBP_SPEC_04	Master Data Governance for Business Partner: Specialist
SAP_MDGBP_STEW_04	Master Data Governance for Business Partner: Data Steward

14.6.2.2 Master Data Governance for Supplier (CA-MDG-APP-SUP)

Use

Authorization Objects

Master Data Governance for Supplier does not have dedicated authorization objects, but instead uses the authorization objects of the business objects Business Partner and Vendor, the authorization objects of the Application Framework for Master Data Governance, and the authorization objects of the Data Replication Framework.

Authorization Object	Description
B_BUPA_GRP **i Note** This authorization object is optional. You need to assign this authorization object only if master data records are to be specifically protected.	Business Partner: Authorization Groups
B_BUPA_RLT	Business Partner: BP Roles
B_BUPR_BZT	Business Partner Relationships: Relationship Categories
DC_OBJECT	Data Cleansing
F_LFA1_APP	Vendor: Application Authorization

Authorization Object	Description
F_LFA1_BEK	Vendor: Account Authorization
	i Note This authorization object is optional. You need to assign this authorization object only if master data records are to be specifically protected.
F_LFA1_BUK	Vendor: Authorization for Company Codes
F_LFA1_GEN	Vendor: Central Data
F_LFA1_GRP	Vendor: Account Group Authorization
M_LFM1_EKO	Purchasing organization in supplier master data
BCV_PERS	Personalize BCV UI for Query View
BCV_QRYVW	Query View
BCV_QUERY	Query
BCV_QUILST	Overview
BCV_QVWSNA	Query View Snapshot
S_START	Start Authorization Check for TADIR Objects
S_PB_CHIP	ABAP Page Builder: CHIP
S_PB_PAGE	ABAP Page Builder: Page Configuration
C_DRAD_OBJ	Create/Change/Display/Delete Object Link
C_DRAW_DOK	Authorization for document access
C_DRAW_STA	Authorization for document status
C_DRAW_TCD	Authorization for document activities
C_DRAW_TCS	Status-Dependent Authorizations for Documents

⚠ Caution

Authorization objects used by all components of Master Data Governance are listed in the document Authorization Objects and Roles Used by SAP MDG, Central Governance [page 485].

Standard Roles

Role	Name
SAP_MDGS_MENU_04	Master Data Governance for Supplier: Menu
SAP_MDGS_DISP_06	Master Data Governance for Supplier: Display
SAP_MDGS_REQ_06	Master Data Governance for Supplier: Requester
SAP_MDGS_SPEC_06	Master Data Governance for Supplier: Specialist
SAP_MDGS_STEW_04	Master Data Governance for Supplier: Data Steward
SAP_MDGS_VL_MENU_04	Master Data Governance for Supplier (ERP Vendor UI): Menu
SAP_MDGS_LVC_MENU_04	Master Data Governance for Supplier (Lean Request UI): Menu
SAP_MDGS_LVC_REQ_04	Master Data Governance for Supplier (Lean Request UI): Requester

14.6.2.3 Master Data Governance for Customer (CA-MDG-APP-CUS)

Use

Authorization Objects

Master Data Governance for Customer does not have dedicated authorization objects, but instead uses the authorization objects of the business objects Business Partner and Customer, the authorization objects of the Application Framework for Master Data Governance, and the authorization objects of the Data Replication Framework.

> **i** Note
>
> Depending on whether you use the Master Data Governance for Customer on a hub system or on a client systema different set of authorization objects is required.

Authorization Object	Description	Hub System	Client System
B_BUPA_GRP **i Note** This authorization object is optional. You need to assign this authorization object only if master data records are to be specifically protected.	Business Partner: Authorization Groups	x	x
B_BUPA_RLT	Business Partner: BP Roles	x	x
B_BUPR_BZT	Business Partner Relationships: Relationship Categories	x	x
B_CCARD	Payment Cards	x	x
DC_OBJECT	Data Cleansing	x	
F_KNA1_APP	Customer: Application Authorization	x	x
F_KNA1_BED **i Note** This authorization object is optional. You do not need to assign this authorization object if no master records are to be specifically protected.	Customer: Account Authorization	x	x
F_KNA1_BUK	Customer: Authorization for Company Codes	x	x
F_KNA1_GEN	Customer: Central Data	x	x
F_KNA1_GRP	Customer: Account Group Authorization	x	x
MDGC_LCOPY	Copy Customer Master Data from MDG Hub	—	x
V_KNA1_BRG	Customer: Account Authorization for Sales Areas	x	x
V_KNA1_VKO	Customer: Authorization for Sales Organizations	x	x
BCV_PERS	Personalize BCV UI for Query View	x	x
BCV_QRYVW	Query View	x	x

Authorization Object	Description	Hub System	Client System
BCV_QUERY	Query	x	x
BCV_QUILST	Overview	x	x
BCV_QVWSNA	Query View Snapshot	x	x
S_START	Start Authorization Check for TADIR Objects	x	x
S_PB_CHIP	ABAP Page Builder: CHIP	x	x
S_PB_PAGE	ABAP Page Builder: Page Configuration	x	x
C_DRAD_OBJ	Create/Change/Display/Delete Object Link	x	x
C_DRAW_DOK	Authorization for document access	x	x
C_DRAW_STA	Authorization for document status	x	x
C_DRAW_TCD	Authorization for document activities	x	x
C_DRAW_TCS	Status-Dependent Authorizations for Documents	x	x

> ⚠ Caution
>
> Authorization objects used by all components of Master Data Governance are listed in the document Authorization Objects and Roles Used by SAP MDG, Central Governance [page 485].

Standard Roles

Role	Name
SAP_MDGC_MENU_04	Master Data Governance for Customer: Menu
SAP_MDGC_DISP_05	Master Data Governance for Customer: Display
SAP_MDGC_REQ_05	Master Data Governance for Customer: Requester
SAP_MDGC_SPEC_05	Master Data Governance for Customer: Specialist
SAP_MDGC_STEW_04	Master Data Governance for Customer: Data Steward

Role	Name
SAP_MDGC_CL_MENU_04	Master Data Governance for Customer (ERP Customer UI): Menu
SAP_MDGC_LCC_MENU_04	Master Data Governance for Customer (Lean Request UI): Menu
SAP_MDGC_LCC_REQ_04	Master Data Governance for Customer (Lean Request UI): Requester

If you want to restrict the authorizations for users or roles to specific values, go to *Create Authorizations for Data Model* and define which entity types and attributes are authorization relevant.

14.6.2.4 Master Data Governance for Material (CA-MDG-APP-MM)

Authorization Objects

Master Data Governance for Material does not have dedicated authorization objects, but instead uses, for example, the authorization objects of the Material Master and the Application Framework for Master Data Governance.

Authorization Object	Description
K_TP_VALU	Transfer Price Valuations
M_MATE_MAF	Material Master: Material Locks
M_MATE_MAT	Material Master: Material
M_MATE_MAR	Material Master: Material Type
M_MATE_WGR	Material Master: Material Group
M_MATE_STA	Material Master: Maintenance Status
M_MATE_MTA	Material Master: Change Material Type
M_MATE_WRK	Material Master: Plant
M_MATE_MAN	Material Master: Central Data
M_MATE_NEU	Material Master: Create
M_MATE_BUK	Material Master: Company Codes

Authorization Object	Description
M_MATE_VKO	Material Master: Sales Organization/Distribution Channel
M_MATE_LGN	Material Master: Warehouse Numbers
C_KLAH_BKL	Authorization for Classification
C_KLAH_BSE	Authorization for Selection
C_TCLA_BKA	Authorization for Class Types
C_DRAD_OBJ	Create/Change/Display/Delete Object Link
C_DRAW_DOK	Authorization for document access
C_DRAW_TCD	Authorization for document activities
C_DRAW_TCS	Status-Dependent Authorizations for Documents
C_DRAW_BGR	Authorization for authorization groups
C_DRAW_STA	Authorization for document status
C_FVER_WRK	PP-PI: Production Version - Plant
DRF_RECEIV	Authorization for outbound messages for receiver systems
DRF_ADM	Create Outbound Messages
PLM_SPUSR	Superuser by Object Type **i Note** You need this authorization object for the object type PLM_MAT only if the search object connector of SAP NetWeaver Enterprise Search is created for the following Enterprise Search software components: • PLMWUI • Software components that include PLMWUI
C_AENR_BGR	CC Change Master – Authorization Group
C_AENR_ERW	CC Eng. Chg. Mgmt. Enhanced Authorization Check
C_AENR_RV1	CC Engineering change mgmt – revision level for material
BCV_QUILST	Overview

> ⚠ Caution
>
> Authorization objects used by all components of Master Data Governance are listed in the document Authorization Objects and Roles Used by SAP MDG, Central Governance [page 485].

Standard Roles

Role	Name
SAP_MDGM_MENU_06	Master Data Governance for Material: Menu
SAP_MDGM_DISP_06	Master Data Governance for Material: Display
SAP_MDGM_REQ_06	Master Data Governance for Material: Requester
SAP_MDGM_SPEC_06	Master Data Governance for Material: Specialist
SAP_MDGM_STEW_06	Master Data Governance for Material: Data Steward

If you want to restrict the authorizations for users or roles to specific values, run the Customizing activity under *Master Data Governance, Central Governance* > *General Settings* > *Data Modeling* > *Define Authorization Relevance per Entity Type* and define which entity types and attributes are authorization relevant.

14.6.2.5 Master Data Governance for Financials (CA-MDG-APP-FIN)

Authorization Objects

Authorization Object	Description
USMD_DIST > ℹ Note > This authorization object is used if you have not activated business function MDG_FOUNDATION. > (Switch: FIN_MDM_CORE_SFWS_EHP5)	Distribution
USMD_EDTN	Edition

> ⚠ Caution
>
> Authorization objects used by all components of Master Data Governance are listed in the document Authorization Objects and Roles Used by SAP MDG, Central Governance [page 485].

Standard Roles

Role	Description
SAP_MDGF_ACC_DISP_07	Master Data Governance for Financials: Accounting Display
SAP_MDGF_ACC_REQ_07	Master Data Governance for Financials: Accounting Requester
SAP_MDGF_ACC_SPEC_07	Master Data Governance for Financials: Accounting Specialist
SAP_MDGF_ACC_STEW_04	Master Data Governance for Financials: Accounting Data Steward
SAP_MDGF_CO_DISP_04	Master Data Governance for Financials: Controlling Display
SAP_MDGF_CO_REQ_06	Master Data Governance for Financials: Consolidation Requester
SAP_MDGF_CO_SPEC_04	Master Data Governance for Financials: Consolidation Specialist
SAP_MDGF_CO_STEW_04	Master Data Governance for Financials: Consolidation Data Steward
SAP_MDGF_CTR_DISP_04	Master Data Governance for Financials: Controlling Display
SAP_MDGF_CTR_REQ_06	Master Data Governance for Financials: Controlling Requester
SAP_MDGF_CTR_SPEC_04	Master Data Governance for Financials: Controlling Specialist
SAP_MDGF_CTR_STEW_04	Master Data Governance for Financials: Controlling Data Steward

If you want to restrict the authorizations for users or roles to specific values, run the Customizing activity under *Master Data Governance, Central Governance* > *General Settings* > *Data Modeling* > *Define Authorization Relevance per Entity Type* and define which entity types and attributes are authorization relevant.

14.6.2.6 Master Data Governance for Custom Objects (CA-MDG-COB)

Authorization Objects

You can use the following authorization objects for Master Data Governance for Custom Objects.

Authorization Object	Description
USMD_DIST	Replication
USMD_DM	Data Model
USMD_EDTN	Edition Type

> ⚠ Caution
>
> Authorization objects used by all components of Master Data Governance are listed in the document Authorization Objects and Roles Used by SAP MDG, Central Governance [page 485].

Standard Role

Role	Name
SAP_MDGX_MENU_04	Master data governance for self-defined objects
SAP_MDGX_FND_SAMPLE_SF_05	Master Data Governance for Custom Objects - Flight Data Model (MDG 8.0)

If you want to restrict the authorizations for users or roles to specific values, run the Customizing activity under *Master Data Governance, Central Governance* > *General Settings* > *Data Modeling* > *Define Authorization Relevance per Entity Type* and define which entity types and attributes are authorization relevant.

14.6.3 Authorization Objects and Roles Used by SAP MDG, Master Data Quality

Authorization Objects

SAP MDG, master data quality uses the authorization objects listed below.

Authorization Object	Description
MDQ_EVAL [page 498]	Evaluation
MDQ_RULREP [page 499]	Rule Repository

> ⚠ Caution
>
> To use *SAP MDG, master data quality* in combination with the functions of SAP MDG, central governance, see the required authorization objects in the documents listed below:
>
> - Master Data Governance for Material (CA-MDG-APP-MM) [page 493]

Standard Roles

Frontend Launchpad Role	Name
SAP_BR_PRODMASTER_STEWARD	Master Data Steward - Product Data
SAP_BR_BPC_EXPERT	Configuration Expert - Business Process Configuration

14.6.3.1 MDQ_EVAL

Use

This document describes details of the authorization object MDQ_EVAL.

Features

The activities listed below are assigned to the authorization object.

Activity	Text	Authorization
01	Create or generate	**Backend** Enables the creation of evaluation run information (for example by using import API) **Manage Imports** Enables the import of objects with errors
02	Change	**Backend** Allows updating evaluation run information **Worklist for Products** • Allows status changes for objects with errors • Allows adding notes for objects with errors

Activity	Text	Authorization
03	Display	**Backend** Enables reading of evaluation data **Worklist for Products** • Restricts displaying the list of objects with errors • Enables displaying the details of an evaluation run • Defines the list of evaluation settings available in the value help **Manage Imports** • Defines the list of evaluation settings available in the value help • Restricts the list of data imports shown to the end user
06	Delete	**Backend** Enables the deletion of evaluation data via report MDQ_DELETE_EVALUATION_DATA

14.6.3.2 MDQ_RULREP

Use

This document describes details of the authorization object MDQ_RULREP.

Features

The activities listed below are assigned to the authorization object.

Activity	Text	Authorization
01	Create or generate	**Backend** Enables the creation of rule data information **Manage Imports** Enables the import of rule data information
02	Change	**Backend** Allows updating rule data information

Activity	Text	Authorization
03	Display	**Manage Imports** • Defines the list of Rule Repositories available in the value help • Restricts the list of data imports shown to the end user

15 SAP S/4HANA Compatibility Packs

15.1 Finance

15.1.1 Travel Management

15.1.1.1 Travel Management

Authorizations

Standard Roles in Travel Management (for Web Dynpro ABAP-Based Applications)

Role	Description
SAP_FI_TV_WEB_TRAVELER_2	*Traveler* The role contains the authorization profile needed to execute the applications of the *Travel and Expenses* Employee Self-Service (ESS) in *SAP NetWeaver Portal*.
SAP_FI_TV_WEB_TRAVELER_EXT_TP	*Traveler* 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. The role contains the authorization profile needed to execute the applications of the *Travel and Expenses* ESS in *SAP NetWeaver Portal*.
SAP_FI_TV_WEB_ESS_TRAVELER_2	*ESS Single Role for Travelers* Users with this role can execute the work center for travelers and the corresponding applications in NWBC. This role is integrated into the ESS role for Web Dynpro ABAP-based applications (SAP_EMPLOYEE_ESS_WDA_1).

Role	Description
SAP_FI_TV_WEB_ASSISTANT_2	*Travel Assistant* Users with this role can execute the work center for travel assistants and the corresponding applications in NWBC. The role contains the authorization profile needed to execute the applications of the *Travel and Expenses* ESS in *SAP NetWeaver Portal*.
SAP_FI_TV_WEB_ESS_ASSISTANT_2	*Travel Assistant* Users with this role can execute the work center for travel assistants and the corresponding applications in NWBC.
SAP_FI_TV_WEB_APPROVER_2	*Approving Manager* Users with this role can execute the work center for approving managers and the corresponding applications in NWBC. This role is integrated into the MSS role for Web Dynpro ABAP-based applications (SAP_MANAGER_MSS_NWBC).
SAP_FI_TV_WEB_POLICY_ADMIN_2	*Travel Policy Administrator* Users with this role can execute frequently used Customizing applications for policy management in NWBC.
SAP_FI_TV_TIC_AGENT	*Travel Interaction Center Agent* 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. The Travel Interaction Center is a Shared Services Center in *SAP Customer Relationship Management (SAP CRM)*.

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 NetWeaver 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 NetWeaver 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 NetWeaver 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 NetWeaver 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.

15.1.1.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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`.

15.2 R&D / Engineering

15.2.1 Product Safety and Stewardship

15.2.1.1 Product Compliance for Discrete Industries

15.2.1.1.1 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 SAP NetWeaver Security Guide also apply.

The SAP NetWeaver 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 12] in the *Introduction* section

15.2.1.1.1.1 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 12] in the *Introduction* section.

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

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).

15.2.1.1.1.2 Standard Roles

In *Product Compliance for Discrete Industries,* you use specific roles in the application to access content. These roles are designed to support your business processes.

The following roles are delivered:

- Roles for Foundation Processes [page 349]
- Roles for Managing Product Compliance for Discrete Industries [page 507]

Unless shown in the tables below, the roles are delivered without authorization profiles. The authorization profiles are generated from these roles.

> **i** Note
>
> The *Product Compliance for Discrete Industries* roles that are delivered contain specific configuration such as object-based navigation (OBN). In consequence, customizing these roles has a certain level of complexity. Custom roles can be created as follows without losing their specific configuration:
>
> 1. Create your custom PFCG role.
> 2. Copy the menu structure from the SAP_EHSM_MASTER role or the others that are delivered.
> 3. Generate the authorization profile.
> 4. Assign the custom role to end users.

15.2.1.1.1.2.1 Roles for Foundation Processes

Role	Description
SAP_EHSM_MASTER	Master PFCG role for *Product Compliance for Discrete Industries*. This role is intended for use as a copy template for the menu structures of the end user roles that are currently assigned.
SAP_EHSM_PROCESS_ADMIN	End user role for the person who is technically responsible for the workflow-based processes of EHS Management. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the S/4HANA system. This role can receive workflow items.

Role	Description
SAP_EHSM_FND_WF_PERMISSION	System user role for the Workflow Engine. This role contains the additional authorization profiles needed to process the workflows in the background. The users who process the workflows in the background should, in addition to the SAP_EHSM_FND_WF_PERMISSION role, be assigned the SAP_BC_BMT_WFM_SERV_USER role. For processing workflows for product compliance for discrete industries, users should also have the same authorization as the following roles: SAP_EHSM_PRC_BASMAT_SPEC SAP_EHSM_PRC_COMPL_ENG SAP_EHSM_PRC_COMPONENT_ENG

15.2.1.1.1.2.2 Roles for Managing Product Compliance for Discrete Industries

Role	Description
SAP_EHSM_ADMINISTRATOR	Administrator role for the person who monitors changes in master data for product compliance, compliance objects, and the application log. This person also corrects data issues, enters data for customers and suppliers, and manually imports incoming documents either from the front-end system or from an application server.
SAP_EHSM_PRC_COMPL_CONSUMER	End user role for the compliance consumer. This role can be adapted for use as four different sub-roles: purchasing agent, sales and services representative, mechanical engineer, and electrical engineer. This user role is responsible for maintaining awareness of regulations and compliance requirements and, depending on the purpose, can be responsible for maintaining product knowledge and data, configuring customer orders, scheduling service requests, research, and evaluating product data, or designing, testing and analysis of components.

SAP_EHSM_PRC_COMPL_MGR	End user role for the compliance manager. This user role monitors compliance-related programs for product lines, and defines policies and procedures for other departments to ensure compliance. The compliance manager approves the manufacturing processes and equipment that will be used in production, and supervises design compliance.
SAP_EHSM_PRC_COMPL_ENG	End user role for the compliance engineer. This user role monitors daily operations that contribute to ensuring compliance. The compliance engineer is responsible for the company compliance data set. He or she maintains compliance data in cooperation with the engineering teams, and cooperates with the compliance manager for up-to-date information about regulations. This role is involved in material-based and component-based engineering changes and new product reviews.
SAP_EHSM_PRC_COMPONENT_ENG	End user role for the component engineer. This user role selects and works with electrical or other components to be incorporated into future products, and handles management and documentation of purchased components. The component engineer approves parts obtained externally, works closely with vendors, and ensures compliance by following the established procedures and policies.
SAP_EHSM_PRC_BASMAT_SPEC	End user role for the basic material specialist. This user role is responsible for the selection of appropriate materials and surfaces for design parts, and approves their release for use. The basic material specialist decides the specific application of materials and surfaces, and maintains the material database.
SAP_EHSM_PRC_AUTO_CHANGE_PROC	System user role for the automated change processing. This role contains the authorization profiles needed to determine compliance information that is affected by a relevant change and executing the worklist of pending compliance information.
SAP_EHSM_PRC_REG_CHG_WLIST_PRO	System user role necessary for background processing of PRC Regulatory Change Worklist Generation (program `R_EHPRC_WL_REGCHG_GENERATE`) and PRC Regulatory Change Worklist Post Processing (program `R_EHPRC_WL_REGCHG_POST_PROC`).

SAP_EHSM_PRC_SUPPL_CHNG_PROC	This role contains as a suggestion all relevant authorization data necessary for background processing of PRC Supplier Change Processing. Supplier Change Monitor The program `R_EHPRC_PBB_SUPPL_CHNG_MON` is executed in background processing in order to monitor changes in supplier to material assignment and to start the workflow *Decide and Prepare for Assessment*if necessary.
SAP_EHSM_PRC_EML_REC	System user role for the e-mail recipient. This role contains the authorization profiles needed to receive and process e-mails.
SAP_BCV_USER	System user role for the display of Business Context Viewer (BCV). This role contains the authorization profiles and menus needed to display a BCV side panel and the BCV configuration.
SAP_BCV_ADMIN	System user role for the administration of Business Context Viewer (BCV). This role contains the authorization profiles and menus needed to administrate the BCV configuration.

15.2.1.1.1.3 Standard Authorization Objects

The following security-relevant authorization objects are used in *Product Compliance for Discrete Industries:*

- Authorization Objects for Foundation Processes [page 352]
- Authorization Objects for Managing Product Compliance [page 510]
- Authorization Objects for Integration [page 364]

15.2.1.1.1.3.1 Authorization Objects for Foundation Processes

Authorization Object	Field	Value	Description
EHFND_CHDC (Change Document)	ACTVT	03 (Display)	Activity
	BO_NAME	EHPRC_COMPLIANCE_DATA (Compliance Data)	Business Object Name
EHFND_WFT (Workflow Tools)	ACTVT	16 (Execute)	Activity
	TCD	All transactions of workflow tools	Transaction Code

Authorization Object	Field	Value	Description
EHFND_WFF (Workflow and Processes)	EHSM_COMP	Product Compliance (PRC)	Component of Product Safety and Stewardship
	PURPOSE	Process Purpose (see Customizing activity Specify Process Definitions)	Process Purpose
	EHSM_PVAR	Process Variant (see Customizing activity Specify Process Definitions)	Name of Process Variant
	EHSM_PCACT	CANCELPROC (Cancel Process)	Activity of Task or Process
EHFND_EXPP (Export Profile)	ACTVT	01 (Create, Generate)	Activity
	EHFND_EXPP		Configured Export Profile
EHFND_REGL (Regulatory List Content)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity

15.2.1.1.1.3.2 Authorization Objects for Managing Product Compliance

Authorization Object	Field	Value	Description
EHPRC_CMWL (Compliance Management Worklist (CMWL))	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
	WL_CAT	REG_CHG (Follow-Up Regulatory Change)	Worklist Category
EHPRC_CPM (RCS: Campaign Usage)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity

EHPRC_OLM1 (RCS: Object List Usage)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	EHPRC_OLGR	See the Customizing activity *Specify Object* List Groups under *Product Safety and Stewardship* > *Product Compliance for Discrete Industries* > *General Configuration*	Object List Group
EHPRC_CDO: RCS: Authorization Object for Compliance Object	ACTVT	01 Create or generate 02 Change 03 Display 06 Delete	Activity
	REQ		Compliance Requirement (Check)
	REV_STATUS		Compliance Data Revision Status
	CDCATEGORY		Compliance Data Category
S_PB_CHIP (ABAP Page Builder: CHIP)	ACTVT	03 (Display) 16 (Execute)	Activity Needed for displaying information on the side panel
	CHIP_NAME	X-SAP-WDY-CHIP:/BCV/CHIP* X-SAP-WDY-CHIP:EHPRC_CW_BCV_CHIP1 EHPRCWDCHIP_SPBN	Web Dynpro ABAP: CHIP ID
S_PB_PAGE (ABAP Page Builder: Page Configuration)	ACTVT	03 (Display)	Activity Needed for displaying information on the side panel
	CONFIG_ID	/BCV/SIDEPANEL	Configuration Identification
	PERS_SCOPE	1 (User))	Web Dynpro: Personalization

BCV_SPANEL (Execute Side Panel)	ACTVT	16 (Execute)	Activity Needed for displaying information on the side panel
	BCV_CTXKEY	EHPRC_COMPL_DATA	Context Key
BCV_USAGE (Business Context Viewer usage)	ACTVT	US (Use)	Activity Needed for displaying information on the side panel
BCV_QRYVW (Query View)	ACTVT	03 (Display)	Activity Needed for displaying information on the side panel
	BCV_CTXKEY	EHPRC_COMPL_DATA	Context Key
	BCV_QRYVID		ID of Query View
BCV_QUERY (Query)	ACTVT	03 (Display)	Activity Needed for displaying information on the side panel
	BCV_CTXKEY	EHPRC_COMPL_DATA	Context Key
	BCV_QRY_ID		Query ID
BCV_QUILST (Overview)	ACTVT	03 (Display)	Activity Needed for displaying information on the side panel
	BCV_CTXKEY	EHPRC_COMPL_DATA	Context Key
	BCV_QUIKID		ID of Overview

15.2.1.1.2 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 SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security

Guide also apply here. Details that specifically apply to *Product Safety and Stewardship* are described in the following sections:

- Communication Channel Security [page 519]
  This topic describes the communication paths and protocols.
- Network Security [page 520]
  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 520]
  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 *SAP NetWeaver Security Guide*:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

15.2.1.1.2.1 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
<AC system>	No	RFC	Connection to accounting system
<EHS system>	No	RFC	Connection to *SAP Product Safety and Stewardship* as part of *SAP ERP* system

> **i 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*.

15.2.1.1.3 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 19] 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`

15.2.1.1.4 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 SAP NetWeaver Security Guide.

15.2.1.1.5 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 22] in the *Introduction* section.

15.2.1.2 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

15.2.1.2.1 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.

15.2.1.2.2 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 12] in the *Introduction* section.

15.2.1.2.2.1 Authorizations

Product Safety and Stewardship for Process Industries uses the authorization concept that is provided by SAP NetWeaver and Microsoft Windows. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver Security Guide and the Microsoft Windows Security Guide also apply.

The following objects for authorization objects are used:

- Profiles
- Authorization objects

Profiles

The table below lists the profiles used. You can display all profiles in the profile list (transaction `SU02`).

Profile	Description
B_MASSMAIN	Mass maintenance tool
C_A.AV	Composite profile for person in charge of work scheduling
C_A.KONSTRUK	Composite profile for person in charge of engineering/ design
C_AENR_*	List of profiles for change management
C_ALL	PP: All authorizations for master data/classif. system
C_EHSG	List of profiles for Global Label Management
C_EHSH_*	Lists of profiles for Product Safety and Stewardship
C_FHMI_*	List of profiles for production resources/tools
C_MSTL_*	List of profiles for material BOMs
C_PS_*	List of profiles for Project Systems
C_ROUT_*	List of profiles for task lists
C_SHE_*	List of profile for list of profiles for Product Safety and Stewardship
E_CS_*	List of profiles for EC-CS
I_PM_*	List of profiles for Plant Maintenance
M_*	List of profiles for Materials Management

Authorization Objects

Object Class	Description
CLAS	Classification
CV	Document Management
EHS	Product Safety and Stewardship
LO	Logistics - General Exclusively the authorization objects for the variant configuration (character string `C_LOVC_*`).
MM_G	Materials Management – Master Data
MM_S	Materials Management – External Services
PM	Plant Maintenance
PP	Production Planning Authorization objects for the applications: • Change management (character string `C_AENR_*`) • Task lists (character string `C_ROUT*`) • BOMs (character string `C_STUE_*`)
PS	Project System

> **i Note**
>
> In *WWI* and *Expert Server Administration* (transaction `CGSADM`) you can create, delete, start, cancel, and configure the *WWI* generation servers (*WWI* servers) and the *Expert* servers. For *Expert*, you can upload and register *Expert* rules that are used to alter specification data.
>
> SAP recommends that you grant authorization to transactions `CG3Z` and `CG3Y` restrictively since they may allow uploading and downloading any files to or from the application server.

15.2.1.2.3 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 SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply here. Details that specifically apply to *Product Safety and Stewardship* are described in the following sections:

- Communication Channel Security [page 519]
  This topic describes the communication paths and protocols.
- Network Security [page 520]
  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 520]
  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 *SAP NetWeaver Security Guide*:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

15.2.1.2.3.1 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.

15.2.1.2.3.2 Network Security

Ports

WWI generation servers (WWI servers) and Expert servers use Remote Function Call (RFC).

For more information, see the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Service Marketplace at *http://service.sap.com/* under *Products* > *Database & technology* > *Security* > *Infrastructure Security*.

15.2.1.2.3.3 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`	No	RFC		RFC destination for *Business Partner*
Basic Data and Tools > *Basic Settings* > *Specify Environment Parameters* > Environment parameter `DEST_HR`	No	RFC		RFC destination for *HR*
Basic Data and Tools > *Basic Settings* > *Specify Environment Parameters* > Environment parameter `DEST_PM`	No	RFC		RFC destination for *Plant Maintenance*
Basic Data and Tools > *Basic Settings* > *Specify Environment Parameters* > Environment parameter `DEST_SRE_DS`	No	RFC		RFC destination of *Report Shipping*

Basic Data and Tools > *Basic Settings* > *Specify Environment Parameters* > Environment parameter `SVT_EHS_RFCDEST`	No	RFC		RFC destination for *Substance Volume Tracking*
Basic Data and Tools > *Basic Settings* > *Specify Environment Parameters* > Environment parameter `WWI_GENSERVER_SYN_DEST`	No	RFC	Calling user	Synchronous generation of reports
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* > Maintain the destination	No	RFC	Configured Background Job user See Customizing activity *Start WWI Dispatcher in Background*	Background generation of reports

Global Label Management > *Prerequisites for Global Label Management* > *Define WWI Settings* > *Configure WWI Server for Print Request Generation*	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 See Customizing activity *Background Jobs for Processing Print Requests*	Process print requests in *Global Label Management*
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

> **i 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.*

15.2.1.2.4 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

15.2.1.2.5 Data Storage Security

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 form 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	Uploade File; Downloade 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

15.2.1.2.5.1 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.

15.2.1.2.6 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**.

15.2.1.2.7 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.

15.2.1.2.8 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. 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\Systems`

For 32bit systems, omit `Wow6432Node`

15.3 Human Resources

15.3.1 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 SAP NetWeaver AS for ABAP (Transactions `SU01` and `PFCG`)	For more information, look for *User Administration and Identity Management in ABAP Systems* in the documentation of SAP NetWeaver at http://help.sap.com/netweaver.
User Management Engine of SAP NetWeaver AS for Java	This tool is used for user management of HR portal roles (business packages). For more information, look for *User Management Engine* in the documentation of SAP NetWeaver at http://help.sap.com/netweaver.

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
  - Admisnistrator
    - 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.

15.3.2 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 *SAP NetWeaver Application Server*. Therefore, the security recommendations and guidelines for authorizations detailed in the Security Guide for *SAP NetWeaver AS ABAP* and in the Security Guide for *SAP NetWeaver AS Java* 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*, see SAP Library for SAP ERP and choose *SAP ERP Central Component* > *Human Resources* > *HR Tools* and the section *Authorizations for Human Resources*.

The *SAP NetWeaver Application Server* authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PFCG`) on *SAP NetWeaver AS ABAP* and the *User Management Engine's* user administration console on *SAP NetWeaver AS Java*.

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 586] and Manager Self-Service [page 601] 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 (*Benefits*) component
SAP_HR_CM*	Roles for the PA-CM (*Compensation Management*) component
SAP_HR_CP*	Roles for the PA-CM-CP (*Personnel Cost Planning*) component
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 PA-PA (*Personnel Administration*) component
SAP_HR_PA_PF_xx_*	Roles for the PA-PF (*Pension Schemes*) component
SAP_HR_PD*	Roles for the PA-PD (*Personnel Development*) component
SAP_HR_RC*	Roles for the PA-RC (*Recruitment*) component
SAP_HR_REPORTING	Role for the Human Resources Analyst **i Note** This role is obsolete. We recommend that you no longer use this role.
SAP_ASR_ADMINISTRATOR	Enhancement of the role SAP_HR_PA_xx_* for the HR administrators that use the functions of the component PA-AS (*HR Administrative Services*)

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 Human Resources authorization objects, see SAP Library for SAP ERP and choose *SAP ERP Central Component* > *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 PROFL (structural profile). A check using this object enables user-specific contexts to be mapped in HR master data.
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 *HR Master Data* 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 PROFL (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 PROFL (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 *HR Administrative Services*. 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 *Authorization Concept of HCM Processes and Forms*.
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 *Authorization Concept for Employee Interaction Center (EIC)*.

> **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*.

15.3.3 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 SAP Library for SAP ERP on the SAP Help Portal at http://help.sap.com/erp *SAP ERP Central Component* > *Human Resources* > *HR Tools* in the following sections:

- *Creating Change Documents for Personnel Administration Infotypes*
- *Creation of Change Documents for Personnel Planning Infotypes*

15.3.4 Core HR and Payroll

15.3.4.1 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*

15.3.4.1.1 Authorizations

Use

The Personnel Management components use the two-part authorization concept from SAP Human Resources. For more information, see section *Authorizations* in the 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 S/4HANA on SAP Help Portal at *Human Resources* > *HR Tools* > *Authorizations for Human Resources* > *Technical Aspects* > *Authorization Objects* .

15.3.4.1.2 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 Special Protection
Interface Toolbox (Transaction PU12)	ALE	Master data, *Benefits* data, Organizational data as defined by the user	
SAP BW	Extractor Program	Master data, Organizational data, *Personnel Development* data	

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP CO (for distributed systems)	RFC	Cost centers, orders, and so on	Authorizations for CO objects are required here
External Files	ASCII	*Personnel Administration* data	Applicable only for country versions Australia and New Zealand
MS Word	Report Interface with SAP NetWeaver		Office Integration
Connection with PDF-based print forms for archiving	HTTP(S)	Person-related data (for example, employee photo)	

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
>
> If you convert the protocol from HTTP to HTTPS and use PDF-based print forms, see SAP Note 1461447.

For more information, see *Transport Layer Security* in the *SAP NetWeaver Security Guide* .

15.3.4.1.3 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

Function Group	Function Module	Description
	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 *Object and Data Provider* (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 *Account Assignment* and *Employee Subgroup*

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.

15.3.4.1.4 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 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_CK` (*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.

15.3.4.1.5 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.

15.3.4.1.6 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*)

15.3.4.1.7 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 (BAdI) 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 a using a grouping option for the authorization check to prevent users without authorization from maintaining person-related data.

15.3.4.1.7.1 Authorizations

Use

HCM Processes and Forms uses the authorization concept provided by the SAP NetWeaver AS for 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 SAP NetWeaver 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 section *Role Administration* in the SAP Library for *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 *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 *Business Package for Employee Self-Service* (up to and including *1.4.1*).
`SAP_ASR_MANAGER`	HR Administrative Services : Manager	This single role contains the authorizations for the Manager role.

> **i 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 *Process Object* of *HCM Processes and Forms*.
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	
S_SRMSY_CL	SAP Records Management : General Authorization Object	
S_TCODE	Transaction Code Check at Transaction Start	
P_ASRCONT	Authorization for Process Content	This authorization object manages the rights to start and execute processes with *HCM Processes and Forms*.

15.3.4.1.7.2 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.

15.3.4.1.7.3 Security for Additional Applications

For the uploading of attachments in *HCM Processes and Forms* you can use Business Add-In (BAdI) `HRASR00ATTACHMENT_HANDLING` for defining the file types allowed and the maximum size of attachments. For more information, see the BAdI documentation in the S/4HANA system.

15.3.4.1.7.4 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.

15.3.4.1.8 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:

- **SAP NetWeaver 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 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 information on security information for Gateway, please see:

Security Settings in the SAP Gateway

The SAP Gateway Foundation Security Guide available via http://help.sap.com//nw74 > *Security Information* > *Security Guide* and search for the document *SAP NetWeaver Gateway Foundation Security Guide*.

15.3.4.2 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.

15.3.4.2.1 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

Title	SAP Note	Comment
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)

15.3.4.2.2 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 *Payroll* 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*.

15.3.4.2.3 Authorizations

Role Concept and Authorization Concept for Payroll

Payroll uses the authorization concept provided by SAP NetWeaver Application Server for 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)	

Authorization Objects	Name	Description	Additional Information
P_PCLX	HR: Cluster	Check when accessing HR files on the PCLx (x = 1, 2, 3, 4) databases	SAP Library for 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 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 S/4HANA under *Authorizations for Human Resources* > *Technical Aspects* > *Authorization Objects* > *P_PE01 (HR: Authorization for Personnel Calculation Schemas)*
P_PE02	HR: Authorization for personnel calculation rule	Authorization check for personnel calculation rules	SAP Library for S/4HANA under *Authorizations for Human Resources* > *Technical Aspects* > *Authorization Objects* > *P_PE02 (HR: Authorization for Personnel Calculation Rule)*
P_PYEVDOC	HR: Posting document	Protection of actions on payroll posting documents	SAP Library for S/4HANA under *Authorizations for Human Resources* > *Technical Aspects* > *Authorization Objects* > *P_PYEVDOC (HR: Posting Document)*

Authorization Objects	Name	Description	Additional Information
P_PYEVRUN	HR: Posting run	Control of actions that are possible for posting runs	SAP Library for 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 S/4HANA under *Authorizations for Human Resources* > *Technical Aspects* > *Authorization Objects* > *P_OCWBENCH (HR: Activities in the Off-Cycle Workbench)*
S_TMS_ACT	Actions on TemSe objects	The authorization determines who may execute which operations on which TemSe objects	SAP Library for 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 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_PYEVDOC, 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_PYEVDOC, 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.

15.3.4.2.4 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 *External Wage Components* (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 SAP NetWeaver Security Guide ALE.

15.3.4.2.5 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 SAP NetWeaver Application Server (AS) ABAP. Payroll uses the standard security concept of SAP NetWeaver AS for 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 SAP NetWeaver Library under Authorization Checks and in SAP NetWeaver Application Server for ABAP. For the SAP NetWeaver Application Server for ABAP Security Guide, see SAP Service Marketplace at http://service.sap.com/securityguide.

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*

15.3.4.2.6 Security for Additional Applications

Display of Documents Using Remote Function Call (RFC)

Posting Data to Accounting

Administrators for Accounting can use the transaction PCP0 (*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_INFTY 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* .

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 ERP 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.

15.3.4.2.6.1 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 ERP 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)

Security Guide of Scenario, Application, or Component	Path
SAP Business Connector (BC)	*SAP Business Connector Security Guide*
SAP NetWeaver Exchange Infrastructure/Process Integration (XI/PI)	*SAP Process Integration (PI) Security Guides*

For a complete list of available SAP Security Guides, see SAP Service Marketplace at http://service.sap.com/securityguide.

Important SAP Notes

Currently, there are no security-relevant SAP Notes for B2A.

Authorizations

For more information, see *Authorizations*.

15.3.4.2.6.1.1 Authorizations

Use

B2A: Communication with Authorities uses the authorization concept provided by SAP NetWeaver AS for 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 (*HR-B2A: B2A Manager*)	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
	B2A_ACTIO		• S – Send Messages • D – Detail View for Messages • R – Reorganize Messages • L – Delete Messages • Z – Convert Status of Messages

15.3.4.2.7 Country-Specific Features

The following chapters contain information on country-specific features.

15.3.4.2.7.1 Country-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)

15.3.4.2.7.2 Country-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
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

Logical File Name	Reports That Use These Logical File Names
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.

Particularly Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the country version for Canada, this includes the social insurance number (SNI number) in the infotype *Personal Data* (0002).

More Information

See *Payroll (PY)* in the S/4HANA Security Guide.

15.3.4.2.7.3 Country-Specific Features: Switzerland

Authorizations

The country version for Switzerland (PA-PA-CH, PY-CH) 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 country version for Switzerland.

Standard Authorization Objects

The country 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 country version for Switzerland.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_CH_PK	KONNR (Individual PF Account Number) AUTGR (HR-CH: Authorization group for PF accounts) PKKLV (HR-CH: Pension fund : Authorization level for account access)		HR-CH: Pension Fund: Account Access (see *Authorizations for Human Resources* > *Technical Aspects* > *Authorization Objects* > *P_CH_PK (HR-CH: Pension Fund: Account Access)*)

For the documentation for the authorization object P_CH_PK, see SAP Library for 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 country 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 PI* and distributor/ authorities: HTTPS Internal communication between HR backend system and PI: RFC Adapter Internal communication between PI and PI: HTTP(S)	Personnel data	Personal data

* PI = SAP NetWeaver Exchange Infrastructure/Process Integration (XI/PI)

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 SAP NetWeaver Security Guide under Transport Layer Security.

For more information about B2A security, see *B2A: Communication with Authorities*.

More Information

See S/4 Security Guide for Human Resources and choose*Payroll (PY)*

15.3.4.2.7.4 Country-Specific Features: Germany

Authorizations

The country 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 country version for Germany (PY-DE, PA-PA-DE).

Standard Roles

For information about the standard roles used by Payroll, see *Authorizations*.

The following table shows the standard roles that the country 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 country version for Germany 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 Germany.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_DBAU_SKV HR: DBAU: Construction Industry Germany - Social Fund Procedure	ACTVT	• Add or Create • Display • Delete	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. For more information, see SAP Library for S/4HANA under *P_DBAU_SKV (HR: DBAU: Construction Pay Germany – Social Fund Procedure)*
	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	This object determines the authorization check within Statements (with SAPScript) for German Payroll. For more information, see SAP Library for S/4HANA under *P_DE_BW (HR-DE: Statements SAPScript)*

Authorization Object	Field	Value	Description
	BSUBJ	Functional Area ID for Statements Logical subdivision of statements according to individual topics Values 01–04	
	BACT	• E = Creation of Statements • A = Asynchronous Archiving • S = Fast Data Entry/Adhoc Query • D = Create Data Records • V = Administrate 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_PFAD
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_RPSPSDD0	RPSPSDD0	HR_DE_DIR_RPSPSDD0
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_RPXKHSD0	RPXKHSD0	HR_DE_DIR_RPXKHSD0
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

More Information

See *Payroll (PY)* under S/4HANA Security Guide Human Resources.

15.3.4.2.7.4.1 B2A: Communication with Authorities (PY-DE-BA)

About This Chapter

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 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)	http://service.sap.com/securityguide *SAP Business Connector Security Guide*
SAP NetWeaver Exchange Infrastructure/Process Integration (XI/PI)	http://service.sap.com/securityguide *SAP Process Integration (PI) Security Guides*

For a complete list of available SAP Security Guides, see SAP Service Marketplace at http://service.sap.com/securityguide.

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 from the HR system to the tax authorities.
- • ELENA: The data is encrypted and signed before being transferred from the HR system to the pension insurance.
- • SI (DEUEV, ...): The data is encrypted and signed before being transferred from the HR system to the health insurance fund.

Authorizations

For more information, see *Authorizations* under *B2A: Communication with Authorities*.

15.3.4.2.7.4.1.1 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): Communication channel RFC External: Middleware -> Tax authorities: Communication channel HTTP	Personnel data	Person-related data
ELENA	HTTP/HTTPS/E-mail	Personnel Data	Person-related data
SI (DEUEV, ...)	HTTP/E-mail	Personnel data	Person-related data

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Particular Protection
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 SAP NetWeaver 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	Transfer of data for ELSTER to middleware (BC, XI)
HR_DE_ELENA	No	HTTP/HTTPS	Transfer of data for ELENA to pension insurance
HR_DE_GKV	No	HTTP	Transfer of data for GKV to health insurance

Security-Relevant Logging and Tracing

- ELSTER: Tracing for error analysis using BI/BC is possible.
- ELENA: Tracing for error analysis using BC 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.

15.3.4.2.7.5 Country-Specific Features: Denmark

Authorizations

The country version for Denmark (PA-PA-DK, PY-DK) 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 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 S/4HANA and choose *Human Resources* > *HR Tools* > *Authorizations for Human Resources* > *Technical Aspects* > *Authorization Objects*.

More Information

See *Payroll (PY)* under S/4HANA Security Guide for Human Resources

15.3.4.2.7.6 Country-Specific Features: Spain

Authorizations

The country version for Spain (PA-PA-ES, PY-ES) 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 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) SUBTY (Subtype) PES_SPRPS (Lock indicator for HR master record) PES_FCODE (Function code) ACTVT (Activity)		Authorization check for the function codes that are permitted for the HR master data of the country version for Spain

More Information

See *Payroll (PY)* under S/4HANA Security Guide for Human Resources.

15.3.4.2.7.7 Country-Specific Features: Great Britain

Communication Channel Security

The following table presents the communication paths used by the country version for Great Britain (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 backend 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.

> → 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.

For more information about B2A security, see *B2A: Communication with Authorities*.

For an introduction and user guide for E-Filing Incoming, see SAP Service Marketplace at http://service.sap.com/hrgb in the Media Center.

Communication Destinations

You can communicate with the GB Inland Revenue 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 Great Britain* (PY-GB).

Logical File Names Used in Payroll Great Britain

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_RPUASHG0	RPUASHG0
HR_GB_DIR_RPUHESG1	RPUHESG1
HR_GB_DIR_RPUTPSG0	RPUTPSG0
HR_GB_DIR_RPUUSSG0	RPUUSSG0
HR_GB_DIR_RPUUSSG1	RPUUSSG1

Logical Path Names Used in Payroll Great Britain

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

More Information

See *Payroll (PY)* under S/4HANA Security Guide for Human Resources

15.3.4.2.7.8 Country-Specific Features: The Netherlands

Authorizations

The country version for The Netherlands (PA-PA-NL, PY-NL) 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 country version for The Netherlands.

Standard Authorization Objects

The country 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* (Personnel Management)
- *Authorizations* (Payroll)

The following table shows the security-relevant authorization objects that are also used in the country version for The Netherlands.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_NL_AEDM	JUPER (Legal person) ACTVT (Activity)		HR: Authorization object for Day-one-announcement
P_NL_LA06	JUPER (Legal person) ACTVT (Activity)		HR: Authorization object for wage return 2006
P_NL_PKAB	ACTVT (Activity)		Authorization object for PF Actuarial file
P_NL_PKEV	KASSE (Pension Fund) EVENT (HR-NL: Event) PKELV (Authorization level for reading event)		Authorization object for PF events
P_NL_PKFKT	PKNL_PKFKT (PK Function)		Authorization object for PF functions
P_NL_PKFXV	KASSE (Pension Fund) PKNL_FXVIE (Function view of fund)		Authorization object for PF function views
P_NL_PKTB	ACTVT (Activity)		Authorization object for PF pay scale calculation

Communication Destinations

You can use the *Gemeentelijke Basis Administratie* (GBA) interface to upload the inbound data for retirement pension plan for the country version for The Netherlands.

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources.

15.3.4.2.7.9 Country-Specific Features: Italy

Important SAP Notes

The following table presents the most important SAP Notes regarding security for the country version for Italy (PA-PA-IT, PY-IT).

Title	SAP Note	Comment
Change of master data in a productive payroll	385319	

Authorizations

The country version for Italy 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 country version for Italy.

Standard Authorization Objects

The country 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-Specific Authorization Objects

The following table shows the security-relevant authorization objects that are also used in the country version for Italy.

Country-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 RPCUEDI0)

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources

15.3.4.2.7.10 Country-Specific Features: Non-Profit Organizations

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 Non-Profit Organizations* (PY-NGO).

Logical File Names Used in Payroll for Non-Profit Organizations

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_UNUCMT_LOADER_FILE	HUNUCMT_LOADER

Logical Path Names Used in Payroll for Non-Profit Organizations

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

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources

15.3.4.2.7.11 Country-Specific Features: Norway

Authorizations

The country version for Norway (PY-NO, PA-PA-NO) 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 country version for Norway.

Standard Authorization Objects

The country 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 country version for Norway.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_NO_ALTIN	ACTVT (Activity)		Norway: Authorization to send data to Altinn Portal

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources.

15.3.4.2.7.12 Country-Specific Features: New Zealand

Sensitive Data

The Human Resources infotypes often contain sensitive data. This data is protected by central authorization objects. For the country version for New Zealand (PY-NZ, PA-PA-NZ), this affects the employee IRD number in the infotype *IRD Nbr New Zealand* (0309). You have the following options for accessing the number:

- Directly using the infotype *IRD Nbr New Zealand* (0309) with the transaction *Maintain HR Master Data* (PA30)
- By choosing the *IRD Number* pushbutton in the infotype *Tax New Zealand* (0313).

The authorizations required to read or change the IRD number depend on the authorizations in the user profile.

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources.

15.3.4.2.7.13 Country-Specific Features: Russia

Authorizations

The country version for Russia (PA-PA-RU, PY-RU) 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 country version for Russia.

Standard Authorization Objects

The country version for Russia 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 Russia.

Country-Specific Authorization Objects

Authorization Object	Field	Value	Description
P_RU_0294C	AUTHC (Authorization level)		HR-RU: Authorization for checking records of infotype 0294
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

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources.

15.3.4.2.7.14 Country-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 S/4HANA Security Guide for Human Resources.

15.3.4.2.7.15 Country-Specific Features: USA

Important SAP Notes

The following table presents the most important SAP Notes regarding security for the country version for USA (PA-PA-US, PY-US).

Title	SAP Note	Comment
Tax Reporter Transaction and Spool Security	430595	

Authorizations

The country version for USA 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 country version for USA.

Standard Authorization Objects

The country 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 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 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 Tax Factory for tax calculation	RFC	Tax data for the country 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 SAP NetWeaver 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 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 version for USA uses.

Communication Destinations

Destination	Provided	Type	Description

BSI	For country 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`

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`	`RPCTRTU1_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 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 S/4HANA system.

More Information

See *Payroll (PY)* in the S/4HANA Security Guide for Human Resources.

15.3.4.2.7.16 Country-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_B2AFILE	Report H99_B2AFILE	HR_XX_DIR_B2AFILE
HR_XX_DIR_RPUFCP01	Report RPUFCP01	HR_XX_DIR_RPUFCP01
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 S/4HANA Security Guide for Human Resources.

15.3.4.3 Self-Services

15.3.4.3.1 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 aforementioned 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 *Project Self-Services* (component EP-PCT-PLM-PSS).

15.3.4.3.2 User Management

Use

User management for *Self-Service* applications uses the mechanisms provided with the *SAP NetWeaver Application Server* , 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 SAP NetWeaver AS for 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 inSAPLibrary for *SAP NetWeaver* (see also *help.sap.com* > *Documentation* > *SAPNetWeaver*).

User Types

For information about the *user types* , see the *SAP NetWeaver 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.

15.3.4.3.3 Authorizations

Use

The *Self-Service* applications use the authorization concept provided by *SAP NetWeaver Application Server* . Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Security Guide for ABAP* also apply to the *Self-Service* applications.

The *SAP NetWeaver Application Server* 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.

15.3.4.3.3.1 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 Maintenance In the *Users and Roles* section in SAP Library for *SAP NetWeaver* (see also *help.sap.com* > *Documentation* > *SAP NetWeaver*).

15.3.4.3.3.2 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_CSKS_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.

15.3.4.3.4 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 `PFCG`. 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 Enterprise Portal, see SAP Library for S/4HANA on SAP Help Portal at *Cross-Application Functions in SAP ERP* > *Roles* > *Business Packages (Portal Content)*.
- For more information about the roles in SAP Business Client, see SAP Library for S/4HANA on SAP Help Portal at *Cross-Application Functions in SAP ERP* > *Roles* > *Roles in SAP NetWeaver Business Client*.
- For more information about SAP Business Client, see SAP Library for SAP NetWeaver on SAP Help Portal at *SAP NetWeaver by Key Capability* > *Application Platform by Key Capability* > *ABAP Technology* > *UI Technology* > *SAP NetWeaver Business Client*.

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.

15.3.4.3.4.1 User Administration and Authentication

User management for Employee Self-Service uses the mechanisms provided with the SAP NetWeaver Application Server for ABAP:

The security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server for ABAP Security Guide apply for *Employee Self-Service (WDA) in SAP NetWeaver 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*

15.3.4.3.4.1.1 User Management

Use

User management for *Employee Self-Service (WDA) in SAP NetWeaver Business Client for HTML* uses the mechanisms provided with the SAP NetWeaver Application Server for 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 *SAP NetWeaver 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.

15.3.4.3.4.1.2 Integration into Single Sign-On Environments

Use

Employee Self-Service supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Security Guide also apply to Employee Self-Service.

For more information about the available authentication mechanisms, see User Authentication and Single Sign-On in the *SAP NetWeaver Library*.

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*.

15.3.4.3.4.2 Authorizations

Use

Employee Self-Service uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to ESS.

The SAP NetWeaver 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 *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.
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 *Business Package for Employee Self-Service* (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 *Single Roles for Employee Self-Service (WDA)*.

Role	Name	Description
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	Authorizations for country-specific services for Hong Kong in Employee Self-Service (WDA).
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).

Role	Name	Description
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 *HR Process and Forms* 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 *Performance Management* application in Employee Self-Service (WDA).
SAP_TMC_EMPLOYEE_6	Employee in Talent Management	Authorizations for ESS services from the *Talent Management and Talent Development* application in Employee Self-Service (WDA). For more information, see *Employee in Talent Management*.
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).

> **i** 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 NetWeaver 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 S/4HANA Security Guide at *Human Capital Management* > *Authorizations*.
- *SAP E-Recruiting*
  See the S/4HANA Security Guide at *Human Capital Management* > *Talent Management* > *SAP E-Recruiting* > *Authorizations*.
- *HCM Processes and Forms*
  See the S/4HANA Security Guide at *Human Capital Management* > *Personnel Administration (PA)* > *HCM Processes and Forms* > *Authorizations*.
- *Travel Management*
  See the S/4HANA Security Guide at *Accounting* > *Financial Accounting* > *Travel Management (FI-TV)*.

15.3.4.3.4.3 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.

15.3.4.3.4.4 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 SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver 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 SAP NetWeaver Security Guide:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

15.3.4.3.4.4.1 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 SAP NetWeaver 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.

15.3.4.3.4.4.2 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 SAP NetWeaver Security Guide.

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see also the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Service Marketplace at http://service.sap.com/ under *Products* > *Database & technology* > *Security* > *Infrastructure Security*.

15.3.4.3.4.4.3 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 the 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*

15.3.4.3.4.5 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.

15.3.4.3.4.6 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.

15.3.4.3.4.7 Security-Relevant Logging and Tracing

Employee Self-Service relies on the logging and tracing mechanisms from SAP NetWeaver.

For more information, see the following topics:

- For the AS ABAP (relevant for *Employee Self-Service (WDA)*):
  Auditing and Logging

15.3.4.3.5 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 `PFCG`. 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 Enterprise Portal, see SAP Library for S/4HANA on SAP Help Portal at *Cross-Application Functions in SAP ERP* > *Roles* > *Business Packages (Portal Content)*.
- For more information about the roles in SAP Business Client, see SAP Library for S/4HANA on SAP Help Portal *Cross-Application Functions in SAP ERP* > *Roles* > *Roles in SAP NetWeaver Business Client*.
- For more information about SAP Business Client, see SAP Library for SAP NetWeaver on SAP Help Portal at http://help.sap.com/netweaver *SAP NetWeaver by Key Capability* > *Application Platform by Key Capability* > *ABAP Technology* > *UI Technology* > *SAP NetWeaver 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.

15.3.4.3.5.1 User Administration and Authentication

User management for Manager Self-Service uses the mechanisms provided with the SAP NetWeaver Application Server for ABAP.

The security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server for ABAP apply for *Manager Self-Service in SAP NetWeaver 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*

15.3.4.3.5.1.1 User Management

Use

User management for Manager Self-Service 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 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 SAP NetWeaver AS for 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.

15.3.4.3.5.1.2 Integration into Single Sign-On Environments

Use

Manager Self-Service supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Security Guide also apply to Manager Self-Service.

For more information about the available authentication mechanisms, see User Authentication and Single Sign-On in the *SAP NetWeaver Library* and section *Integration in Single Sign-On Environments* in the S/4HANA Security Guide.

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*.

15.3.4.3.5.2 Authorizations

Use

Manager Self-Service uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to Manager Self-Service. The SAP NetWeaver 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 *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 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.
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.

Role	Description
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 NetWeaver 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.
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.

Authorization Object	Description
K_CSKS_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.

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 S/4HANA Security Guide at *Human Capital Management* > *Authorizations*.
- *SAP E-Recruiting*
  See the S/4HANA Security Guide at *Human Capital Management* > *Talent Management* > *SAP E-Recruiting* > *Authorizations*.
- *HCM Processes and Forms*
  See the S/4HANA Security Guide at *Human Capital Management* > *Personnel Administration (PA)* > *HCM Processes and Forms* > *Authorizations*.
- *Travel Management*
  See the 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 0PERS_VAR. If required, you can fill this DataStore Object from structural authorizations (see *Structural Authorizations - Values* (0PA_DS02) and *Structural Authorizations - Hierarchy* (0PA_DS03)).

More Information

For more information, see the SAP Help Portal BI Content documentation for Human Resources at http://help.sap.com *SAP NetWeaver* > *SAP NetWeaver by Key Capability* > *Information Integration by Key Capability* > *BI Content* > *BI Content 705* > *Human Resources* > *Organizational Management* > *ODS Objects*.

15.3.4.3.5.3 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 NetWeaver 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
`icf/set_HTTPonly_flag_on_cookies`	0	Client-Dependent
`login/ticket_only_by_https`	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.

15.3.4.3.5.4 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 SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver 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 SAP NetWeaver Security Guide:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

15.3.4.3.5.4.1 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 SAP NetWeaver Security Guides.

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see also the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Service Marketplace at http://service.sap.com/ under *Products* > *Database & technology* > *Security* > *Infrastructure Security* .

15.3.4.3.5.4.2 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

15.3.4.3.5.5 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 .

15.3.4.3.5.6 Security-Relevant Logging and Tracing

Manager Self-Service relies on the logging and tracing mechanisms from SAP NetWeaver.

For more information, see the following topics:

- For the AS ABAP (relevant for *Manager Self-Service in SAP NetWeaver Business Client*):
  - Auditing and Logging
  - Tracing and Logging (for NWBC)

15.3.5 Talent Management

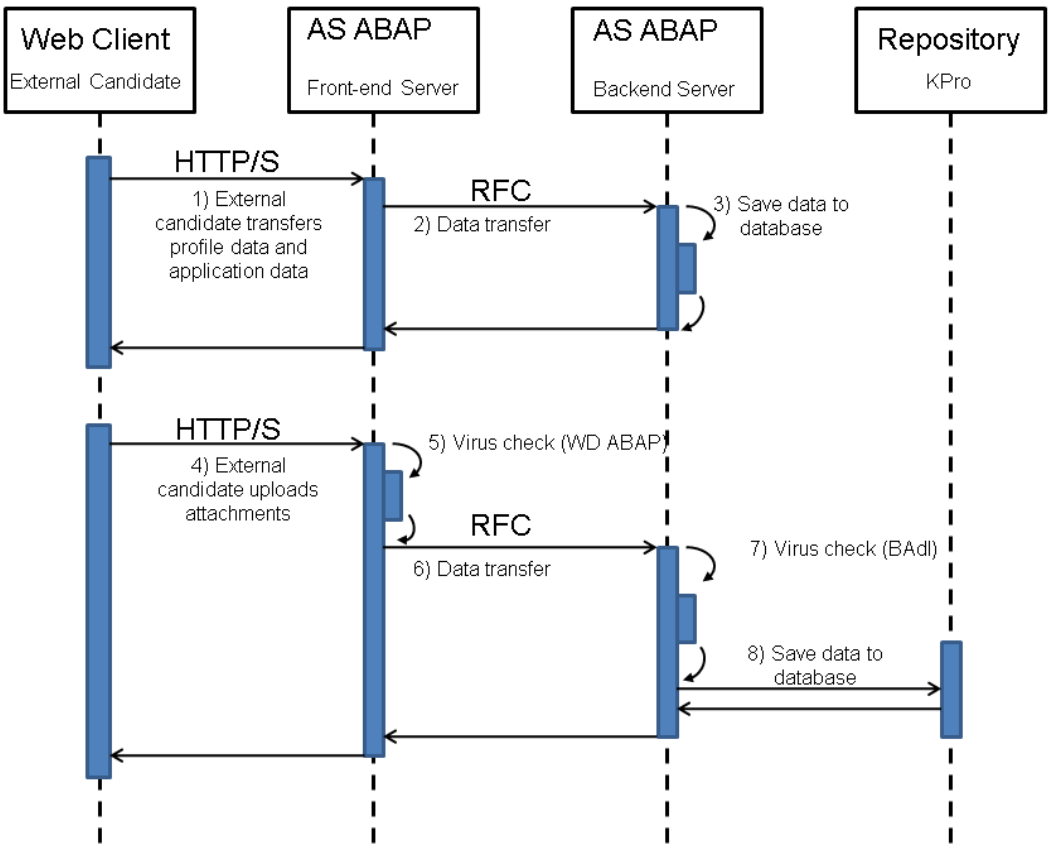
15.3.5.1 SAP E-Recruiting

15.3.5.1.1 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.

15.3.5.1.1.1 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 Action
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

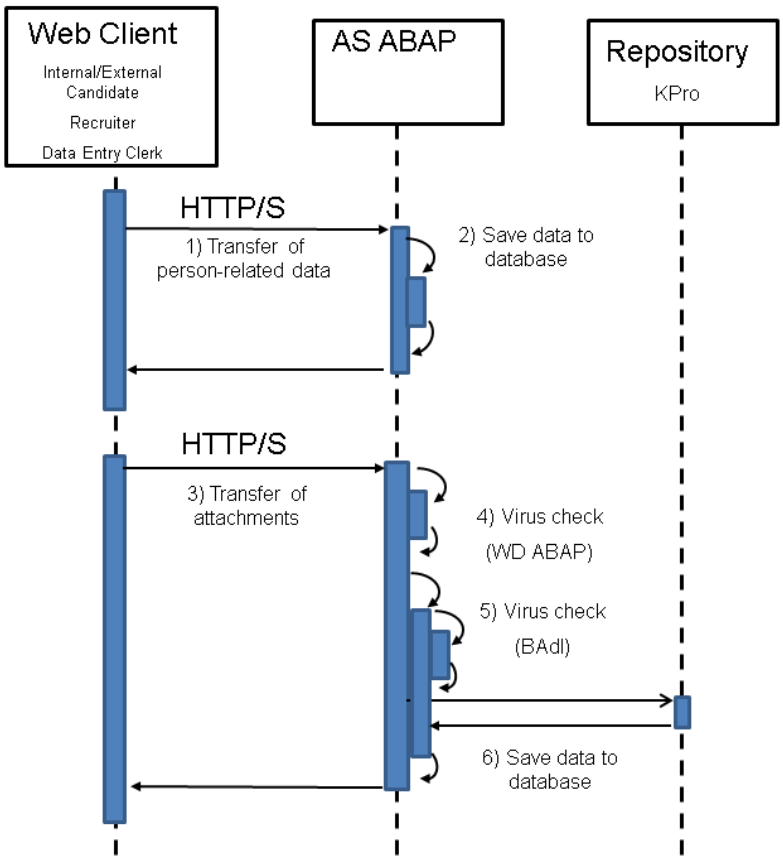
Step	Description	Security Action
7	Virus check (BAdI)	Additional virus check using the BAdI HRRCF00_DOC_UPLOAD (backend server) (see Customizing activity *BAdI: Upload Documents)*
8	Save data to database	Not relevant

15.3.5.1.1.2 Data Entry in Nondistributed System

The figure below provides an overview of the data flow for the following scenario: Data entry in the 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.

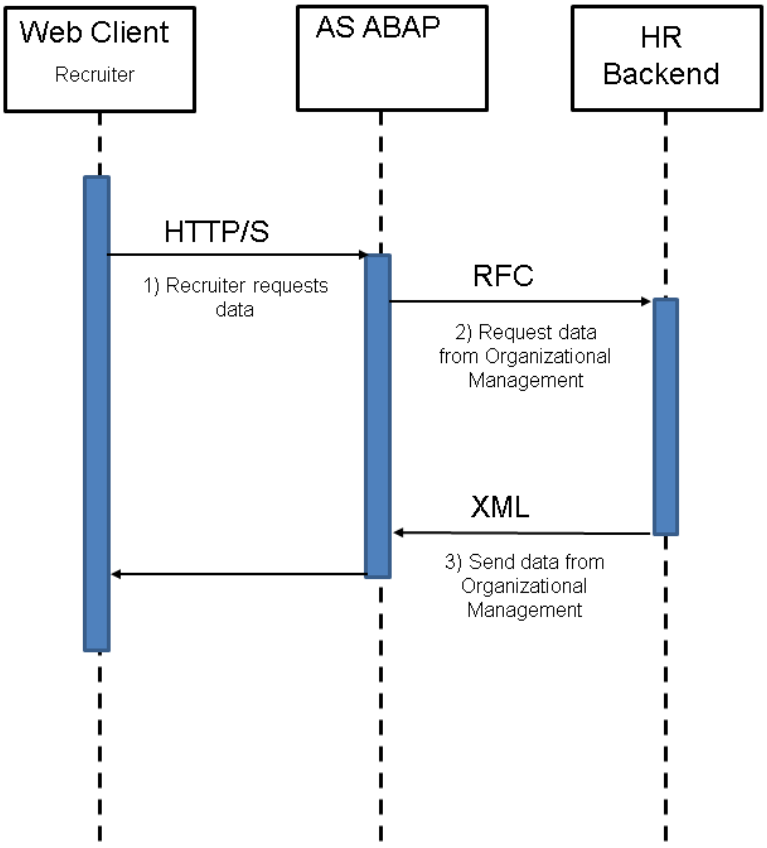


The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Action
1	Transfer of data	External candidate has to confirm the data privacy statement.
2	Save data to database	Not relevant
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 (BAdI)	Additional virus check using the BAdI HRRCF00_DOC_UPLOAD (backend server) (see Customizing activity *BAdI: Upload Documents)*
6	Save data to database	Not relevant

15.3.5.1.1.3 Integration of Org. Mgmt/E-Recruiting in Distributed System

The figure below provides an overview of the data flow for the scenario: Integration of Organizational Management in SAP E-Recruiting in a distributed system.

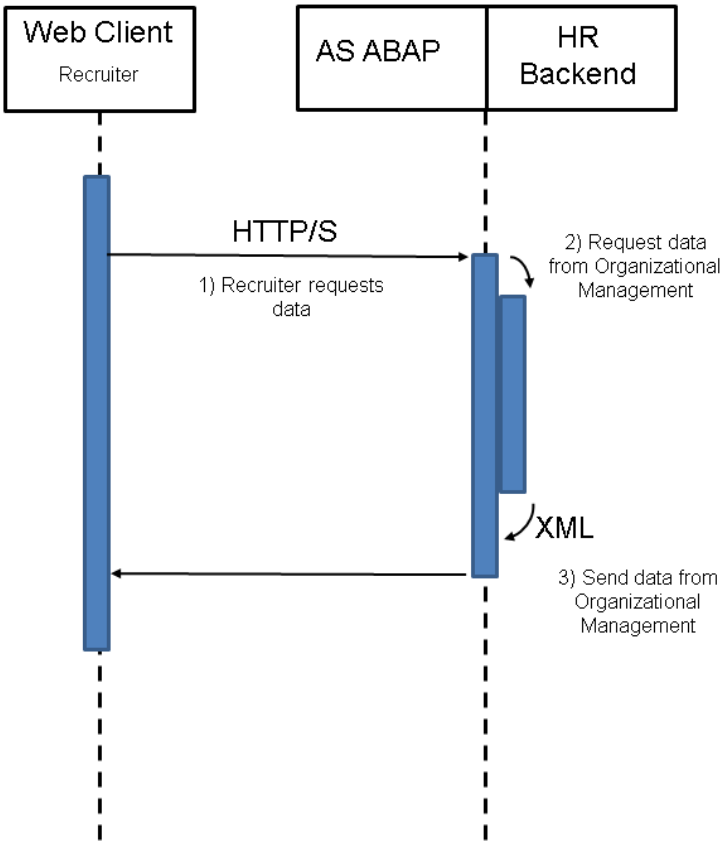


The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Description	Security Action
1	The recruiter requests data overviews for organizational units, positions, or jobs.	Not relevant
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

15.3.5.1.1.4 Integration of Org. Mgmt/E-Recruiting in Integrated System

The figure below provides an overview of the data flow for the 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 Action
1	The recruiter requests data overviews for organizational units, positions, or jobs.	Not relevant
2	The SAP NetWeaver Application Server requests the Organizational Management data in the integrated HR system.	Not relevant

Step	Description	Security Action
3	The integrated HR system transfers the data using XML to the SAP NetWeaver Application Server.	XML encryption

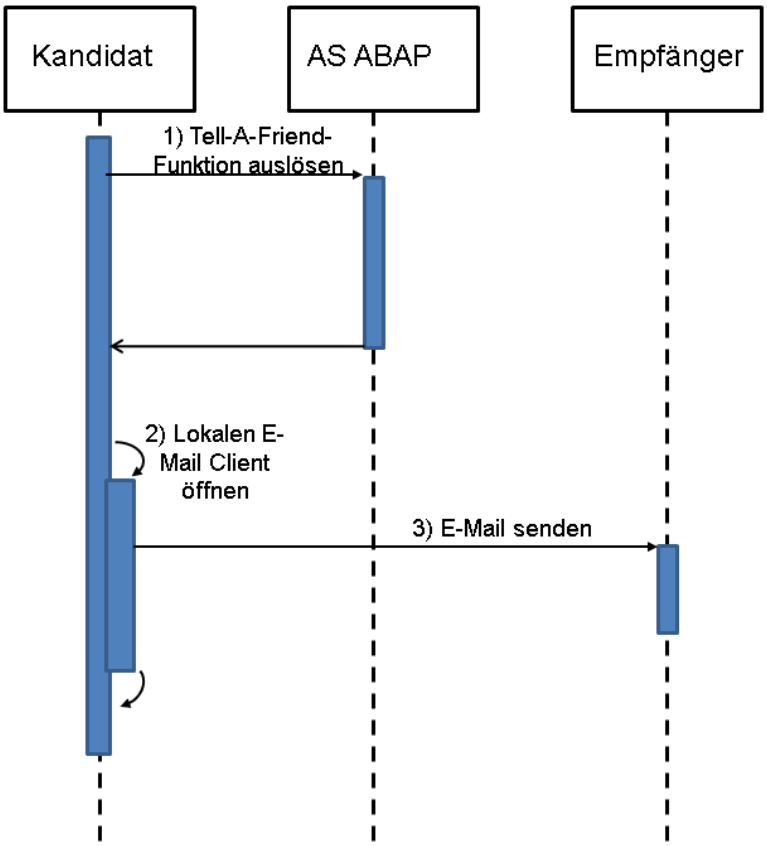
15.3.5.1.1.5 Recommendation of Job Posting (Tell a Friend)

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_METHODin 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* .



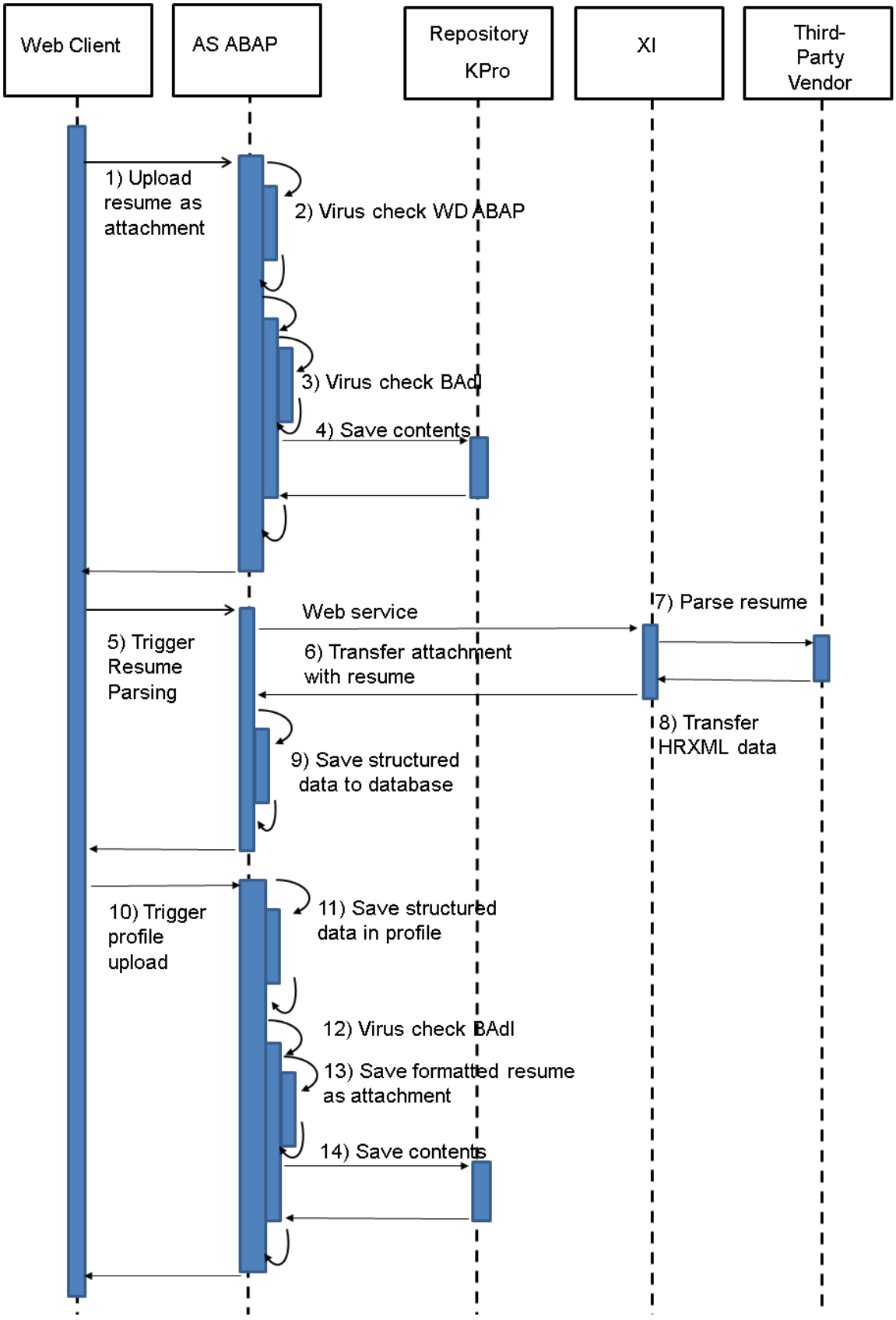
The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

Step	Name	Security Action
1	Trigger Tell a Friend function	Not relevant
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_METHODin the Customizing activity *Assign Values to Interface Parameters (Web Dynpro ABAP)* .
3	Send e-mail	Not relevant

15.3.5.1.1.6 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.

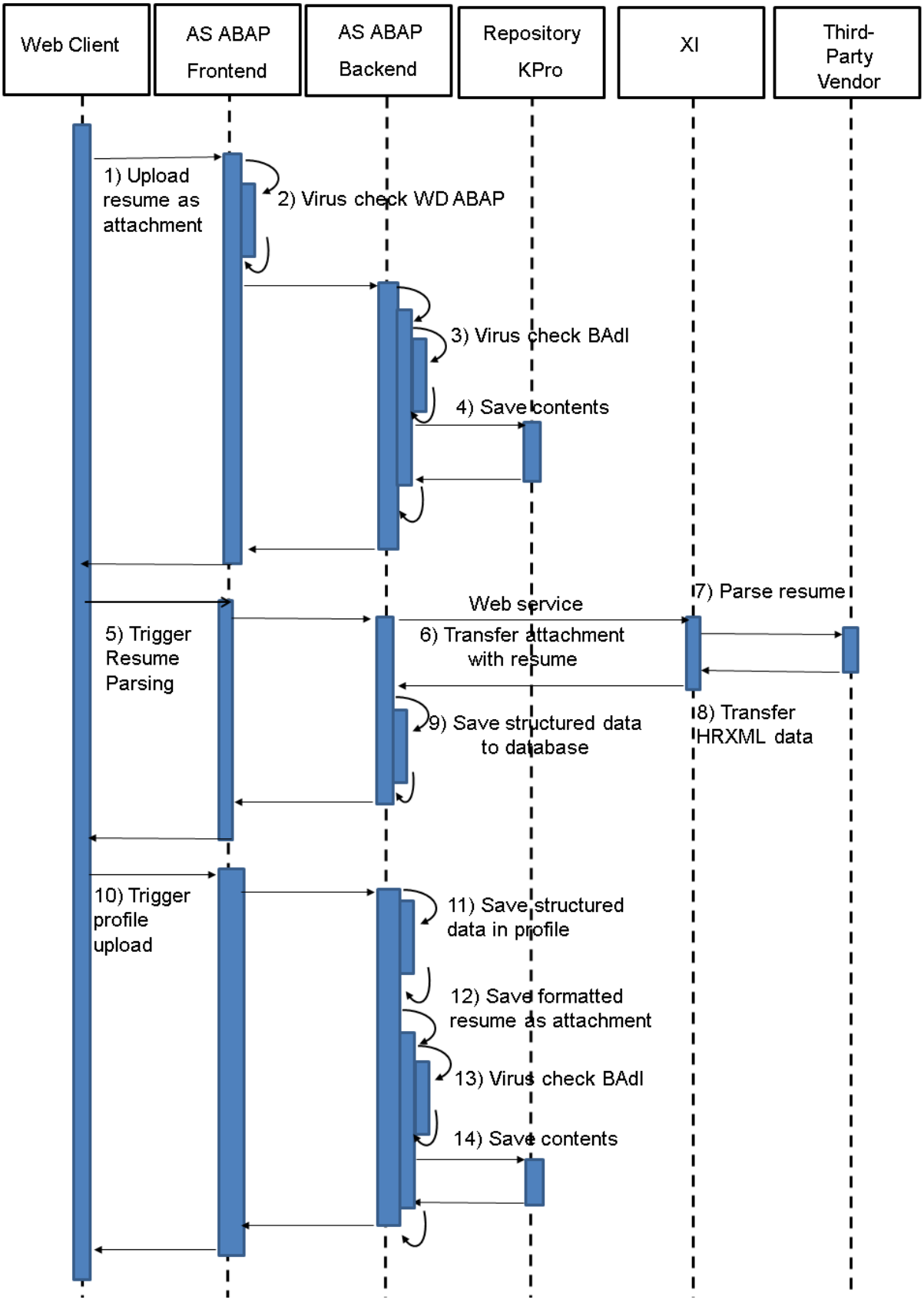

Web Client
AS ABAP
Repository
KPro
XI
Third-
Party
Vendor
1) Upload
resume as
attachment
2) Virus check WD ABAP
3) Virus check BAdI
4) Save contents
Web service
7) Parse resume
5) Trigger
Resume
Parsing
6) Transfer attachment
with resume
8) Transfer
HRXML data
9) Save structured
data to database
10) Trigger
profile
upload
11) Save structured
data in profile
12) Virus check BAdI
13) Save formatted resume
as attachment
14) Save contents

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	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 *http:service.sap.com/securityguide* → *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

15.3.5.1.1.7 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.


Web Client
AS ABAP Frontend
AS ABAP Backend
Repository KPro
XI
Third-Party Vendor
1) Upload resume as attachment
2) Virus check WD ABAP
3) Virus check BAdI
4) Save contents
5) Trigger Resume Parsing
Web service
6) Transfer attachment with resume
7) Parse resume
8) Transfer HRXML data
9) Save structured data to database
10) Trigger profile upload
11) Save structured data in profile
12) Save formatted resume as attachment
13) Virus check BAdI
14) Save contents

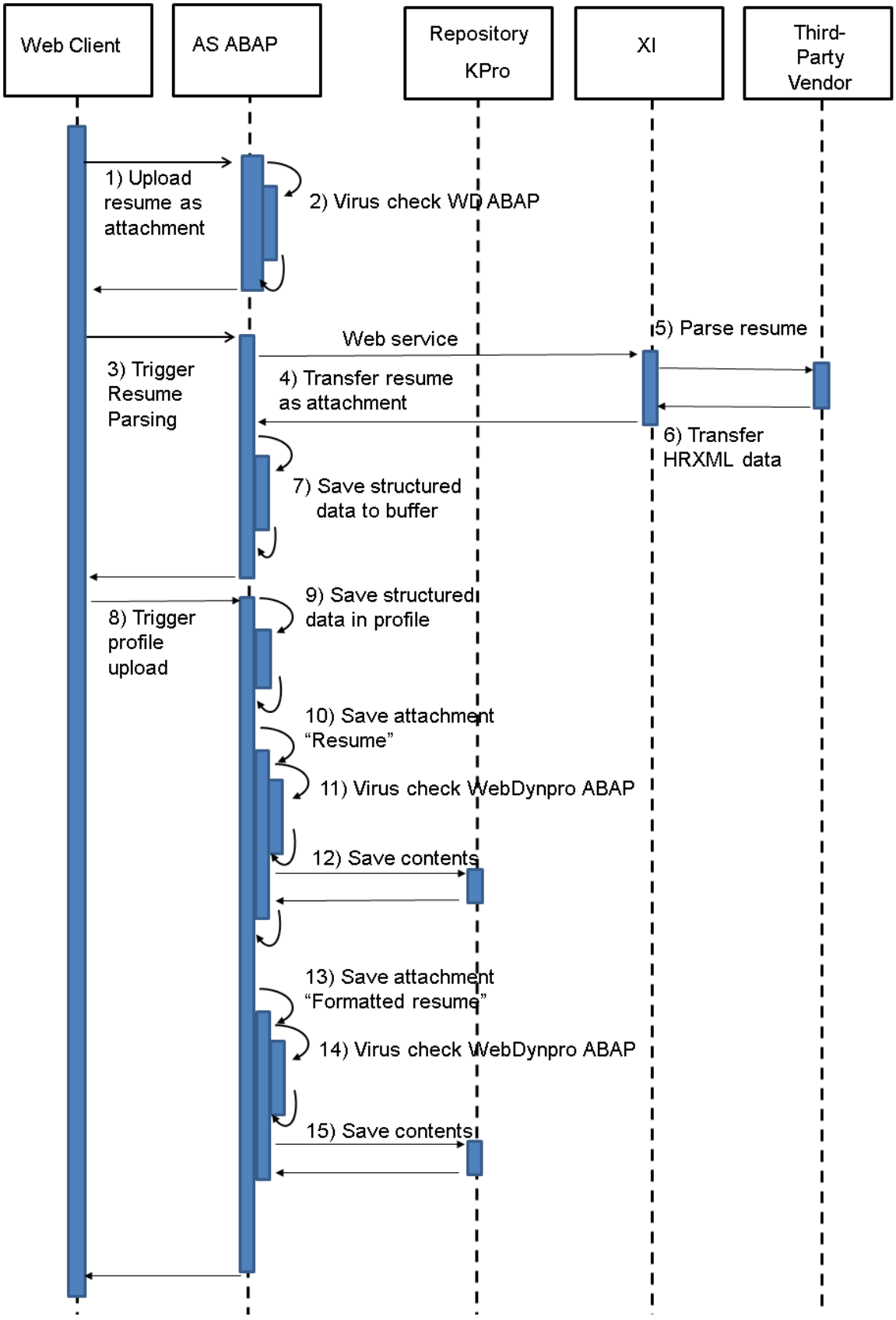
The table below lists the security aspect that has to be taken into account for the process step and the security action that is taken.

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	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 *http:service.sap.com/securityguide* → *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

15.3.5.1.1.8 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.

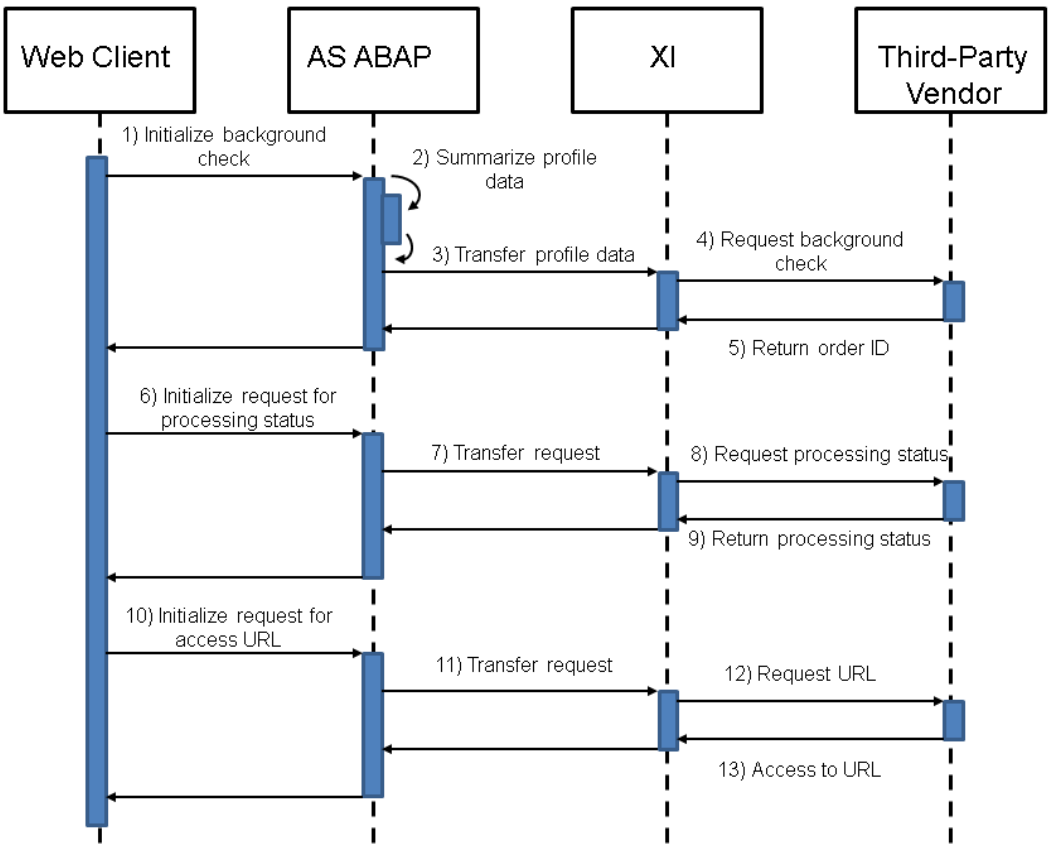

Web Client
AS ABAP
Repository
KPro
XI
Third-
Party
Vendor
1) Upload
resume as
attachment
2) Virus check WD ABAP
Web service
5) Parse resume
3) Trigger
Resume
Parsing
4) Transfer resume
as attachment
6) Transfer
HRXML data
7) Save structured
data to buffer
9) Save structured
data in profile
8) Trigger
profile
upload
10) Save attachment
“Resume”
11) Virus check WebDynpro ABAP
12) Save contents
13) Save attachment
“Formatted resume”
14) Virus check WebDynpro ABAP
15) Save contents

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 *http:service.sap.com/securityguide → 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

15.3.5.1.1.9 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
8	Request processing status	For XI-relevant security topics, see: SAP Process Integration Security Guide

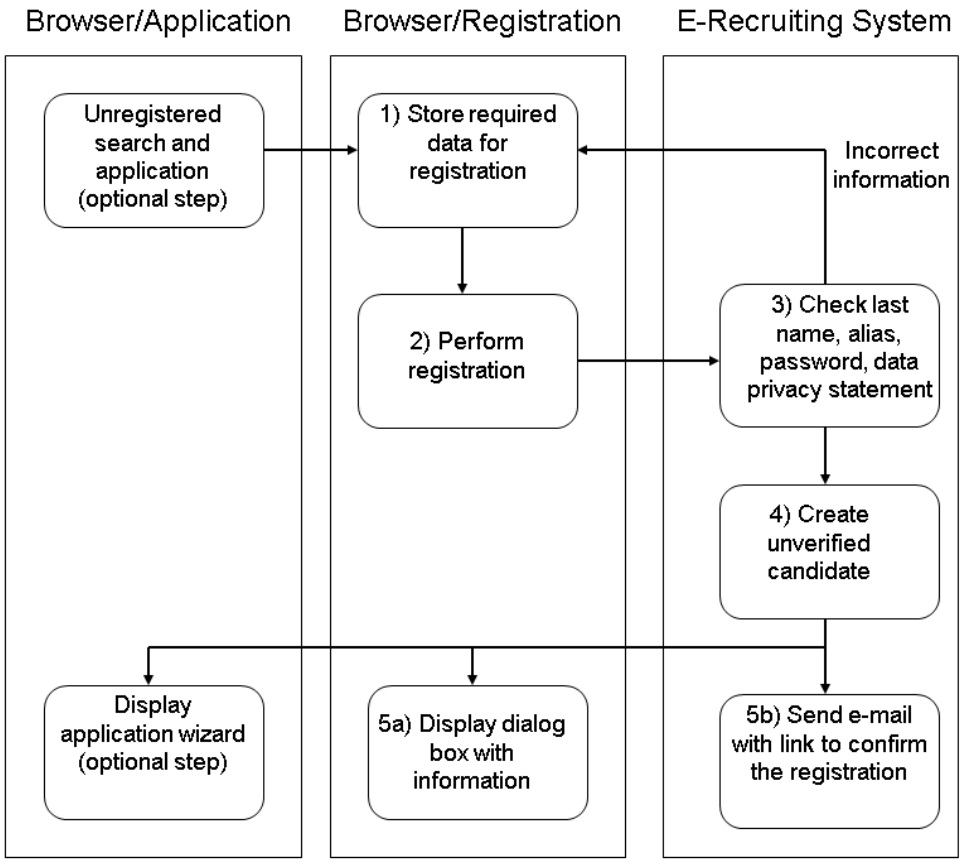
Step	Name	Security Measure
9	Return processing status	Not Relevant
10	Initialize request for access URL	Not Relevant
11	Transfer request	Not Relevant
12	Request URL	For XI-relevant security topics, see: SAP Process Integration Security Guide
13	Access to URL that the third-party vendor uses to display the report for the background check	Not Relevant

15.3.5.1.1.10 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 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 S/4HANA under *Human Resources* > *Talent Management* > *SAP E-Recruiting (PA-ER)* > *Candidate*.

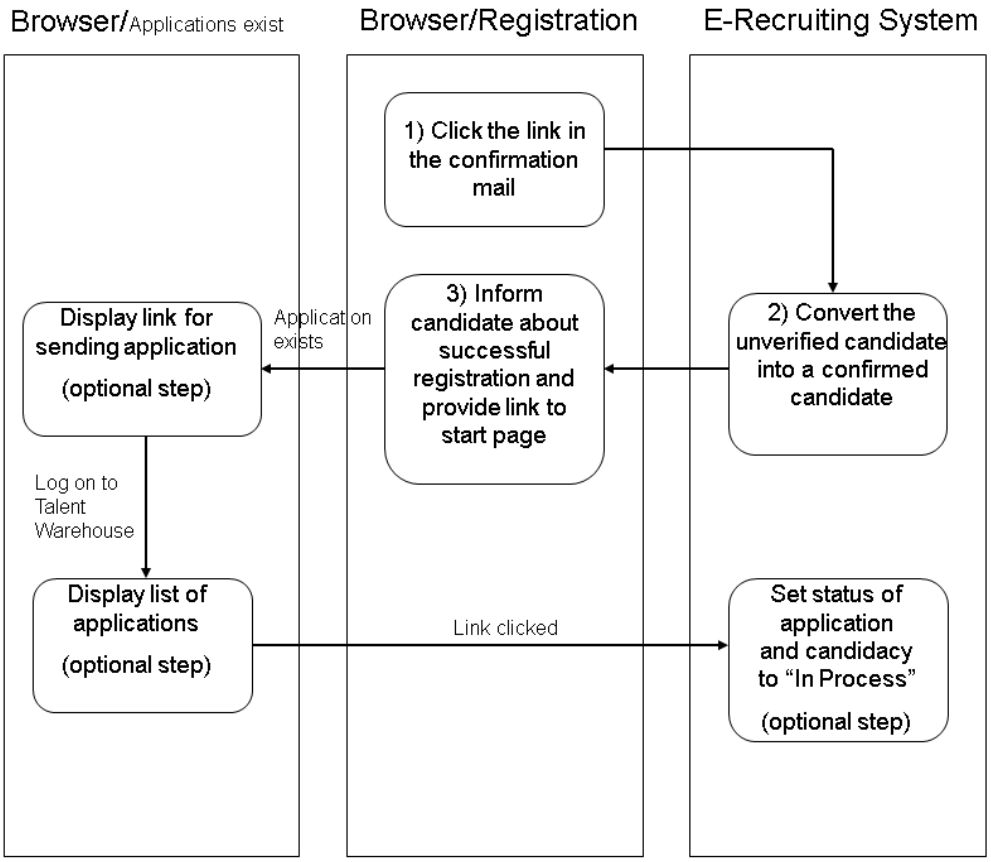
> **i Note**
>
> This process is relevant if the switch RECFA VERIF is set in the Customizing activity *Set System Parameters* .



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)* .
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 *Specify E-Recruiting Services (WebDynpro ABAP)* .
2	The unregistered candidate performs the registration.	

Step	Description	Security Action
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 *Candidate Overview* infotype (5102) in the *Status of E-Mail Verification* field, the system enters the value 1 (*Outstanding*). 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 *Determine Rules for Periodic Services* , 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.	In the Customizing activity *Determine Rules for Periodic Services* , you can specify the following (in addition to the validity period of the link for the confirmation): • 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 *Candidate Overview* infotype (5102) in the *Status of E-Mail Verification* field, the system enters the value 0 (*Confirmed*).
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 *In Process* .	Recruiters can now view the application and the candidate profile.

15.3.5.1.1.11 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.

15.3.5.1.1.12 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	ERCAdjEntry	-	-	-
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	ERCApprReqWD	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

15.3.5.1.2 User Administration and Authentication

SAP E-Recruiting uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server for ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server for ABAP 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.

15.3.5.1.2.1 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 S/4HANA Security Guide for Human Resources.

Standard Users

We do not deliver standard users within SAP E-Recruiting.

15.3.5.1.2.2 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.

15.3.5.1.3 Authorizations

SAP E-Recruiting uses the authorization concept provided by SAP NetWeaver AS for 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 SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on theSAP 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 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* .

15.3.5.1.3.1 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	*Internal Candidate (Server)* under *Roles (User Profiles)* 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 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	• 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.

15.3.5.1.3.2 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 **i Note** This role is obsolete and has been replaced with the role SAP _ERC_REC_ADMIN_CI_4.
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. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_REC_ADMIN_CI_4.
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. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_REC_ADMIN_CI_4.
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. **i Note** This role is obsolete and has been replaced with the role SAP _ RCF _ DATA _TYPIST_ERC_CI_4.
SAP _ RCF _ DATA _TYPIST_ERC_CI_4	Data Entry Clerk

Role	Description
SAP _ RCF _RECRUITER_ERC_CI_2	Recruiter (Obsolete) The role has access to the following data: • Candidate data: The data is displayed for all candidates who stored their data in the Talent Pool. • All publications • All requisition data • All application data • All data for the selection processes The role also contains the authorization for minimum data entry for incoming paper applications. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_RECRUITER_CI_4.
SAP _ RCF _RECRUITER_ERC_CI_4	Recruiter (NWBC) (Obsolete) 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 _RE-CRUITER_SR_ERC_CI_4 and SAP _ RCF _RE-CRUITER_ERC_CI_2. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_RECRUITER_CI_4.
SAP _ RCF _RECRUITER_SR_ERC_CI_4	Recruiter (NWBC) (Obsolete) This role contains the recruiter's menu for display based on SAP Business Client for HTML. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_RECRUITER_CI_4.
SAP _ERC_RECRUITER_CI_4	Recruiter

Role	Description
SAP _ RCF _ RES _RECRUITER_ERC_CI_2	Restricted Recruiter (Obsolete) 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). **i Note** This role is available only if you activate the business function HCM _ERC_CI_3. This role is obsolete and has been replaced with the role SAP _ERC_ RES _RECRUITER_CI_4.
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	Authorization object that specifies within SAP E-Recruiting which SAP E-Recruiting application a user can call. The authorization object is used for the recruiter's, administrator's, and data entry clerk's applications.
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: • 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	• 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	• POWL _APPID: ERC-WORKCENTER	Authorization object that specifies the authorizations for the Personal Object Worklist (POWL) iViews.

15.3.5.1.3.3 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	*Manager* This role is required so that managers can access SAP E-Recruiting from the Portal (*Manager Self Service*). The manager wants to fill the vacant jobs in his or her area. To do this, the manager creates requisitions with the status *In Process* that are then processed further by recruiters. The role has access to the following data: Candidate data: The manager can see only the candidate data that is assigned to requisitions for which the manager is responsible. Requisition data and data for selection processes: The manager can only see data for which he or she is responsible. The role also contains the authorization to respond to questionnaires about candidates that are assigned to the relevant requisitions.
SAP _RFC_MANAGER_SERVICE	Service user 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.

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.

15.3.5.1.3.4 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	Unregistered Candidate (Client) (Obsolete) 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). If you execute unregistered scenarios directly on the back-end system, you must also assign this role to the service user in the backend system. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_ UNR _ CAND _CLIENT_CI_4.
SAP _ERC_ UNR _ CAND _CLIENT_CI_4	Unregistered Candidate (Client)
SAP _ RCF _UNREG_CANDIDATE_SERVER	Unregistered Candidate (Server) 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).
SAP _ RCF _UNREGISTERED_CANDIDATE	(Unregistered) Candidate – Service User (Obsolete) 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. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_ UNR _CANDIDATE_CI_4.
SAP _ERC_ UNR _CANDIDATE_CI_4	Unregistered Candidate

Role	Description
SAP _ RCF _EXT_CANDIDATE_CLIENT	External Candidate (Client) (Obsolete) 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). **i Note** This role is obsolete and has been replaced with the role SAP _ERC_EXT_ CAND _CLIENT_CI_4.
SAP _ERC_EXT_ CAND _CLIENT_CI_4.	External Candidate (Client)
SAP _ RCF _EXT_CANDIDATE_SERVER	External Candidate (Server) 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).
SAP _ RCF _EXTERNAL_CANDIDATE	External Candidate (Obsolete) 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. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_EXT_CANDIDATE_CI_4.
SAP _ERC_EXT_CANDIDATE_CI_4	External Candidate
SAP _ RCF _ INT _CANDIDATE_CLIENT	Internal Candidate (Client) (Obsolete) 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). 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. **i Note** This role is obsolete and has been replaced with the role SAP _ERC_ INT _ CAND _CLIENT_CI_4.

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: • Requisition data • Posting data • Application data • Data for the selection process **i Note** This role is obsolete and has been replaced with the role SAP _ERC_ INT _ CAND _CLIENT_CI_4.
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). **i Note** This role is obsolete and has been replaced with the role SAP _ERC_ INT _ CAND _CLIENT_CI_4.

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	• 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 RFC_CLIENT RFC_EQUSER RFC_ INFO RCF _SYSID RCF _TCODE RCF _USER		Authorization check for RFC users (for example, *Trusted System*) (For more information, see the documentation for *Authorization Object S_RFCACL* .)
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 *Authorization Object S_ICF* .)  You can use the authorization object S_ICF to safeguard the use of RFC destinations and access to individual SICF services.

15.3.5.1.4 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.

15.3.5.1.5 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 SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver 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 SAP NetWeaver Security Guide:

- Network and Communication Security

- Security Aspects for Connectivity and Interoperability

15.3.5.1.5.1 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 Special Protection
Front-end client that uses SAP GUI for Windows for the application server	DIAG	All Customizing data	Passwords
Front-end client that uses a Web browser for the application server	HTTP, HTTPS  We generally recommend you use HTTPS.	All application data	Passwords, personal data

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 Transport Layer Security in the SAP NetWeaver Security Guide.

Print

SAP E-Recruiting has numerous options for printing contents. For information about security when printing, see *SNC User's Guide* under *http://service.sap.com/security* → *Security in Detail* → *Infrastructure Security* .

15.3.5.1.5.2 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 SAP NetWeaver 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 SAP NetWeaver Security Guides.

For other components, for example, SAPinst, SAProuter, or SAP Web Dispatcher, see also the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Service Marketplace at http://service.sap.com/ under *Products* > *Database & technology* > *Security* > *Infrastructure Security*.

15.3.5.1.5.3 Communication Destinations

The following sections provide an overview of the communication destinations that are relevant for the user in the SAP E-Recruiting roles.

15.3.5.1.5.3.1 Communication Destinations (Recruiter, Administrator, and Data Entry Clerk)

The following table provides an overview of the communication destinations that SAPE-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	User, Authorizations	Description
SAP E-Recruiting to SAP Human Resources Management	No	RFC	See Customizing	Customizing: *SAP E-Recruiting* > *Applicant Tracking* > *Activities* > *Set Up Data Transfer for New Employees*
From SAP Human Resources Management to SAP E-Recruiting	No	RFC	See Customizing	*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	*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.

15.3.5.1.5.3.2 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	User, 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_GRPS_ 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

15.3.5.1.5.3.3 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	User, Authorizations	Description
SAP E-Recruiting (front-end) to SAP E-Recruiting (backend)	No	RFC	See Customizing	*SAP E-Recruiting* > *Technical Settings* > *User Interfaces* > *Candidate* > *Frontend Candidate* > *Enter RFC Destination of Receiving Backend System* You enter the RFC destination as a value of the `RECFA UI2BL` parameter.
SAP E-Recruiting (backend) to SAP E-Recruiting (front-end)	No	RFC	See Customizing	*SAP E-Recruiting* > *Technical Settings* > *User Interfaces* > *Candidate* > *Backend Candidate* > *Specify System Parameters for Web Dynpro* You enter the RFC destination as a value of the `RECFA BL2UI` parameter.

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.

15.3.5.1.6 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

15.3.5.1.7 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 require any other databases in addition to this standard.

SAP E-Recruiting stores the data in the following locations:

Data	Location
Master Data	PD infotype tables
Attachments and user-defined texts	Knowledge Provider (KPro)
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.

15.3.5.1.8 Enterprise Services Security

The following chapters in the SAP NetWeaver 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

15.3.5.1.9 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. In this way, you can include external virus scanners to increase the security of your system.

You can use the Business Add-In (BAdI) 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 BAdI using the *BAdI: Upload Documents* Customizing activity.

Accessing Attachments using Microsoft Internet Explorer

You use *Microsoft Internet Explorer* and want to view attachments in the browser. *Microsoft Internet Explorer* checks the contents of the attachment to determine the file type and to display the attachment correctly (*MIME Type Sniffing*). Malicious files of an undesirable file type could therefore be displayed in the browser or cause damage in some other way. To avoid this potential threat to security, deselect *MIME Type Sniffing* in the security settings of *Microsoft Internet Explorer* .

15.3.5.1.10 Security-Relevant Logging and Tracing

Application Log

SAP E-Recruiting uses the logging and tracing mechanisms from SAP NetWeaver. 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 SAP NetWeaver 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*.

15.3.5.1.11 Services for Security Lifecycle Management

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 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 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.

Additional Information

For more information about these services, see:

- SAP EarlyWatch Alert: *http://service.sap.com/ewa*
- SAP Security Optimization Service / Security Notes Report: *http://service.sap.com/sos*
- Comprehensive list of SAP Security Notes: *http://service.sap.com/securitynotes*
- Configuration Validation: *http://service.sap.com/changecontrol*

- RunSAP Roadmap, including the Security and the Secure Operations Standard: *http://service.sap.com/runsap* (See the RunSAP chapters 2.6.3, 3.6.3, and 5.6.3.)

15.3.5.2 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.

15.3.5.2.1 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 mangers 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

For more information about the technical system landscape, see the sources listed in the table below.

Topic	Guide/Tool	Quick link to SAP Service Marketplace or SDN
Technical description of SAP ERP and basic components such as SAP NetWeaver	*Master Guide*	http://service.sap.com/instguides
High availability	*High Availability for SAP Solutions*	http://sdn.sap.com/irj/sdn/ha
Design of the technical landscape	See available documents	http://sdn.sap.com/irj/sdn/landscape-design
Security	See available documents	http://sdn.sap.com/irj/sdn/security

15.3.5.2.2 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 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 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).

15.3.5.2.3 Authorizations

Performance Management uses the authorization concept provided by SAP NetWeaver Application Server for ABAP (AS ABAP). Therefore, the security recommendations and guidelines for authorizations detailed in the SAP NetWeaver Security Guide ABAP also apply to Performance Management.

The SAP NetWeaver 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 SAP NetWeaver AS for 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 S/4HANA and choose *Human Resources* > *HR Tools* > *Authorizations for Human Resources*).

15.3.5.2.3.1 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

> **i 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.

15.3.5.2.3.2 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 structural authorizations, see SAP Library under *ERP Central Component* > *Human Resources* > *Personnel Management* > *Personnel Administration* > *Technical Processes in Personnel Administration* > *Authorizations for Human Resources*.

15.3.5.2.3.2.1 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*.

15.3.5.2.3.2.2 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*.

15.3.5.2.3.2.3 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 668]). 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*.

15.3.5.2.3.2.4 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 675]). 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.

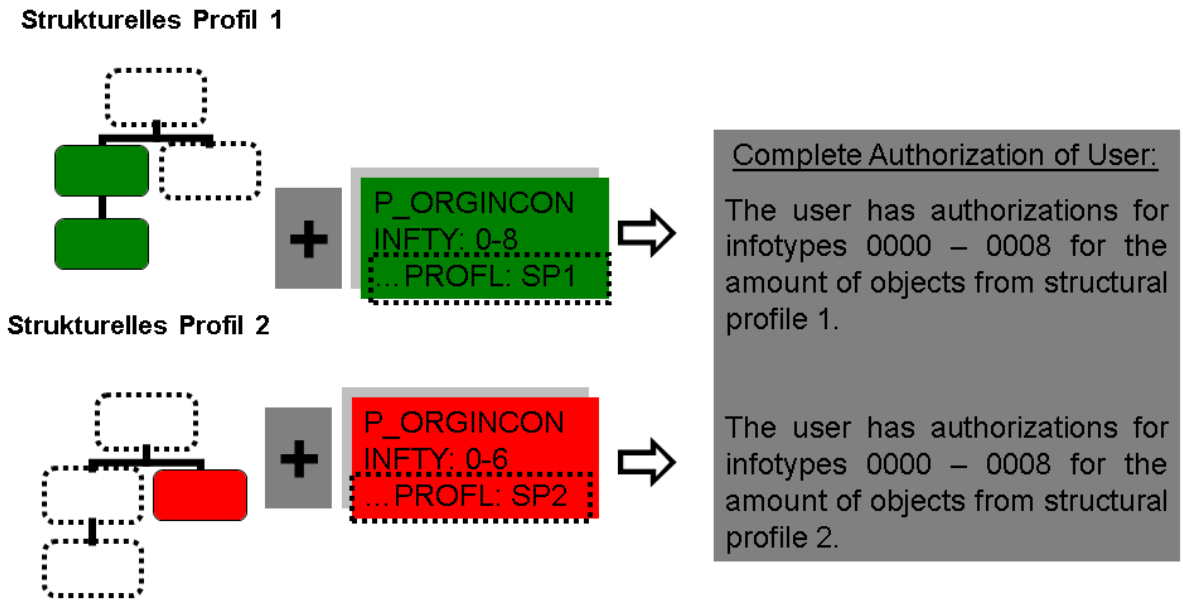
For more information on the authorizations, see the SAP Library under *ERP Central Component* > *Human Resources Management* > *Personnel Management* > *Personnel Administration* > *Technical Processes in Personnel Administration* > *Authorizations for Human Resources Management*.

15.3.5.2.3.2.5 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.



Example for context-sensitive authorization checks

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 (BAdI) HRBAS00_GET_PROFL, you do not need to maintain table T77UA manually. This BAdI 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*.

15.3.5.2.3.2.6 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*.

15.3.5.2.3.3 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*.

15.3.5.2.3.3.1 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 in 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:
>
> | | *Appraisal Template* Field | *Authorization Profile* Field |
> |---|---|---|
> | 1. Proficiency | Template A: Objective Setting Agreements | Structural Profile A: Area A |
> | 2. 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).

15.3.5.2.3.3.2 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 675]. 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 672] (see also Authorization Object P_HAP_DOC [page 669]).
- 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 672]), note that you must also consider the structural profiles from the authorization object P_HAP_DOC.

15.3.5.2.3.4 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

15.3.5.2.3.4.1 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 simulataneously.

- 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 sytem 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.

15.3.5.2.3.4.2 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 simulataneously 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.

15.3.5.2.3.4.3 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.

15.3.5.2.3.4.4 BSP-Specific Authorization Checks

For information about the authorizations for the BSP application, see SAP Note 616900.

15.3.5.2.3.4.5 BAdI for Authorization Checks

The BAdI HRHAP00_AUTHORITY is delivered for extended authorization checks and it can be used as a customer-specific implementation.

15.3.5.2.4 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 SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver 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 SAP NetWeaver Security Guide:

- Network and Communication Security
- Security Aspects for Connectivity and Interoperability

15.3.5.2.4.1 Communication Channel Security

The table below shows the communication paths used by Peformance 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	

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

Peformance Management provides the options for printing content. For information about security while printing, see the *SNC User's Guide*. You can find this at http://service.sap.com/security by looking under *Security in Detail* > *Infrastructure Security*.

15.3.5.2.4.2 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 SAP NetWeaver Security Guides. For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see also the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Service Marketplace at http://service.sap.com/ under *Products* > *Database & technology* > *Security* > *Infrastructure Security*.

15.3.5.2.5 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*.

15.3.5.2.6 Data Storage Security

HANA

The Performance Management data is saved to the databases of SAP Web Application Server (Web AS) or S/4HAN 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

15.3.5.2.7 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*.

15.3.5.2.8 Security-Relevant Logging and Tracing

Performance Management uses logging and tracing mechanisms from SAP NetWeaver 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.

15.3.5.3 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.

15.3.5.3.1 Authorizations

Use

Talent Management uses the following authorization concepts:

- SAP NetWeaver 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 `PFCG`) 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 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 *Employee in Talent Management* under *Single Roles in Talent Management*)	None

For the documentation for the standard roles, see SAP Library for 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 *Talent Management Specialist* under *Single Roles in Talent Management*)	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 *Talent Management Superuser* under *Obsolete Single Roles in Talent Management*)	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 *Manager in Talent Management* under *Single Roles in Talent Management*)	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 *Single Roles in Talent Management*)	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 SAP NetWeaver Application Server for ABAP under SAP Business Partner Secuirty

Authorization Object	Description	More Information
CA_POWL	Authorizations for the personal object worklist (POWL)	SAP Library for 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	SAP NetWeaver 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	SAP NetWeaver Library under *SAP NetWeaver by Key Capability* > *Application Platform by Key Capability* > *ArchiveLink* in the section Authorizations
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 S/4HANA under *PLOG (Personnel Planning)*
P_HAP_DOC	Authorization object that controls a user's access to appraisal templates	SAP Library for S/4HANA under *P_HAP_DOC (Appraisal Systems: Appraisal)*
P_ORGIN	Authorization object used to check the authorization for accessing HR infotypes	SAP Library for 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 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 S/4HAAN 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 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.

  > **i 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 `PLOG` 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*.

15.3.5.3.2 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 Path	Protocol Used	Type of Data Transferred	Data Requiring Special 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	

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.

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 Transport Layer Security in the SAP NetWeaver Security Guide.

15.3.5.3.3 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: • 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_SUCCESSIONS 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 ERP 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	*Transfer Successor Assignments to Talent Management* (RPTMC_MIGRATE_SUCCESSIONS)
HRSCP_MIGRATION	HRSCP_MIG_TG_GET_ALL	*Transfer Talent Groups from E-Recruiting to Talent Management* (RPTMC_MIGRATE_TALENT_GROUPS)
HRSCP_MIGRATION	HRSCP_MIG_TG_GET_DETAILS	*Transfer Talent Groups from E-Recruiting to Talent Management* (RPTMC_MIGRATE_TALENT_GROUPS)
HRSCP_MIGRATION	HRSCP_MIG_TG_GET_TALENTS	*Transfer Talent Groups from E-Recruiting to Talent Management* (RPTMC_MIGRATE_TALENT_GROUPS)
HRSCP_TP_SYNC	HRSCP_TP_SYNC_GET_EDU_WE_INFO	*Synchronization of Talent Profile with Candidate Profile* (RPTMC_TP_SYNC_EDU_WE_RCF)

15.3.5.3.4 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*.

15.3.5.3.5 Data Storage Security

Data Storage

The Talent Management data is stored in the SAP NetWeaver Application Server or 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.

15.3.5.3.6 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. The documentation is located on SAP Service Marketplace at http://service.sap.com/instguides ▶ *SAP Solution Extensions* ▶ *SAP Talent / Org Visualization by Nakisa* ▶.

15.3.5.3.7 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.

15.3.5.4 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.

15.3.5.4.1 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 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 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*.

15.3.5.4.2 Authorizations

Use

Enterprise Compensation Management uses the following authorization concepts:

- SAP NetWeaver 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 `PFCG`).
- 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 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 *S/4HANA Security Guide for Human Resources* > *Authorizations*.

15.3.5.4.3 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 **i Note** We generally recommend using HTTPS	All application data	Passwords, personal data
SAP Business Information Warehouse (SAP BW)	Extractor program	HR master data, organizational data, Enterprise Compensation 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

Enterprise Compesation Management provides a number of options for printing content. For information about security while printing, see the *SNC User's Guide*. You can find this at http://service.sap.com/security by looking under *Security in Detail* > *Infrastructure Security*.

15.3.5.4.4 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_SIDEBYSIDE_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 Secuirty Guide.

15.3.5.4.5 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, see the SAP NetWeaver Security Guide at https://help.sap.com/nw *Release/Language* > *SAP NetWeaver Library* > *Administrator's Guide* > *SAP NetWeaver Security Guide* > *Security Guides for the Operating System and Database Platforms* >.

15.3.5.4.6 Security-Relevant Logging and Tracing

Enterprise Compensation Management uses logging and tracing mechanisms from SAP NetWeaver. 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)

15.3.6 Time and Attendance Management

15.3.6.1 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.

15.3.6.1.1 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.

For a complete list of the available SAP security guides, see SAP Service Marketplace at **http://service.sap.com/securityguide**.

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	Comment
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 also SAP Service Marketplace at **http://service.sap.com/securitynotes**.

Additional Information

For more information about specific topics, see the Quick Links as shown in the table below.

Content	Quick Link on SAP Service Marketplace or SDN
Security	**http://sdn.sap.com/irj/sdn/security**
Security Guides	**http://service.sap.com/securityguide**
Related SAP Notes	**http://service.sap.com/notes** **http://service.sap.com/securitynotes**
Released platforms	**http://service.sap.com/pam**
Network security	**http://service.sap.com/securityguide**
SAP Solution Manager	**http://service.sap.com/solutionmanager**
SAP NetWeaver	**http://sdn.sap.com/irj/sdn/netweaver**

15.3.6.1.2 User Management

Use

User management in SAP Personnel Time 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 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 SAP NetWeaver AS for ABAP (Transactions SU01, PFCG)	For more information, see *User and Role Administration of AS ABAP*	

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.

15.3.6.1.3 Authorizations

Use

TheSAPPersonnel Time Management component uses the authorization concept provided bySAPNetWeaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in theSAPNetWeaver AS Security Guide ABAP also apply toSAPPersonnel Time Management.

TheSAPNetWeaver 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*

Role and Authorization Concept forSAPPersonnel Time Management

Standard Roles

The table below shows the standard roles that are used by theSAPPersonnel 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 theUSA

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used bySAPPersonnel Time Management.

Authorization Object	Field	Value	Description
P_PERNR	AUTHC	E, R	http://help.sap.com/erp2005_ehp_02/helpdata/en/35/26b181afab52b9e10000009b38f974/content.htmAuthorizationobject that is used to assign different authorizations to users for accessing their own personnel number. P_PERNR is relevant for Self-Service Scenarios (RoleSAP_EMPLOYEE)
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	http://help.sap.com/erp2005_ehp_02/helpdata/en/35/26b181afab52b9e10000009b38f974/content.htmAuthorizationobject that is 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

15.3.6.1.4 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:

`RPTEXTPT`: 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_RPTEDO00`	`RPTEDO00`	`HR_XX_DIR_RPTEDO00`
`HR_XX_DIR_RPTEUP00`	`RPTEUP00`	`HR_XX_DIR_RPTEUP00`

Logical File Name	Reports That Use These Logical File Names	Logical File Path
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

15.3.6.2 Cross-Application Time Sheet (CA-TS)

15.3.6.2.1 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 SAP NetWeaver Application Server for ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server for 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.

15.3.6.2.1.1 User Management

User management for the Cross-Application Time Sheet (CA-TS) 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 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).

15.3.6.2.1.2 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 SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Secuirty 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 in the SAP NetWeaver Library.

15.3.6.2.2 Authorizations

Use

The Cross-Application Time Sheet (CA-TS) uses the authorization concept provided by the SAP NetWeaver AS for ABAP and 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 to the Cross-Application Time Sheet (CA-TS).

The SAP NetWeaver 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.



For more information about how to create roles, see *Role Administration* .

The following section shows the typical scenarios, the relevant roles and the authorization objects thatCross-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_ESSUSER_ERP05	Employee Self-Service (WD JAVA): You need this role if you want to enable all your company's employees to record their working times.
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	http://help.sap.com/erp2005_ehp_02/helpdata/en/35/26b181afab52b9e10000009b38f974/content.htmAuthorizationobject that is 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

Authorization Object	Field	Value	Description
P_ORGIN	AUTHC	E, R	http://help.sap.com/erp2005_ehp_02/helpdata/en/35/26b181afab52b9e10000009b38f974/content.htmAuthorizationobject that is used during the authorization check for HR infotypes. P_ORGIN is relevant for Adminstrator 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 Adminstrator 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	The *Time Supervisor* 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. 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.

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	http://help.sap.com/erp2005_ehp_02/helpdata/en/35/26b181afab52b9e10000009b38f974/content.htmAuthorizationobject 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	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 *SAP Cross-Application Time Sheet*.

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	

15.3.6.2.3 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.

15.3.6.2.4 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 SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver 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 SAP NetWeaver Security Guide:

- Network and Communication Security
- Security Guides for Connectivity and Interoperability Technologies

15.3.6.2.4.1 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 SAP NetWeaver Security Guide.

15.3.6.2.4.2 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 SAP NetWeaver 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 SAP NetWeaver Security Guides.

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, also see the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Service Marketplace at http://service.sap.com/ under *Products* > *Database & technology* > *Security* > *Infrastructure Security*.

15.3.6.2.4.3 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	Anonympus dialog user specified in connections between both systems	Customizing: *Time Sheet → Settings for All User Interfaces → Data Transfer for Distributed Systems (ALE)*
Cross-Application Time Sheet (CA-TS) to cProjects	No	RFC	Anonympus dialog user specified in connections between both systems	Customizing: *Time Sheet → Settings for All User Interfaces → Data Transfer for Distributed Systems (ALE)*

Destination	Delivered	Type	User, Authorizations	Description
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.

15.3.6.2.5 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

15.3.6.2.6 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 NetWeaver Process Integration Security Guide*

15.3.6.2.7 Security-Relevant Logging and Tracing

Cross-Application Time Sheet (CA-TS) relies on the logging and tracing mechanisms from SAP NetWeaver:

- Auditing and Logging
- Tracing and Logging

15.3.6.2.8 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: `http://service.sap.com/ewa`
- Security Optimization Service / Security Notes Report: `http://service.sap.com/sos`
- Comprehensive list of Security Notes: `http://service.sap.com/securitynotes`
- Configuration Validation: `http://service.sap.com/changecontrol`
- RunSAP Roadmap, including the Security and the Secure Operations Standard: `http://service.sap.com/runsap` (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)

15.4 Industries

15.4.1 Engineering, Construction, and Operations

15.4.1.1 Equipment and Tools Management

15.4.1.1.1 Authorizations

Equipment and Tools Management (ETM) uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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
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_3GDBER	Planning Area in Recipient
J_3G_TCODE	Transaction Code

15.4.1.1.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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

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*.

15.5 Service

15.5.1 Warranty Management

15.5.1.1 Authorizations

Warranty (LO-WTY) uses the authorization concept provided by the SAP NetWeaver AS for ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply.

The SAP NetWeaver 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 NetWeaver 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

15.5.1.2 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 http://help.sap.com/s4hana_op_1610_001 ▶ *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*.

16 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.

16.1 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.

16.2 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, search for "The SAP Cryptographic Library Installation Package" in the documentation of SAP NetWeaver at http://help.sap.com/nw.

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, search for the phrase *Using the ICM Monitor* in the documentation of SAP NetWeaver at help.sap.com.
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.

   > **i** 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*. Choose *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.

16.3 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.

16.4 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.

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.

16.5 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.

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 a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

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

Example Code

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

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

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.

www.sap.com/contactsap

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

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

THE BEST RUN SAP