



PUBLIC  
2015-11-10

# Security Guide for SAP S/4HANA, on-premise edition 1511

# Content

- 1 Introduction. . . . . 6**
- 2 Before You Start. . . . . 7**
- 3 SAP S/4HANA, on-premise edition System Landscape Information. . . . . 8**
- 4 User Administration and Authentication. . . . . 10**
  - 4.1 User Management. . . . . 10
    - Non-SAP Fiori Technology. . . . . 10
    - SAP Fiori Technology. . . . . 12
  - 4.2 User Data Synchronization. . . . . 12
  - 4.3 Integration into Single Sign-On Environments. . . . . 12
- 5 Network and Communication Security. . . . . 14**
  - 5.1 Communication Channel Security. . . . . 14
  - 5.2 Network Security. . . . . 15
  - 5.3 Communication Destinations. . . . . 15
- 6 ICF Security. . . . . 16**
- 7 Data Storage Security . . . . . 17**
- 8 Virus Scanning. . . . . 18**
  - 8.1 Virus Scanning in File Uploads. . . . . 18
  - 8.2 General Recommendations for Virus Scan Profiles. . . . . 19
  - 8.3 Further Protection Against Active Content. . . . . 21
- 9 Session Security Protection. . . . . 22**
- 10 Additional System Hardening Activities. . . . . 23**
- 11 Data Protection. . . . . 25**
- 12 SAP S/4HANA Cross Application Infrastructure. . . . . 26**
  - 12.1 Data Security in SAP ILM. . . . . 26
    - Data Security in SAP ILM System Connections. . . . . 26
    - Users and Authorizations in SAP ILM. . . . . 27
    - Security of Stored Data in SAP ILM. . . . . 28
    - Logs in SAP ILM. . . . . 29
- 13 SAP S/4HANA Enterprise Management. . . . . 31**

13.1	Asset Management. . . . .	31
	Maintenance Operations. . . . .	31
13.2	Financial Accounting. . . . .	32
	Authorizations in Financial Accounting. . . . .	33
	General Ledger Accounting (FI-GL). . . . .	34
	Closing Cockpit. . . . .	40
	Accounts Payable Accounting (FI-AP). . . . .	43
	Accounts Receivable Accounting (FI-AR). . . . .	48
	Bank Accounting (FI-BL). . . . .	53
	Asset Accounting (FI-AA). . . . .	56
	Special Purpose Ledger (FI-SL). . . . .	58
13.3	Controlling. . . . .	60
	Authorizations. . . . .	60
	Profit Center Accounting (EC-PCA) . . . . .	92
	Network and Communication Security . . . . .	93
13.4	Master Data Framework . . . . .	94
	Technical System Landscape . . . . .	94
	Authorizations. . . . .	95
	Communication Channel Security . . . . .	95
13.5	Joint Venture Accounting . . . . .	96
	Authorizations . . . . .	96
	Communication Channel Security. . . . .	96
13.6	Manufacturing. . . . .	97
	Authorizations in Manufacturing. . . . .	97
	Production Engineering. . . . .	104
	Production Planning. . . . .	110
	Production Orchestration and Execution. . . . .	115
	Quality Management. . . . .	128
	Maintenance Operations. . . . .	135
13.7	R&D / Engineering. . . . .	136
	Product Safety and Stewardship. . . . .	136
13.8	Sales. . . . .	139
	Authorizations. . . . .	139
	Communication Channel Security. . . . .	141
	Deletion of Personal Data in Sales. . . . .	142
13.9	Sourcing and Procurement. . . . .	144
	Authorizations. . . . .	144
	Data Storage Security. . . . .	151
	Other Security-Relevant Information. . . . .	153
	Supplier Information and Master Data. . . . .	155
	Supply Chain. . . . .	160

13.10	Enterprise Technology. . . . .	167
	Middleware. . . . .	167
<b>14</b>	<b>SAP S/4HANA LoB Products for specific Industries. . . . .</b>	<b>206</b>
14.1	Automotive. . . . .	206
	Vehicle processes for Wholesale and Retail. . . . .	206
14.2	Banking. . . . .	207
	SAP Financial Customer Information Management (FS-BP). . . . .	207
	Bank Customer Accounts (BCA). . . . .	208
	Loans Management (FS-CML). . . . .	210
	Collateral Management (CM). . . . .	215
	Reserve for Bad Debt (FS-RBD). . . . .	218
14.3	Public Sector. . . . .	225
	Finance. . . . .	225
14.4	Utilities. . . . .	231
	Authorizations. . . . .	231
	Data Storage Security. . . . .	236
	Enterprise Services Security. . . . .	237
<b>15</b>	<b>SAP S/4HANA LOB Products. . . . .</b>	<b>238</b>
15.1	Asset Management. . . . .	238
	Maintenance Operations. . . . .	238
	Environment, Health and Safety. . . . .	239
15.2	Commerce. . . . .	259
	Commerce Management. . . . .	259
15.3	Finance. . . . .	263
	Treasury and Financial Risk Management. . . . .	263
	Financial Operations. . . . .	305
	Contract Accounting. . . . .	334
15.4	Manufacturing. . . . .	338
	Maintenance Operations. . . . .	338
<b>16</b>	<b>SAP S/4HANA Compatibility Packs. . . . .</b>	<b>340</b>
16.1	Finance. . . . .	340
	Travel Management. . . . .	340
	Real Estate Management. . . . .	343
16.2	R&D / Engineering. . . . .	344
	Product Safety and Stewardship. . . . .	344

# Document History

Version	Date	Description
1.0	November 10, 2015	Initial Version

# 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, on-premise edition.

To assist you in securing SAP S/4HANA, on-premise edition, 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, on-premise edition 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, on-premise edition is based on SAP NetWeaver and the SAP HANA Platform. With respect to Fiori Apps SAP Gateway plays a fundamental role. This means that the corresponding Security Guides are also applicable for SAP S/4HANA, on-premise edition. 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.

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

### Important SAP Notes

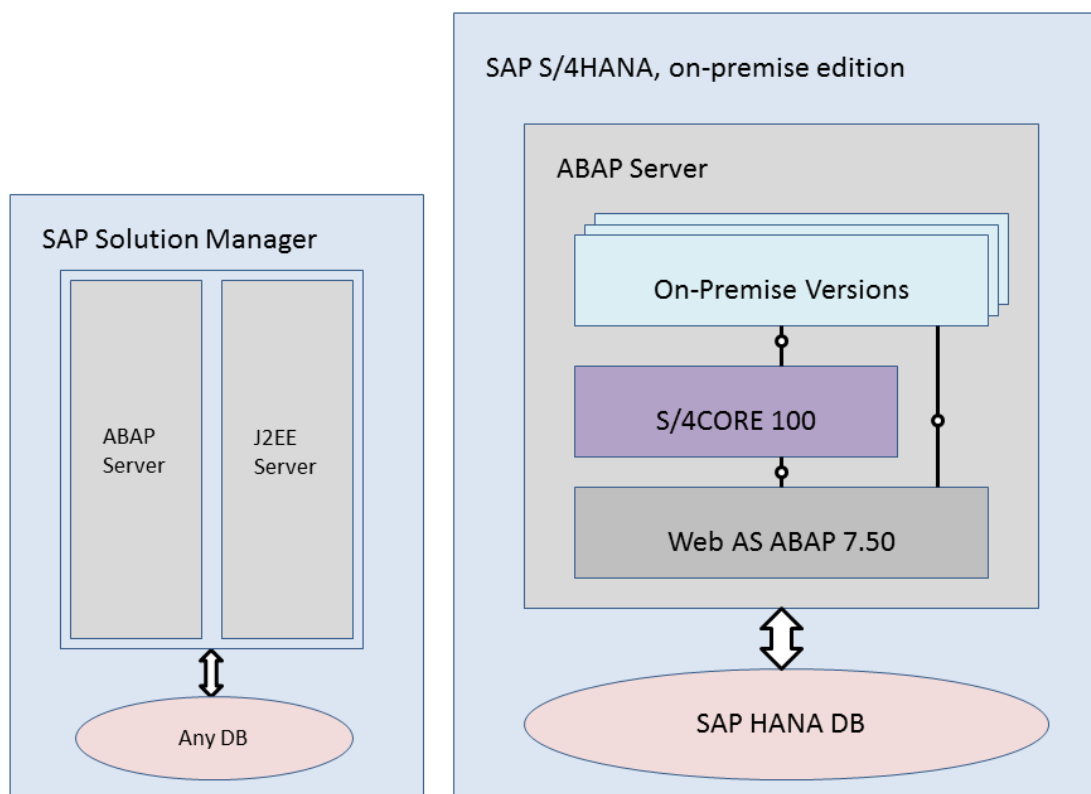
SAP Note [1538539](#) contains information about saving temporary files when using Adobe Acrobat Reader in SAP applications. SAP Note [138498](#) contains information on single sign-on solutions. SAP Notes relating to security for the subcomponents of SAP S/4HANA, on-premise edition are referenced in 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, on-premise edition System Landscape Information

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

#### Example: SAP S/4HANA, on-premise edition New Installation

A new installation of SAP S/4HANA, on-premise edition 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.





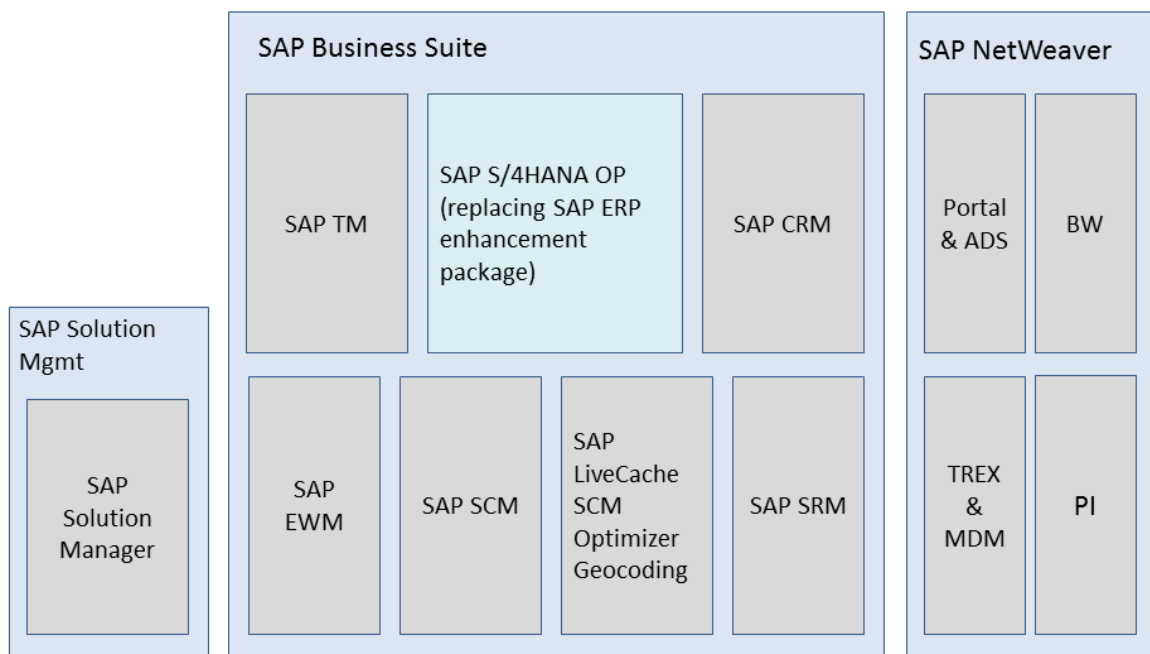
Simple SAP S/4HANA Deployment



## Example: SAP S/4HANA, on-premise edition in an SAP Business Suite Landscape

It is possible to integrate SAP S/4HANA, on-premise edition into an existing SAP Business Suite landscape by replacing the SAP ERP enhancement package product with the SAP S/4HANA, on-premise edition. When performing this conversion in your system landscape, you need to do some adaptations, for example you need convert your existing business processes to the simplified SAP S/4HANA, on-premise edition 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, on-premise edition processes is described in the *Simplification List*.

For more information about the *Simplification List*, see the *SAP S/4HANA, on-premise edition Conversion Guide* at the SAP Help Portal under [http://help.sap.com/s4hana\\_op\\_1511](http://help.sap.com/s4hana_op_1511)  [Product Documentation](#) .



Example SAP Business Suite landscape with an embedded SAP S/4HANA, on-premise edition 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, on-premise edition 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, on-premise edition 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, on-premise edition.

### 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 <a href="#">User and Role Administration of Application Server ABAP</a> at <a href="http://help.sap.com">help.sap.com</a> ► <a href="#">Enterprise Management</a> ► <a href="#">SAP ERP</a> ► <a href="#">SAP ERP 6.0 EHP7</a> ► <a href="#">SAP ERP Security Guide</a> ► <a href="#">SAP ERP Central Component Security Guide</a> ► <a href="#">User Administration and Authentication</a> ► <a href="#">User Administration</a> ►.
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, on-premise edition

- 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	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	See SAP NetWeaver Security Guide	Optional	SAP NetWeaver Security Guide
SAP ECC	SAP Users	Dialog users	Mandatory	The number of users depends on the area of operation and the business data to be processed

## 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\\_1511](http://help.sap.com/s4hana_op_1511)  *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, on-premise edition 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, on-premise edition 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>  **SAP NetWeaver Security Guide** > **Security Guides for SAP NetWeaver Functional Units** > **Security Guides for the Application Server** > **Security Guides for AS ABAP** > **SAP NetWeaver Application Server for ABAP Security Guide** .
- **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>  **SAP NetWeaver 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\\_1511](http://help.sap.com/s4hana_op_1511)  **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, on-premise edition 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 dividing the system into groups, placing the groups in different network segments, and then protecting each segment from unauthorized access by a firewall.

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

### Ports

SAP S/4HANA is executed in 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 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.

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

For details, 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 info can be found in the RFC/ICF Security Guide at [http://help.sap.com/s4hana\\_op\\_1511](http://help.sap.com/s4hana_op_1511) under [▶ SAP NetWeaver for SAP S/4HANA, on-premise edition ▶ 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.



# 7 Data Storage 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 `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.

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

For more information, see the following:

- [Logical File Names](#) 
- [Protecting Access to the File System](#) 
- [Security Audit Logs](#) 

# 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 <https://help.sap.com/nw75>  [Application Help](#)  [SAP NetWeaver Library: Function-Oriented View](#)  [Application Server](#)  [Application Server Infrastructure](#)  [Components of SAP NetWeaver Application Server](#)  [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 Session Security Protection

## Secure Session Management

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

## Session Security Protection on the AS ABAP

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

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

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

These additional flags are configured through the following profile parameters:

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

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










# 10 Additional System Hardening Activities

## Click-Jacking Protection

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

SAP S/4HANA, on-premise edition 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, see the SAP NetWeaver documentation at: <https://help.sap.com/nw75>   [SAP NetWeaver Security Guide](#)  [Security Guides for SAP NetWeaver Functional Units](#)  [Security Guides for the Application Server](#)  [Security Guides for AS ABAP](#)  [SAP NetWeaver Application Server for ABAP Security Guide](#)  [Special Topics](#)  [Using a Whitelist for Clickjacking Framing Protection](#) .









Webdynpro, WebGUI, and non-Fiori UI5-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 see the SAP NetWeaver documentation at: <https://help.sap.com/nw75>   [Security Guide](#)  [English](#)  [RFC/ICF Security Guide](#)  [RFC Scenarios](#)  [Security Measures –Overview \(RFC\)](#)  [Unified Connectivity](#) .

## Scenario-Based Authorization Checks

The Scenario-Based Authorizations Framework 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 customizing object, which can be transferred through your landscape.


By default, all 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, see the SAP NetWeaver documentation at: <https://help.sap.com/nw75>  [Security Guide](#)  [English](#)  [User Administration and Authentication](#)  [User Management](#)  [Identity Management](#)  [User and Role Administration of Application Server ABAP](#)  [Configuration of User and Role Administration](#)  [Customizing Scenario-Based Authorizations](#) .

## 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`.

For 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 it switched off using transaction `SE97`. This improves the security level because clearly all roles need to contain appropriate authorizations.

Installations that are migrated from an SAP ERP enhancement package to SAP S/4HANA may feature an extended adoption of roles. You can avoid this by setting `auth/check/calltransaction=2`. This keeps the check behavior as it was before.

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



# 11 Data Protection

## Use

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

This section and any other sections in this Security Guide do not give any advice on features to best support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

### i Note

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

SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data.

SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

## Glossary

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Business purpose	A legal, contractual, or in other form justified reason for the processing of <b>personal data</b> . The assumption is that any purpose has an end that is usually already defined when the purpose starts.

# 12 SAP S/4HANA Cross Application Infrastructure

## 12.1 Data Security in SAP ILM

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

For more information refer to the following topics in the security guide:

Data Security in SAP NetWeaver ILM System Connections in the Security guide.

Users and Authorizations in SAP NetWeaver ILM

Security of Stored Data in SAP NetWeaver ILM

Logs in SAP NetWeaver ILM

### 12.1.1 Data Security in SAP ILM System Connections

#### System Landscape Components

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

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

#### Data Security for System Connections

Communication between systems takes 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.

## **12.1.2 Users and Authorizations in SAP ILM**

### **User**

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

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

### **Authorizations**

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

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

Assigning Authorizations for Retention Management Cockpit

Assigning Authorizations for Retention Warehouse Cockpit

Transactions and Authorizations in SAP NetWeaver ILM

## 12.1.3 Security of Stored Data in SAP ILM

### Security of Archived Data in the File System

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

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

For more information, see:

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

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

### Security of Data in the ILM Store

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

### Metadata Security in the Store Hierarchy

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

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

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

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

## Backup of Complete Data in the Retention Warehouse System

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

### 12.1.4 Logs in SAP ILM

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

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

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

# 13 SAP S/4HANA Enterprise Management

## 13.1 Asset Management

### 13.1.1 Maintenance Operations

#### 13.1.1.1 Authorizations in Plant Maintenance

Plant Maintenance 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 `PF03`) 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
<code>SAP_COCKPIT_EAMS_MAINT_WORKER2</code>	<i>Maintenance Worker 2</i>  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	<p><i>Generic EAM Functions 2</i></p> <p>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.</p>

## 13.2 Financial Accounting

### Network and Communication Security

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

- Application Link Enabling(ALE)/IDoc
- Standard interfaces to BI, CRM, and SRM systems
- Batch-Input
 

Ensure that no unauthorized access can take place at the time of data transfer using encryption and with the help of your network.
- Remote Function Call(RFC) / Business Application Programming Interface (BAPI)
- File Interface
 

Ensure that no unauthorized access can take place at the time of data transfer using encryption and with the help of your network.
- SAP Process Integration (PI)
- E-mail, fax

#### ❁ Example

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

### Communication Destinations

All the technical users generally available can be used.



## Data Storage Security

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

### 13.2.1 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

## 13.2.2 General Ledger Accounting (FI-GL)

### 13.2.2.1 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_TO11	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_TO11_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

## 13.2.2.2 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\_OX**
  - Programs using this logical file name:
    - RFBISA00
    - RFBISA01
    - RFBISA51
  - Parameter used in this context:
    - <PARAM\_1> *Program Name*
- **FI\_INFOSYS\_TRANSPORT**
  - Programs using this logical file name:
    - RGRJTE00
    - RGRLTE00
    - RGRMTE00
    - RGR RTE00
    - RGRSTE00
    - RGRVTE00
    - RGRXTE00
    - RGSSTE00
    - RGSVTE00
    - RGRJT100
    - RGRMT100
    - RGSST100
    - RGSVT100
  - Parameter used in this context:
    - <PARAM\_1> Program name
- **FI\_VALUATION**

- Programs using this logical file name:
  - FAGL\_FCV
  - FAGL\_FC\_VALUATION
  - SAPF100
- Parameters used in this context:
  - <PARAM\_1> *Program name*
  - <PARAM\_2> Key date (from the selection screen)
  - <PARAM\_3> Valuation area (from the selection screen) for FAGL\_FCV and FAGL\_FC\_VALUATION valuation method (from the selection screen) for SAPF100

### Logical Path Names

The logical file names listed above all use the logical file path **FI\_ROOT**.

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

### Logical File Names

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

- **FI\_EXTERNAL**

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

Program	<PARAM_1>	<PARAM_2>	<PARAM_3>
RFAWVZ58	Program name (SY-REPID)	String 'AWV'	Parameter 'Key Date'
RFAWVZ5A	Program name (SY-REPID)	String 'AWV'	Parameter 'Key Date'
RFAWVZ5P	Program name (SY-REPID)	String 'AWV'	
RFAWVZ5A_NACC	Program name (SY-REPID)	String 'AWV'	Parameter 'Key Date'
RFAWVZ5P_NACC	Program name (SY-REPID)	String 'AWV'	
RFBIDETO	Program name (SY-REPID)	Parameter 'Client'	
RFBIKRTO	Program name (SY-REPID)	Parameter 'Client'	
RFFROE84	Program name (SY-REPID)	Parameter 'Customers/ vendors'	Parameter 'Key Date'
RFFRDDEO	Program name (SY-REPID)	Parameter 'Company Code'	Parameter 'Type'
RFFRLIST	Program name (SY-REPID)		
RFFRMOD1	Program name (SY-REPID)		

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'
RFSBLIWO	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 'Report- ing Quarter'	Parameter 'Reporting Quar- ter'
RFASLD11	Program name (SY-REPID)	Parameter year for 'Report- ing Quarter'	Parameter 'Reporting Quar- ter'
RFASLD11B	Program name (SY-REPID)	Parameter year for 'Report- ing Quarter'	Parameter 'Reporting Quar- ter'
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 Respon- sible'	See note 1
RFUSVS14	Program name (SY-REPID)	Concatenated parameters <Company Code>_<Year>	See note 1
RFUVPT00	Program name (SY-REPID)	Parameter 'Company Code'	See note 2

Notes:

- Note 1
  - If the file specified in the parameter "File for Leasing" is accessed, PARAM\_3 contains the value READ; consequently, the file content is read only and added to the output file.
  - If the file specified in the parameter "UNIX File for Output" is accessed, PARAM\_3 contains the value "WRITE".
- Note 2
  - If the file listed in the parameter "File Name - Application Server" on the "Periodic File O" tab page is accessed, PARAM\_3 contains the string PERIOD\_WRITE.
  - If the file listed in the parameter "ECSL File Name (AS)" on the "Periodic File O" tab page is accessed, PARAM\_3 contains the string PERIOD\_READ.
  - If the file listed in the parameter "XML File App. OP" on the "Annual File O/P" tab page is accessed, PARAM\_3 contains the string YEAR\_READ.
  - If the file listed in the parameter "File Name - Application Server" on the "Annual File O/P" tab page is accessed, PARAM\_3 contains the string YEAR\_WRITE.

- **FI\_RFASLD12\_FILE**

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

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

### Logical Path Names

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

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

## 13.2.3 Closing Cockpit



## 13.2.3.1 Authorizations

### Standard Roles

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

Standard Roles of the Closing Cockpit

Standard Role	Description
SAP_AIO_AP_CLERK-K	AP Supervisor
SAP_AIO_AR_CLERK-K	AR Supervisor
SAP_AIO_COSTACC-K	Central Cost Accountant
SAP_AIO_FINACC-K	Account Manager
SAP_AIO_FINACC-S	Assets Accountant
SAP_EP_RW_FDMN	AC - FI - Customers
SAP_EP_RW_FKMN	AC - FI - Vendors
SAP_EP_RW_FSMN_4	AC - General Ledger - Closing
SAP_EP_RW_FSMN_NEW4	AC - General Ledger (New) - Closing

Roles in the Closing Cockpit for the Connection to SAP Central Process Scheduling

#### **i** Note

You need the following roles only if you connect the Closing Cockpit to *SAP Central Process Scheduling* (CPS).

Role	Description
SAP_BC_BATCH_ADMIN_REDWOOD	Redwood Scheduler: Add-on for Batch Administrators
SAP_BC_REDWOOD_COMMUNICATION	Role for Redwood Job Scheduling, Communications Users
SAP_BC_REDWOOD_COMM_EXT_SDL	Additional Role for Redwood Communications Users

### Standard Authorization Objects

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

Authorization Objects of the Closing Cockpit

Authorization Object	Description
B_SMAN_WPL	Schedule Manager: Authorizations for Task Lists
S_TCODE	Transaction Code Check for Transaction Start
F_CLOCO	Authorizations for Closing Cockpit
S_BTCH_EXT	External Scheduler (SAP Central Process Scheduling)

#### **i** Note

You need the S\_BTCH\_EXT authorization object only if you connect the Closing Cockpit to [SAP Central Process Scheduling by Redwood](#) (CPS). SAP CPS is **not** a part of SAP ERP.

For more information about [SAP CPS](#), see the Internet address [www.sdn.sap.com/irj/sdn/nw-scheduling](http://www.sdn.sap.com/irj/sdn/nw-scheduling).

## 13.2.3.2 More Security Information

### Network and Communication Security

If you want to connect the Closing Cockpit to SAP Central Process Scheduling (CPS), see also the security notes related to SAP CPS. For more information (including the relevant guides), see the [SAP Service Marketplace](#) at [www.sdn.sap.com/irj/sdn/nw-scheduling](http://www.sdn.sap.com/irj/sdn/nw-scheduling).

### Security in Internet Communication Framework

You should only activate those services that are necessary for the applications in your system. The following service is required for the Closing Cockpit:

Name of the service: ClOCo

Path: /sap/public/BusinessSuite/

Use transaction SICF to activate this service.

If your firewalls filter by URLs, you have to note the URLs of the services and modify the settings for your firewall accordingly.

For more information, see *Activating/Deactivating ICF Services* in the SAP NetWeaver documentation in the SAP Library.

For more information about ICF security, see *RFC/ICF Security Guide*.

## Data Storage Security

The data of the Closing Cockpit is stored at the following locations:

- In the database of the SAP system
- In the *Business Document Service* (BDS)

The Closing Cockpit does **not** store any personal or sensitive data.

## 13.2.4 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
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

Role	Description
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: X Account Authorization for Customers			
F_BKPF_BEK	Accounting Document: Account Authorization for Vendors		X	
F_BKPF_BES	Accounting Document: Account Authorization for G/L Accounts			X

Authorization Object	Description	Customer	Vendor	G/L Accounts
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	
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		

Authorization Object	Description	Customer	Vendor	G/L Accounts
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
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	

Authorization Object	Description	Customer	Vendor	G/L Accounts
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	
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	

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_KNKA_AEN	Credit Management: Change Authorization for Certain Fields	X		
F_KNKA_KKB	Credit Management: Authorization for Credit Control Area	X		

## 13.2.5 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
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



Role	Description
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

Authorization Object	Description	Customer	Vendor	G/L Accounts
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	
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		

Authorization Object	Description	Customer	Vendor	G/L Accounts
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
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	

Authorization Object	Description	Customer	Vendor	G/L Accounts
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	
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	

Authorization Object	Description	Customer	Vendor	G/L Accounts
F_KNKA_AEN	Credit Management: Change Authorization for Certain Fields	X		
F_KNKA_KKB	Credit Management: Authorization for Credit Control Area	X		

## 13.2.6 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>.

### 13.2.6.1 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
<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>i Note</b></p> <p>You require this authorization if you want to use the bank statement overview. You can only display the bank statement overview in the SAP NetWeaver Business Client.</p> </div>	
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

## 13.2.6.2 Data Storage Security

For information on communication with external systems, see the general part of this Guide under [Financial Accounting \[page 32\]](#).

### → 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 your 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\_RFEBKATO\_FILE
  - Program using this logical file name:
    - RFEBKATO
- FI\_RFEBKATX\_FILE
  - Program using this logical file name:
    - RFEBKATX
- FI\_RFEBKAT1\_FILE
  - Program using this logical file name:
    - RFEBKAT1
- FI\_RFEBESTO\_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.

## More Information

For more information, see the following SAP Notes:

Title	SAP Note
Bank Statement: Potential Directory Traversal	1509800
Potential Directory Traversals in Applications	1497003

## 13.2.7 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.

## 13.2.8 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> <i>Program Name</i>	FI_ROOT
RGRLTE00			
RGRMTE00			
RGR RTE00			
RGR STE00			
RGRVTE00			
RGRXTE00			

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

### Activating the Validation of Logical Paths and File Names

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

## 13.3 Controlling

### 13.3.1 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)	<ul style="list-style-type: none"> <li>SORG (Service Organization)</li> <li>VART (Business Transaction Type)</li> <li>ACTVT (Activity)</li> </ul>	A5	Display reports
K_FP_B_EXP (Authorization Object for Express Planning)	<ul style="list-style-type: none"> <li>EXP_SCEN (Planning Scenario)</li> <li>EXP_INST (Express Planning Instance)</li> <li>ACTVT (Activity)</li> </ul>	02	Change
		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)	<ul style="list-style-type: none"> <li>PVARIANT (Screen Variant for Manual Actual Postings in CO)</li> <li>VRGNG (Business Transaction)</li> </ul>		Assigns authorization to define posting variants for each business transaction.
K_MLMBDISP (CO Material Ledger: Display Material Valuation Document)	<ul style="list-style-type: none"> <li>BWKEY (Valuation area)</li> </ul>		Assigns authorization to display the material valuation document.

Authorization Object	Field	Value	Description
K_ML_MTART (CO Material Ledger: Material Type)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> <li>MTART (Material type)</li> </ul>	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)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> <li>BWKEY (Valuation area)</li> </ul>	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.
		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)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> <li>BWKEY (Valuation area)</li> </ul>	03	Display
		16	Execute
		44	Flag
K_CBPR_VA	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>ACTVT (Activity)</li> </ul>	02	Change Assigns authorization for changing business process groups.

Authorization Object	Field	Value	Description
		03	Display Assigns authorization for displaying business process groups.
K_CBPR_PLA	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• PRZNR (Business Process)</li> <li>• ACTVT (Activity)</li> </ul>	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	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• ACTVT (Activity)</li> </ul>	02	Change Assigns authorization for changing cost object groups.
		03	Display Assigns authorization for displaying cost object groups.
K_ABC	<ul style="list-style-type: none"> <li>• AUTHAREA (Authorization Area for Business Processes)</li> <li>• CO_ACTION (Actions for CO-OM Authorization Check)</li> <li>• KSTAR (Cost Element)</li> </ul>		Assigns authorization for maintenance actions in business process master data, manual business process planning, the template, and the information system.
K_CSLA_SET	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create activity types.
		02	Change Assigns authorization to change activity types.

Authorization Object	Field	Value	Description
		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_CSXS_BUD (CO-CCA: Cost Center Budget Planning)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• KOSTL (Cost Center)</li> <li>• ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to change the budget of cost centers.
		03	Display Assigns authorization to display the budget of cost centers.
K_CSXS_SET (CO-CCA: Cost Center Groups)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to change cost center groups.
		03	Display Assigns authorization to display cost center groups.
		06	Delete
K_CSXS (CO-CCA: Cost Center Master)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• KOSTL (Cost Center)</li> <li>• ACTVT (Activity)</li> </ul>	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.



Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• KOSTL (Cost Center)</li> <li>• ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to change the planning of cost centers.
		03	Display Assigns authorization to display the planning of cost centers.
K_ CSKA_SET (CO-CCA Cost Element Groups)	<ul style="list-style-type: none"> <li>• KTOPL (Chart of Accounts)</li> <li>• ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• CO_KAINT (Cost Element Classification (Primary/Secondary))</li> <li>• ACTVT (Activity)</li> </ul>	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.

Authorization Object	Field	Value	Description
		08	Display change documents Assigns authorization to view cost element change documents.
K_CSKB_PLA (CO-CCA: Cost Element Planning)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• KSTAR (Cost Element)</li> <li>• ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>• RESPAREA (CO-OM Responsibility Area)</li> <li>• CO_ACTION (Actions for CO-OM Authorization Check)</li> <li>• KSTAR (Cost Element)</li> </ul>		Assigns authorization for the maintenance of cost center master data, manual cost center planning, and the information system.
K_REPO_CCA (CO-CCA: Reporting on Cost Centers/Cost Elements)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• KOSTL (Cost Center)</li> <li>• KSTAR (Cost Element)</li> <li>• ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to change statistical key figure groups.
		03	Display Assigns authorization to display statistical key figure groups.

Authorization Object	Field	Value	Description
K_ORDER (CO-OPA: General authorization object for internal orders)	<ul style="list-style-type: none"> <li>RESPAREA (CO-OM Responsibility Area)</li> <li>AUFART (Order Type)</li> <li>AUTHPHASE (Internal order authorization: Authorization phase)</li> <li>CO_ACTION (Actions for CO-OM Authorization Check)</li> <li>KSTAR (Cost Element)</li> </ul>		Assigns authorization for the following actions while working with internal orders: <ul style="list-style-type: none"> <li>Maintenance of order master data</li> <li>Manual order planning</li> <li>Budgeting of orders</li> <li>Actions in the information system</li> </ul>
		02	Change
		03	Display
			Assigns authorization to change order groups.
			Assigns authorization to display authorization objects in CO-PA planning.
K_KELP_GP (CO-PA Planning: Integrated Planning)	<ul style="list-style-type: none"> <li>CEERKRS (Operating concern)</li> <li>ACTVT (Activity)</li> </ul>	16	Execute
			Assigns authorization to restrict the way integrated planning is used.
K_KELP_VER (CO-PA Planning: Plan Version)	<ul style="list-style-type: none"> <li>CEVERSI (Plan version (CO-PA))</li> </ul>		Assigns authorization to process plans depending on plan version.
K_KELP_RC (CO-PA Planning: Planning Layouts)	<ul style="list-style-type: none"> <li>CEERKRS (Operating concern)</li> <li>CEFORM (Form)</li> <li>ACTVT (Activity)</li> </ul>	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.		

Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>WERKS (PLANT)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>WERKS (PLANT)</li> <li>ACTVT (Activity)</li> </ul>	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_BU (CO-PC-OBJ: WIP Calculation and Results Analysis)	<ul style="list-style-type: none"> <li>BUKRS (Company Code)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>PRCTR (Profit Center)</li> <li>ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to change processed objects in WIP calculation and results analysis.

Authorization Object	Field	Value	Description
		03	Display Assigns authorization to display processed objects in WIP calculation and results analysis.
K_CBEW (CO-PC: Concurrent Costing - Cstg Master Data)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	01	Create or generate
		02	Change
		03	Display
		06	Delete
K_CKPH (CO-PC: Cost Objects)	<ul style="list-style-type: none"> <li>KTRAT (Cost Object Category)</li> <li>ACTVT (Activity)</li> </ul>	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.
		06	Delete Assigns authorization to delete cost object IDs.
		72	Plan
		A5	Display reports
K_KEKO (CO-PC: Product Costing)	<ul style="list-style-type: none"> <li>KLVAR (Costing Variant)</li> <li>BUKRS (Company Code)</li> <li>ACTVT (Activity)</li> </ul>	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.

Authorization Object	Field	Value	Description
		39	Check
K_CKBOB (CO-PC: Product Drill-down)	<ul style="list-style-type: none"> <li>WERKS (Plant)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>WERKS (Plant)</li> <li>ACTVT (Activity)</li> </ul>	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.
		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)	<ul style="list-style-type: none"> <li>BUKRS (Company Code)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>IDENT (Hierarchy ID)</li> <li>KOKRS (Controlling Area)</li> <li>ACTVT (Activity)</li> </ul>	03	Display Assigns authorization to display a summary of order costs.

Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>IDENT (Hierarchy ID)</li> <li>KOKRS (Controlling Area)</li> <li>ACTVT (Activity)</li> </ul>	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.
K_TEMPL (CO: Auth. Template (ABC-allocation, formula planning, other))	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>TPLCLASS (Valid Environments)</li> <li>TEMPLATE (Template)</li> <li>ACTVT (Activity)</li> </ul>		
K_VRGNG (CO: Bus. Trans., Actual Postings and Plan/act. Allocations)	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>CO_VRGNG (CO Business Transaction)</li> <li>ACTVT (Activity)</li> </ul>	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).

Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>BASSL (Calculation Base for Overheads)</li> <li>ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to change the overhead rate base.
		03	Display Assigns authorization to display the overhead rate base.
K_ZKALSM (CO: Costing sheet)	<ul style="list-style-type: none"> <li>KALSM (Procedure)</li> <li>ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to change the costing sheet.
		03	Display Assigns authorization to display the costing sheet.
K_ZENTSL (CO: Credit)	<ul style="list-style-type: none"> <li>ENTSL (Credit for overhead)</li> <li>ACTVT (Activity)</li> </ul>	02	Change
		03	Display
K_KMBO_DCT (CO: Document Type for Manual Funds Reservation)	<ul style="list-style-type: none"> <li>BUKRS (Company Code)</li> <li>KBLART (Doc.Type: Manual document entry)</li> <li>ACTVT (Activity)</li> </ul>	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.



Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• KFPBLA (Document type: Transfer price agreement/allocation)</li> <li>• ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create transfer price agreements with particular document types.
		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)	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> <li>• KFPBLA (Document type: Transfer price agreement/allocation)</li> </ul>	01	Create or generate Assigns authorization to create transfer price allocations with particular document types.

Authorization Object	Field	Value	Description
	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>CEAPPL (Application class for drilldown reporting)</li> <li>TABLE (Table Name)</li> <li>CEFORM (Form)</li> <li>ACTVT (Activity)</li> </ul>	01	Create or generate  Assigns authorization to create row and column structures for drilldown reporting.
		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)	<ul style="list-style-type: none"> <li>IDENT (Hierarchy ID)</li> <li>KOKRS (Controlling Area)</li> <li>ACTVT (Activity)</li> </ul>	03	Display  Assigns authorization to display general controlling summarization (without classification).

Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>• CEAPPL (Application class for drilldown reporting)</li> <li>• TABLE (Table Name)</li> <li>• CEREPID (Report)</li> <li>• ACTVT (Activity)</li> </ul>	01	Create or generate
		02	Change
		03	Display
		04	Print, edit messages
		16	Execute
		21	Transport
		28	Display line items
		29	Display saved data
		32	Save
		60	Import
		61	Export
		65	Reorganize
		66	Refresh
		L0	All functions
L1	Function range level 1		
L2	Function range level 2		
K_ORGUNIT (CO: Organizational Units Used in Actual Postings)			

Authorization Object	Field	Value	Description
K_ZZUSSL (CO: Overhead)	<ul style="list-style-type: none"> <li>ZUSSL (Overhead rate)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>ZUSSL (Overhead rate)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>BRGRU (Authorization Group)</li> <li>ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create authorization for planner profiles.
		02	Change Assigns authorization to change authorization for planner profiles.
		03	Display Assigns authorization to display authorization for planner profiles.
		06	Delete
		16	Execute
K_REPO_USR (CO: Reporting / User Settings)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> <li>KUSRGR (Indicator for user group)</li> </ul>	02	Change Assigns authorization to change user settings for overhead cost controlling.
		03	Display Assigns authorization to display user settings for overhead cost controlling.

Authorization Object	Field	Value	Description
K_KA_TREC (CO: Summarization Levels)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> <li>CEAPPL (Application class for drilldown reporting)</li> <li>TABLE (Table Name)</li> </ul>	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)	<ul style="list-style-type: none"> <li>BRGRU (Authorization Group)</li> <li>ACTVT (Activity)</li> </ul>	02	Change
		03	Display
		72	Plan
		DP	Delete plan
K_KC_PL (EC-BP: Authorization for Planning Layouts)	<ul style="list-style-type: none"> <li>CFASPET (Aspect (application area))</li> <li>CEFORM (Form)</li> <li>ACTVT (Activity)</li> </ul>		Assigns authorization to create, change, and display planning layouts. It also assigns authorization to display and change plan data.
K_KC_DE (EC-EIS Authorization - Entry Layout / Data Entry)	<ul style="list-style-type: none"> <li>CFASPET (Aspect (application area))</li> <li>CEFORM (Form)</li> <li>ACTVT (Activity)</li> </ul>	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.

Authorization Object	Field	Value	Description
		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))	01	Create or generate
	• CFFIENM (Field Name)	02	Change
	• CFHVERS (Hierarchy variant)	03	Display
	• ACTVT (Activity)	06	Delete
K_ KC_PRC (EC-EIS: Authorization for Presentation of Form)	• CFASPET (Aspect (application area))	01	Create or generate Assigns authorization to create a form.
	• CEFORM (Form)	02	Change Assigns authorization to change a form.
	• ACTVT (Activity)	03	Display Assigns authorization to display a form.
		16	Execute Assigns authorization to use a form in the information system.
K_ KC_DSK (EC-EIS: Authorization for Structures and Key Figures)	<ul style="list-style-type: none"> <li>• CFASPET (Aspect (application area))</li> <li>• CFAPPLC (Application class for DD objects (not used))</li> <li>• CFOKCOD (EC-EIS/BP function code)</li> <li>• TCD (Transaction Code)</li> </ul>		
K_ KC_DS (EC-EIS: Authorizations for Data Structure Maintenance)	<ul style="list-style-type: none"> <li>• CFASPET (Aspect (application area))</li> <li>• CFKYRSP (Application)</li> <li>• CFOKCOD (EC-EIS/BP function code)</li> <li>• TCD (Transaction Code)</li> </ul>		Assigns authorization for maintaining and displaying data structure and key figures.

Authorization Object	Field	Value	Description
K_ KC_DB (EC-EIS: Authorizations for the Data Basis)	<ul style="list-style-type: none"> <li>CFASPET (Aspect (application area))</li> <li>CFRECTY (Record type)</li> <li>CFVERSO (Data area (previously version))</li> <li>CFPERDE (Period)</li> <li>CFVALTY (Value type)</li> <li>CFOKCOD (EC-EIS/BP function code)</li> <li>TCD (Transaction Code)</li> </ul>		
		01	Create or generate
		02	Change
		03	Display
		06	Delete
		16	Execute
K_ PCAI_UEB (EC-PCA: Actual Data Transfer)	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> </ul>		Assigns authorization to transfer actual data.
K_ PCAD_UM (EC-PCA: Assessment/Distribution)	<ul style="list-style-type: none"> <li>GLRRCTY (Record Type)</li> <li>ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create cycles.
		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.

Authorization Object	Field	Value	Description
K_PCAB_DEL (EC-PCA: Delete Transaction Data)	<ul style="list-style-type: none"> <li>GLRLDNR (Ledger)</li> </ul>		Assigns authorization to delete transaction data for profit centers.
K_PCAF_UEB (EC-PCA: FI Data Transfer)	<ul style="list-style-type: none"> <li>BUKRS (Company Code)</li> </ul>		
K_PCAL_GEN (EC-PCA: Generate and activate ledger)	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	90	Copy Assigns authorization to transfer data from materials management (MM).
K_PCAP_UEB (EC-PCA: Plan Data Transfer)	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>CEVERSN (Version)</li> <li>CEGJAHR (Fiscal Year)</li> </ul>		Assigns authorization to transfer plan data to profit centers.
K_PCAP_SET (EC-PCA: Planning Hierarchy)	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create profit centers.



Authorization Object	Field	Value	Description
		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.
Activate Assigns authorization to activate inactive profit centers.	<ul style="list-style-type: none"> <li>• KOKRS (Controlling Area)</li> </ul>		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)	<ul style="list-style-type: none"> <li>• RESPAREA (CO-OM Responsibility Area)</li> <li>• CO_ACTION (Actions for CO-OM Authorization Check)</li> <li>• KSTAR (Cost Element)</li> </ul>		
K_PCAS_UEB (EC-PCA: SD Data Transfer)	<ul style="list-style-type: none"> <li>• ACTVT (Activity)</li> </ul>	90	Copy Assigns authorization to transfer data from sales and distribution (SD).
K_PCAS_SRP (EC-PCA: Standard Reports and Datasets)	<ul style="list-style-type: none"> <li>• GLRLDNR (Ledger)</li> <li>• ACTVT (Activity)</li> </ul>	02	Change

Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>• BUKRS (Company Code)</li> <li>• PRCTR (Profit Center)</li> <li>• KSTAR (Cost Element)</li> <li>• ACTVT (Activity)</li> </ul>	01	Create or generate
		02	Change
		03	Display Assigns authorization to display documents.
		06	Delete
		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.

Authorization Object	Field	Value	Description
K_ML_MGV (Material Ledger: Master Data of Quantity Structure Tool)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> <li>WERKS (Plant)</li> </ul>	01	Create or generate
		02	Change
		03	Display
K_KEPL_TC (Profit Planning)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	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 authorization checked for CO-PA authorizations.
K_KEPL_FR (Profit Planning: Initial Screen)	<ul style="list-style-type: none"> <li>CEERKRS (Operating concern)</li> <li>ACTVT (Activity)</li> </ul>	02	Change
		03	Display
		16	Execute
		21	Transport
		GL	General overview
K_KEI_TC (Profitability Analysis: Actual Data)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create line items.
		02	Change Assigns authorization to perform periodic valuation or top-down actual distribution.

Authorization Object	Field	Value	Description
		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_KED_TC (Profitability Analysis: Conditions)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create condition tables and pricing reports.
		02	Change Assigns authorization to change condition tables and pricing reports.
		03	Display Assigns authorization to display condition tables and pricing reports.
		16	Execute Assigns authorization to execute condition lists.
K_KED_UM (Profitability Analysis: Cost Center Assessment)	<ul style="list-style-type: none"> <li>CEERKRS (Operating concern)</li> <li>CEPLIKZ (Plan/Actual Indicator)</li> <li>ACTVT (Activity)</li> </ul>	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.

Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	01	Create or generate
		02	Change Assigns authorization to change derivation strategies.
		03	Display Assigns authorization to display derivation strategies.
K_KEA_ALE (Profitability Analysis: Distribution)	<ul style="list-style-type: none"> <li>CEERKRS (Operating concern)</li> <li>ACTVT (Activity)</li> </ul>	01	Create or generate
		02	Change
		03	Display
		16	Execute
		64	Generate
K_KEA_TC (Profitability Analysis: Maintain Operating Concern)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create operating concerns.
		02	Change Assigns authorization to change operating concerns.

Authorization Object	Field	Value	Description
		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)	<ul style="list-style-type: none"> <li>• CEERKRS (Operating concern)</li> <li>• ACTVT (Activity)</li> </ul>	01	Create or generate Assigns authorization to create, change, and test realignments.
		03	Display Assigns authorization to display and test realignments.
		16	Execute Assigns authorization to execute realignments including scheduling and starting background jobs.
K_KEA_ERG (Profitability Analysis: Set Operating Concern)	<ul style="list-style-type: none"> <li>• CEERKRS (Operating concern)</li> </ul>		
K_KEDT_TC (Profitability Analysis: Transfer Data to CO-PA)	<ul style="list-style-type: none"> <li>• ACTVT (Activity)</li> </ul>	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.

Authorization Object	Field	Value	Description
		58	Display takeover
K_KEB_BER (Profitability Report: Authorization Objects)	<ul style="list-style-type: none"> <li>• CEERKRS (Operating concern)</li> <li>• ACTVT (Activity)</li> </ul>	02	Change
		03	Display
K_KEB_RC (Profitability Report: Forms)	<ul style="list-style-type: none"> <li>• CEERKRS (Operating concern)</li> <li>• CEFORM (Form)</li> <li>• ACTVT (Activity)</li> </ul>	01	Create or generate
		02	Change
		03	Display
		21	Transport
		60	Import
K_KEB_REP (Profitability Report: Report Name)	<ul style="list-style-type: none"> <li>• CEERKRS (Operating Concern)</li> <li>• CEREPID (Report)</li> <li>• ACTVT (Activity)</li> </ul>	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.
		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.

Authorization Object	Field	Value	Description
		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.
		02	Change Assigns authorization as follows: <ul style="list-style-type: none"> <li>• To change and delete reports</li> <li>• Test monitor for profitability reports</li> <li>• Assign a hierarchy for account-based CO-PA</li> <li>• Maintain variables</li> <li>• Maintain the report tree</li> </ul>
		03	Display Assigns authorization to display reports.
		16	Execute Assigns authorization to execute reports.



Authorization Object	Field	Value	Description
		65	Reorganize Assigns authorization to reorganize the following: <ul style="list-style-type: none"> <li>• Report data</li> <li>• Reports</li> <li>• Forms</li> <li>• Layouts</li> </ul>
		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.
K_KC_DB_VS (SAP-EIS Authorization for Data Basis Version & Plan/Act Ind.)	<ul style="list-style-type: none"> <li>• CFASPET (Aspect (application area))</li> <li>• CFVERSION (Version)</li> <li>• CFPLANT (Plan/Act. indicator (EC-EIS/EC-BP))</li> <li>• CFOKCOD (EC-EIS/BP function code)</li> </ul>		Assigns authorization for the aspect, version, and plan/actual indicator.
K_KC_PR (SAP-EIS: Authorization for Presentation)	<ul style="list-style-type: none"> <li>• CFHIEID (User group)</li> <li>• CFLFDID (Sequence number for hierarchical node)</li> <li>• CFREPID (Report)</li> <li>• CFJDEST (Storage place of SAP-EIS report)</li> <li>• CFOKCOD (EC-EIS/BP function code)</li> <li>• TCD (Transaction Code)</li> </ul>		
K_KC_PBR (SAP-EIS: Authorization for Presentation Objects)	<ul style="list-style-type: none"> <li>• CFASPET (Aspect (application area))</li> <li>• ACTVT (Activity)</li> </ul>	02	Change Assigns authorization to create and change an authorization object.
		03	Display Assigns authorization to display an authorization object.

Authorization Object	Field	Value	Description
K_TEST (Test)	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>		
K_TP_VALU (Transfer Price Valuations)	<ul style="list-style-type: none"> <li>KOKRS (Controlling Area)</li> <li>VALUTYP (Valuation View)</li> <li>ACTVT (Activity)</li> </ul>	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)	<ul style="list-style-type: none"> <li>BUKRS (Company Code)</li> <li>WERKS (Plant)</li> <li>CWPRICLABL (Price Type)</li> <li>ACTVT (Activity)</li> </ul>	02	Change	
			03	Display
K_PRS_LS (CO Authorization for Prof. Services Lean Staffing)	<ul style="list-style-type: none"> <li>PRCTR (Profit Center)</li> <li>ACTVT (Activity)</li> </ul>	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))	<ul style="list-style-type: none"> <li>ACTVT (Activity)</li> </ul>	06	Delete
			Assigns authorization to delete log entries in the Period-End Partner (PEP).
		13	Execute

Authorization Object	Field	Value	Description
K_MLNUSER (CO Material Ledger: Individual settlement; (no longer used))	<ul style="list-style-type: none"> <li>BWKEY (Valuation area)</li> </ul>		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))	<ul style="list-style-type: none"> <li>BWKEY (Valuation area)</li> </ul>		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](http://help.sap.com) 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

## 13.3.2 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	1515306

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

### Authorizations

#### Standard Roles

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

Standard Roles in Profit Center Accounting

Role	Description
SAP_AUDITOR_BA_EC_PCA	AIS - Profit Center Accounting
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

Role	Description
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 Objects in Profit Center Accounting

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_PCAL_UEB	EC-PCA: Actual Data Transfer
K_PCAL_GEN	EC-PCA: Generate and Activate Ledger
K_PCAM_UEB	EC-PCA: MM Data Transfer
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

## 13.3.3 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).

### 13.3.3.1 Communication Destinations

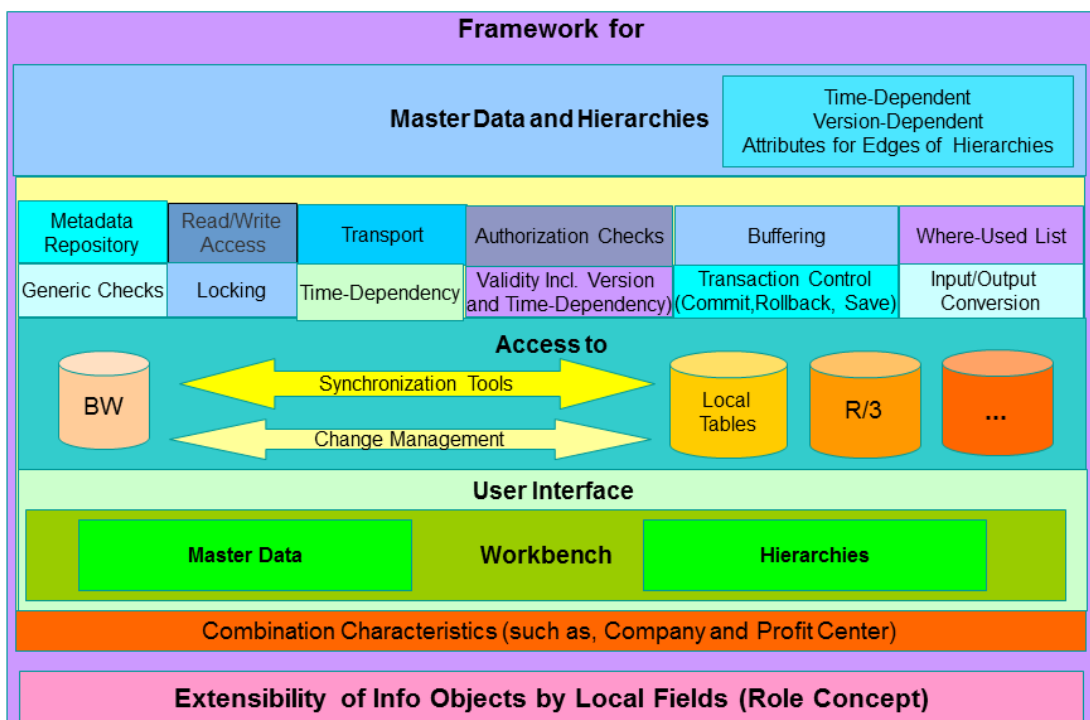
Technical users are required for communication over ALE, for batch reporting, and for third-party providers that access Controlling data.

## 13.4 Master Data Framework

### 13.4.1 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 <i>Master Data Framework</i> and the underlying technical components, such as <i>SAP NetWeaver</i>	Master Guide	service.sap.com/instguides
Technical configuration High availability	Technical Infrastructure Guide	service.sap.com/ti
Security		service.sap.com/security

## 13.4.2 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 <i>MDF Garbage Collector</i>

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

## 13.4.3 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.

## 13.5 Joint Venture Accounting

### 13.5.1 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

### 13.5.2 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



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

## 13.6 Manufacturing

### 13.6.1 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

<b>Role</b>	<b>Description</b>
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)

<b>Role</b>	<b>Description</b>
SAP_PP_CAPA_PLAN	Plan Capacities
SAP_PP_CAPA_PLAN_EVAL	Evaluate Capacity Planning

Roles: Kanban (PP-KAB)

<b>Role</b>	<b>Description</b>
SAP_PP_KAB_CONTROL	KANBAN Control
SAP_PP_KAB_REPORTING	KANBAN Evaluation

Roles: Production Planning (PP-MP)

<b>Role</b>	<b>Description</b>
SAP_PP_MP_FORECAST	Material Forecast
SAP_PP_MP_LONG_TERM_PLANNING	Long-term planning
SAP_PP_MP_MPS_PLANNING	Master Production Scheduling

Roles: Material Requirements Planning (PP-MRP)

<b>Role</b>	<b>Description</b>
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

<b>Role</b>	<b>Description</b>
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)

<b>Role</b>	<b>Description</b>
SAP_PP_REM_CONFIRMATION	Repetitive Manufacturing - Backflushing
SAP_PP_REM_MASTERDATACHANGE	Repetitive Manufacturing – Change Master Data
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)

<b>Role</b>	<b>Description</b>
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_RECIPES_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_RECIPES_EXP	Edit Master Recipe
SAP_PP_PI_MASTER_RECIPES_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
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

<b>Role</b>	<b>Description</b>
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)

<b>Role</b>	<b>Description</b>
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
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

Authorization Object	Description
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
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

Authorization Object	Description
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

## 13.6.2 Production Engineering

### 13.6.2.1 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	<p>Production Engineering - Discrete Manufacturing</p> <p>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.</p> <p>This business role is required for discrete manufacturing.</p>
SAP_BR_PRODN_ENG_PROC	<p>Production Engineer - Process Manufacturing</p> <p>The corresponding business role required for the process industry.</p>

## 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)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
	BEGRU		Authorization Group
	STLAN	1 (Production)	BOM Usage
		4 (Plant Maintenance)	
	STLTY	M (Material BOM)	BOM Category
C_STUE_NOH	NOHIS		Authorization to Edit BOMs without a Change Number

Authorization Object	Field	Value	Description	
C_STUE_WRK	ACTVT	01 (Create or generate)	Activity	
		02 (Change)		
		03 (Display)		
	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		Linked SAP Object
		STPO_DOC		
	STATUS		Document Status	

## 13.6.2.2 Authorizations for Process and 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
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)	Activity
		02 (Change)	
		03 (Display)	

Authorization Object	Field	Value	Description
	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
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

Authorization Object	Field	Value	Description
	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
	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

Authorization Object	Field	Value	Description
	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

## 13.6.3 Production Planning

### 13.6.3.1 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 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	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 (Materials Planner)
	MDAKT	A (MRP: Current Stock/ Requirements List)	Activity Types in Materials Planning
		R (MRP: current material overview)	
B (MRP: total planning)			
E (MRP: single-item planning)			
	WERKS		Plant
M_PLAF_ORG	DISPO		MRP Controller (Materials Planner)

Authorization Object	Field	Value	Description
	MDAKT	A (MRP: current stock/ requirements list)  F (MRP: Firm Planned Order)  H (MRP: Create Planned Or- der)  S (MRP: MRP list, coll. dis- play/planned order coll. con- version)  U (MRP: planned order, indi- vidual conversion)  V (MRP: change planned or- der)	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
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



Authorization Object	Field	Value	Description
M_BANF_WRK	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
	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)	Activity
		02 (Change)	
		03 (Display)	
		BSART	
M_LPET_EKG	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		EKGRP	
M_LPET_EKO	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		EKORG	

Authorization Object	Field	Value	Description
M_LPET_WRK	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
	WERKS		Plant
C_AFKO_ATY	ACTVT	01 (Create or generate)	Activity
	AUTYP	10 (Production order)	Order Category
		40 (Process order)	
C_AFKO_AWA	ACTVT	01 (Create or generate)	Activity
	AUTYP	10 (Production order)	Order Category
		40 (Process order)	
	AUFART		Order Type
	WERKS		Plant
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)	Activity
		02 (Change)	
		03 (Display)	
		43 (Release)	
	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)

Authorization Object	Field	Value	Description
C_PPBD	AKTTYP	A (Display)	Activity category in transaction (Cr/Ch/D)
		H (Add)	
V (Change)			
	WERKS		Plant
S_PROGRAM	P_GROUP	PPH_MRP	ABAP Program Authorization Group
	P_ACTION	BTCSUBMIT (Schedule programs for background processing)	User Action in ABAP Program
		SUBMIT (Execute ABAP program)	
VARIANT (Edit variants and execute ABAP program)			
S_BTCH_JOB	JOBACTION	DELE (Delete Background Jobs)	Job operations
		RELE (Release Jobs (Released Automatically When Scheduled))	
		SHOW (Display Job Queue)	
	JOBGROUP	Summary of jobs for a group	

## 13.6.4 Production Orchestration and Execution

### 13.6.4.1 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 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
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

Authorization Object	Description
C_NAV_PROF	Navigation Profile
C_TCLA_BKA	Authorization for Class Types
S_PROGRAM	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	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
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

Authorization Object	Description
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
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

Authorization Object	Description
C_CFRU_AAWK	CIM: Confirmation
C_FVER_WRK	PP-PI: Production Version - Plant
C_KAPA_ABG	CIM: Capacity leveling

## 13.6.4.2 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
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)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
		16 (Execute)	
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)	Final postings
		2 (Postprocessing)	
	BF_POST	1 (Post without correction)	Authorization for posting/correcting
		2 (Display BOM/routing)	
		3 (Change BOM/routing)	
	BF_REPPT	1 (Post previous RPs subsequently)	Reporting points (subsequent posting)
		2 (Reset RP quantities)	
BF_SCRAP	X (Yes)	Authorization for the scrap backflush	
BF_TYPE	B (Assembly backflush)	Backflush types	
	K (Component backflush)		
	L (Activity backflush)		
LGORT		Storage location	



Authorization Object	Field	Value	Description
	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)
M_MSEG_WWA	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant
M_MSEG_WWF	ACTVT	01 (Create or generate) 02 (Change) 03 (Display)	Activity
	WERKS		Plant

Authorization Object	Field	Value	Description
C_BCKFLUSH		24 (Archive)	Activity
		31 (Confirm)	
		A8 (Process mass data)	
	WERKS		Plant

### 13.6.4.3 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	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 (Materials Planner)
	MDAKT	A (MRP: Current Stock/ Requirements List)	Activity Types in Materials Planning
		R (MRP: current material overview)	
B (MRP: total planning)			
E (MRP: single-item planning)			
	WERKS		Plant
M_PLAF_ORG	DISPO		MRP Controller (Materials Planner)
	MDAKT	A (MRP: current stock/ requirements list)	Activity Types in Materials Planning
		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)	
	WERKS		Plant
M_BANF_BSA	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
	BSART		Purchasing Document Type
M_BANF_EKG	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
	EKGRP		Purchasing Group

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

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)	Activity
		02 (Change)	
		03 (Display)	
		43 (Release)	
	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)	Activity category in transaction (Cr/Ch/D)
		H (Add)	
	V (Change)		
	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
S_BTCH_JOB	JOBACTION	DELE (Delete Background Jobs)	Job operations
		RELE (Release Jobs (Released Automatically When Scheduled))	
		SHOW (Display Job Queue)	
	JOBGROUP		Summary of jobs for a group

## 13.6.4.4 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

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_CFRU_AAWK	CIM: Confirmation
C_FVER_WRK	PP-PI: Production Version - Plant
C_KAPA_ABG	CIM: Capacity leveling

## 13.6.5 Quality Management

### 13.6.5.1 Authorizations

Quality management and compliance 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 `PF03`) 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_PLM_AUDITOR	Auditor
SAP_QM_ADMIN	Administrator
SAP_QM_BATCH_INFO	Display Batch Data



<b>Role</b>	<b>Description</b>
SAP_QM_CA_INCOMING_CERT	Monitoring of Certificate Receipt
SAP_QM_CA_OUTCERT_MAINT	Administration of Certificate Master Data
SAP_QM_CA_OUTGOING_CERT	Creation of Certificates in Sales and Distribution
SAP_QM_IM_COSTS	Administration of QM Orders
SAP_QM_IM_COSTS_DISPLAY	Display of Quality-Related Costs
SAP_QM_IM_DEFECTS_REC	Defects Recording
SAP_QM_IM_LOT_COMPLETION	Inspection Lot Completion
SAP_QM_IM_LOT_MAINTAIN	Processing of Inspection Lots
SAP_QM_IM_QMANAG_WORKLIST	Worklist for Quality Managers
SAP_QM_IM_QPLANNER_INSP	Inspection Processing by Quality Planner
SAP_QM_IM_RES_REC	Results Recording
SAP_QM_IM_SAMPLE	Sample Management
SAP_QM_IT_CALIB_INFO	Calibration Information
SAP_QM_IT_CALIB_INSP	Calibration Inspection
SAP_QM_IT_CALIB_PLANNING	Calibration Planning
SAP_QM_IT_CALIB_PROCUREMENT	Procurement of Test Equipment
SAP_QM_IT_EQUI_MAINTAIN	Maintenance of Test Equipment
SAP_QM_IT_PM_NOTIF	Processing of Maintenance Notifications
SAP_QM_PP_OPERATOR	Production Operator in Production
SAP_QM_PP_SUPERVISOR	Production Supervisor
SAP_QM_PT_BASIC_DATA	Maintenance of Basic Data
SAP_QM_PT_CHANGE_MANAG_DISPLAY	Change Management - Display
SAP_QM_PT_IPLANNING	Inspection Planning
SAP_QM_PT_LOG_MASTER_DISPLAY	Display Logistics Master Data
SAP_QM_PT_LOG_MASTER_MAINT	Edit Logistics Master Data
SAP_QM_PT_MAT_MANAG_DISPLAY	Display Materials Management Information

Role	Description
SAP_QM_PT_QMANAG_MASTER_DISP	Display Logistics Master Data for Quality Managers
SAP_QM_QC_CONTROL_ALL	Overall Quality Control
SAP_QM_QC_QMIS	Quality Evaluations (QMIS)
SAP_QM_QC_QMIS_ALL	Quality Evaluations (QMIS), All
SAP_QM_QMANAG_GR	Quality Manager - Goods Receipt
SAP_QM_QMANAG_PP	Quality Manager - Production
SAP_QM_QN_NOTIF_BASIC	Extended Processing of Notifications
SAP_QM_QN_NOTIF_COSTS	Notification Costs - Order Processing
SAP_QM_QN_NOTIF_DISPLAY	Display Quality Notifications
SAP_QM_QN_NOTIF_MAINT	Processing of Notifications
SAP_QM_QN_TASK_MAINT	Processing of Tasks
SAP_QM_QN_TASK_PROCESSOR	Task Processor
SAP_SR_QUALITY_INSPECT_5	Quality Inspector

## 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	

Authorization Object	Fields	Description	Comment
Q_CAT_SSET	Selected Set Plant Catalog Status of Selected Set	Catalog Maintenance of Selected Sets	
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	

Authorization Object	Fields	Description	Comment
Q_MATERIAL	Material Authorization Group for Activities in QM Activity for QM Material Authorization Plant	Material Authorization	
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	

Authorization Object	Fields	Description	Comment
Q_STCK_CHG	Plant Stock Type Authorizations for Stock Postings	Change Stock Posting Fields in Usage Decision Transactions	
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.

## 13.6.5.2 Internet Communication Framework Security (ICF)

You should only activate those services that are needed for the applications running in your system. For quality management and compliance 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.

## 13.6.5.3 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 Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
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.

## **13.6.6 Maintenance Operations**

### **13.6.6.1 Authorizations in Plant Maintenance**

Plant Maintenance 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 for Plant Maintenance

Role	Description
SAP_COCKPIT_EAMS_MAINT_WORKER2	<p><i>Maintenance Worker 2</i></p> <p>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.</p>
SAP_COCKPIT_EAMS_GENERIC_FUNC2	<p><i>Generic EAM Functions 2</i></p> <p>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.</p>

## 13.7 R&D / Engineering

### 13.7.1 Product Safety and Stewardship

#### 13.7.1.1 Product Development for Discrete Industries

##### 13.7.1.1.1 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

## 13.7.1.2 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	<i>Compliance Manager for Recycling</i>
SAP_ISREA_HEAD_SUSTAINABILITY	<i>Head of Sustainability and Environment</i>
SAP_ISREA_MASTERDATA_EXPERT	<i>Specialist for Recycling Master Data</i>
SAP_ISREA_PACKAGING_ENGINEER	<i>Packaging Engineer</i>
SAP_ISREA_SPECIALIST	<i>Specialist for Recycling Accounting</i>
com.sap.pct.erp.rea.financial_accountant	SAP Enterprise Portal role <i>Financial Accountant</i>
com.sap.pct.erp.rea.person_responsible_master_data	SAP Enterprise Portal role <i>Person Responsible Master Data</i>
com.sap.pct.erp.rea.superadmin_masterdata	SAP Enterprise Portal role <i>Superadministrator Master Data</i>
com.sap.pct.erp.rea.compliance_manager	SAP Enterprise Portal role <i>Compliance Manager</i>
SAP_SR_REA_COMP_MAN_5	Role in SAP NetWeaver Business Client that corresponds to the SAP Enterprise Portal role <i>Compliance Manager</i>
SAP_SR_REA_FIN_ACCOUNTANT_5	Role in SAP NetWeaver Business Client that corresponds to the SAP Enterprise Portal role <i>Financial Accountant</i>
SAP_SR_REA_PERS_RESP_MD_5	Role in SAP NetWeaver Business Client that corresponds to the SAP Enterprise Portal role <i>Person Responsible Master Data</i>
SAP_SR_REA_SUPER_ADMIN_MD_5	Role in SAP NetWeaver Business Client that corresponds to the SAP Enterprise Portal role <i>Superadministrator Master Data</i>

## Standard Authorization Objects

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

Authorization Object	Name	Description
/J7L/LDE	<i>REA Lean Data Entry</i>	Controls the authorizations for the applications for lean data entry
J_7L_CONF	<i>REA: Authorization for Configuration</i>	Controls the authorizations for the import and export of recycling partner master data
J_7L_VARIA	<i>REA: Authorization for Variants</i>	Controls the access to master data objects in the Recycling Administration component depending on the respective variant
J_7L_CUST	<i>REA: Customizing</i>	Controls the authorizations for Customizing in the Recycling Administration component
J_7L_INFO	<i>REA: Information System</i>	Controls the authorizations for the applications in the information system of the Recycling Administration component
J_7L_PERIO	<i>REA: Declarations to Recycling Partners</i>	Controls the authorizations for declarations
J_7L_INFNC	<i>REA: Interfaces and Batch Programs</i>	Controls the authorizations for programs for mass processing (background processing)
J_7L_STAMM	<i>REA: Master Data</i>	Controls the authorizations for editing master data in the Recycling Administration component

## 13.8 Sales

### 13.8.1 Authorizations

*Sales and Distribution* (SD) 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 the SAP S/4HANA on-premise edition, 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 `PFCG` of the corresponding back-end clients.

The table below shows the business roles used by *Sales and Distribution* as template roles.

Role	Description
SAP_BR_BILLING_CLERK	Billing Clerk
SAP_BR_INTERNAL_SALES_REP	Internal Sales Representative
SAP_BR_PRICING_SPECIALIST	Pricing Specialist
SAP_BR_TAX_SPECIALIST	Tax Specialist
SAP_BR_SALES_MANAGER	Sales Manager

## Standard Authorization Objects

The table below shows the main security-relevant authorization objects used by *Sales and Distribution*.

Authorization Object	Description
V_AKKP_ART	Financial Documents: Authorization for Financial Document Category and Financial Document Type
V_ECCN	Foreign Percentages in Bills of Material
V_EMBK_GEG	Licenses: Authorization for Legal Regulations
V_KNA1_BRG	Customer: Account Authorization for Sales Areas

Authorization Object	Description
V_KNA1_VKO	Customer: Authorization for Sales Organizations
V_KONA_VKO	Agreement: Authorization for Sales Area/Agreement Type
V_KONH_VKO	Condition: Authorization for Sales Organizations
V_KONH_VKS	Condition: Authorization for Condition Types
V_SDPNL_CA	Address Data of Contact Person
V_VBAK_AAT	Sales Document: Authorization for Sales Document Types
V_VBAK_VKO	Sales Document: Authorization for Sales Areas
V_VBKA_VKO	Sales Activities: Authorization for Organizational Data and Sales Activity Type

## Global Trade Management

The table below shows the security-relevant authorization objects used by *Global Trade Management*.

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

## 13.8.2 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
/SAPSSL/LEG_ARCH GTS	Archiving
/SAPSSL/LEG_LCE_APP GTS	Legal Control Export: Specialist
/SAPSSL/LEG_LCI_APP GTS	Legal Control Import: Specialist
/SAPSSL/LEG_SPL_APP GTS	Sanctioned Party List: Specialist
/SAPSSL/LEG_SYS_COMM GTS	(Technical) System Communication

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

#### **i Note**

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

For more information, see Transport Layer Security and Web Services Security in the SAP NetWeaver Security Guide.

## 13.8.3 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.

## 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
Customer master data	Archiving object FI_ACCRECV
Deliveries	Archiving object RV_LIKP
Shipment documents	Archiving object SD_VTTK
Shipment cost documents	Archiving object SD_VFKK
Advanced Returns Management data	Archiving object MSR_TRC
Trading contracts	<ul style="list-style-type: none"> <li>• Archiving object WB2</li> <li>• Report WB2_UPDATE_EOP_FROM_ARCHIVE</li> </ul>
Campaigns	Data destruction object SD_CAMPAGN_DESTRUCTION

## Relevant Application Objects and Available EoP Functionality

Application	Implemented Solution (EoP or WUC)	Further Information
<ul style="list-style-type: none"> <li>• <a href="#">Sales &amp; Distribution</a> (ERP_SD)</li> </ul>	EoP check	<p>This EoP check includes business in the areas of the following:</p> <ul style="list-style-type: none"> <li>• Sales</li> <li>• Billing</li> <li>• Delivery</li> </ul>

Application	Implemented Solution (EoP or WUC)	Further Information
<ul style="list-style-type: none"> <li>• <i>Empties Management in SD</i> (ERP_SD_BIL_EM)</li> </ul>	EoP check	<p>This EoP check includes business in the areas of the following:</p> <ul style="list-style-type: none"> <li>• Supplier Empties data from invoice receipt</li> <li>• Customer Empties account for customers</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Global Trade Management Position Management</i> (LO_GT_PM)</li> <li>• <i>Global Trade Management Trading Contract</i> (LO_GT_TC)</li> <li>• <i>Global Trade Management Trading Expenses</i> (LO_GT_TE)</li> <li>• <i>Global Trade Management TEW</i> (LO_GT_TEW)</li> </ul>	EoP check	<p>This EoP check includes business in <i>Global Trade Management</i> (LO-GT).</p>

## 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\\_1511](http://help.sap.com/s4hana_op_1511) under ► *Product Assistance* ► *Enterprise Business Applications* ► *Sales* ►.

## 13.9 Sourcing and Procurement

### 13.9.1 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
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

<b>Role</b>	<b>Description</b>
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
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

Role	Description
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	<p>This transaction role allows evaluations to be collected, structured, and configured for the audit area:</p> <ul style="list-style-type: none"> <li>• Business Audit - Process View</li> <li>• Purchasing: From Purchase Order to Outgoing Payment</li> <li>• Purchasing</li> </ul>
SAP_AUDITOR_BA_MM_PUR_A	<p>This role provides read access for the audit area:</p> <ul style="list-style-type: none"> <li>• Business Audit - Process View</li> <li>• Purchasing: From Purchase Order to Outgoing Payment</li> <li>• Purchasing</li> </ul>
SAP_MM_IV_CLERK_BATCH1	Enter Invoices for Verification in the Background
SAP_MM_IV_CLERK_BATCH2	Manual Processing of Invoices Verified in the Background
SAP_MM_IV_CLERK_GRIR_MAINTAIN	GR/IR Clearing Account Maintenance
SAP_MM_IV_CLERK_GRIR_MAINTAIN	GR/IR Clearing Account Maintenance
SAP_MM_IV_CLERK_ONLINE	Online Invoice Verification
SAP_MM_IV_CLERK_PARK	Park Invoices
SAP_MM_IV_CLERK_RELEASE	Invoice Release
SAP_MM_IV_SUPPLIER_FINANCE	Settlement Information for Vendor (External Supplier) on the Internet
SAP_MM_IV_CLERK_AUTO	Automatic Settlements

Role	Description
SAP_AUDITOR_BA_MM_IV	This transaction role allows evaluations to be collected, structured, and configured for the audit area: <ul style="list-style-type: none"> <li>• Business Audit - Individual Account Closing</li> <li>• Profit and Loss Statement</li> <li>• Material Expense</li> </ul>
SAP_AUDITOR_BA_MM_IV_A	This authorization role provides read access for the audit area: <ul style="list-style-type: none"> <li>• Business Audit - Individual Account Closing</li> <li>• Profit and Loss Statement</li> <li>• Material Expense</li> </ul>

## 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
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

Authorization Object	Description
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
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

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

## 13.9.2 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
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



Authorization Object	Description
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

## 13.9.3 Other Security-Relevant Information

### Open Catalog Interface

#### Use

The Open Catalog Interface (OCI) incorporates external product catalogs into SAP S/4HANA applications using Hyper Text Transfer Protocol (HTTP). This way, the data required to create purchasing document items in SAP S/4HANA can be transferred directly from the external catalog to the SAP S/4HANA application.

#### Reason and Prerequisites

SAP S/4HANA and the catalog communicate via HTTP/HTTPS URL parameters. It is possible for an end user to identify these parameters and also change them using specialized tools. Security depends heavily on the fact whether the catalogue system resides before or behind the firewall.

#### Solution

SAP recommends the following to the customers who wish to integrate SAP S/4HANA and catalogs using Open catalog Interface (OCI):

- Double check the values transferred from the catalogue into the SAP S/4HANA application manually. Check whether the values are the same one as the one in the catalogue.
- In addition to that, authority checks are happening on SAP S/4HANA side: the application checks whether the user is allowed to change the data on SAP S/4HANA side which is transferred from the catalogue. Example: if a price is transferred from the catalogue into the purchasing document, the system checks whether the user has the authority to change the price in the purchasing document in general.
- To prevent end users from sniffing the catalog login data (User names, password), avoid specifying the login information in the OCI Catalog configuration in Customizing. Instead, configure the catalog to accept individual user authentication information from the end user. This can be done in the form of SSO (Single Sign-On) tools, Digital Certificates or Individual Login Information (User name/password). These features are dependent upon whether the Catalog provider supports the above mentioned features to logon.

You define the setting for the OCI in Customizing for *Materials Management* under ► *Purchasing* ► *Environment Data* ► *Web Services: ID and Description* ►.

## Security-Relevant Logging and Tracing

Use

Purchasing uses change documents to track changes made to purchasing documents. This includes changes to security-sensitive data such as prices. The following authorization objects specific to purchasing documents allow the restriction of the visibility of those change documents using the value 08 of the authorization field `ACTVT` (Activity):

Authorization Object	Description
M_ANFR_BSA	Document Type in RFQ
M_ANFR_EKG	Purchasing Group in RFQ
M_ANFR_EKO	Purchasing Organization in RFQ
M_ANFR_WRK	Plant in RFQ
M_ANFR_LGO	Storage Locations in RFQ
M_ANGB_BSA	Document Type in Quotation
M_ANGB_EKG	Purchasing Group in Quotation
M_ANGB_EKO	Purchasing Organization in Quotation
M_BANF_BSA	Document Type in Purchase Requisition
M_BANF_EKG	Purchasing Group in Purchase Requisition
M_BANF_EKO	Purchasing Organization in Purchase Requisition
M_BANF_FRG	Release Code in Purchase Requisition
M_BANF_WRK	Plant in Purchase Requisition
M_BANF_LGO	Storage Location in Purchase Requisition
M_BEST_BSA	Document Type in Order
M_BEST_EKG	Purchasing Group in Purchase Order
M_BEST_EKO	Purchasing Organization in Purchase Order
M_BEST_WRK	Plant in Purchase Order
M_BEST_LGO	Storage Location in Purchase Order
M_EINF_EKG	Purchasing Group in Purchasing Info Record
M_EINF_EKO	Purchasing Organization in Purchasing Info Record

Authorization Object	Description
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

## 13.9.4 Supplier Information and Master Data

### 13.9.4.1 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 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.

## 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	<p>Enables users to initiate a download of up-to-date data from D&amp;B. Since downloading data from D&amp;B is subject to charges, you should assign this role only to employees who are aware of this implication.</p> <p>Enables users to interact with an instance of a business object of Supplier Information and Master Data in a specific way. The authorization object is used in the /SRMSMC/DNB_REQUESTOR role.</p>
/SRMSMC/BO	/BOFU/BO	/SRMSMC/BO_QNR (Questionnaire) /SRMSMC/BO_SEP (Supplier Evaluation Profile) /SRMSMC/BO_SES (Supplier Evaluation Scorecard) /SRMSMC/BO_SEV (Supplier Evaluation) /SRMSMC/BO_SRS (Supplier Evaluation Response) /SRMSMC/MO_PUC (Purchasing Category) /SRMSMC/MO_QLIB (Question Library) /SRMSMC/BO_ACT (Activity) /SRMSMC/BO_TSK (Task) /SRMSMC/MO_BUPA	As the type of business object that the user can access, you can specify the values listed.

## 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.

## 13.9.4.2 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.

### 13.9.4.3 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 \[page 18\]](#) and [Application-Specific Virus Scan Profile \(ABAP\) \[page 159\]](#).

### 13.9.4.4 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 \[page 18\]](#).

## 13.9.5 Supply Chain

### 13.9.5.1 Efficient Logistics and Order Fulfillment

#### 13.9.5.1.1 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
SAP_BR_INVENTORY_ACCOUNTANT	Inventory Accountant
SAP_BR_PHYS_INV_SUPERVISOR	Physical Inventory Supervisor
SAP_BR_PHYS_INV_COUNTER	Physical Inventory Counter

### 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



Authorization Object	Field	Description
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)
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

Authorization Object	Field	Description
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

### 13.9.5.1.2 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 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

<b>Role</b>	<b>Description</b>
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
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

<b>Role</b>	<b>Description</b>
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
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

Role	Description
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

## 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

Authorization Object	Description
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

### 13.9.5.1.3 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.

## 13.10 Enterprise Technology

### 13.10.1 Middleware

#### 13.10.1.1 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 \[page 167\]](#))
- Predefined role templates (see [Role Templates \[page 183\]](#))
- The integration of custom-defined authorization objects (see [Set Up Interface-Specific and Key Field-Specific Authorizations \[page 204\]](#))
- 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*)

##### 13.10.1.1.1 Role

You need the `SAP_BR_ADMINISTRATOR_INTFMONI` role to see the SAP Application Interface Framework on the Fiori launch pad.

##### 13.10.1.1.2 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.

## 13.10.1.1.2.1 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
/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.



## 13.10.1.1.2.2 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)
/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

Value	Description
/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
/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

Value	Description
/AIF/V_IFKEY	Define Interface Key Fields for Variants
/AIF/V_NS	Define Namespace
/AIF/V_PERS_RTCCG	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

### 13.10.1.1.2.3 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	<p>You can enter the following activities:</p> <p>Execute (16) (means selecting from index tables)</p> <p>Archive (24) (means starting the archiving report using SARA)</p> <p>Reload (25) (means restoring archived data using SARA)</p> <p>Read (33) (means reading message content from persistence)</p> <p>Write (34) (means updating message content in persistence)</p> <p>Display archive (56)</p> <p>Administer (70) (means starting an external technical monitoring tool like qRFC for PI messages)</p> <p>Analyze (71) (means displaying application log messages)</p> <p>Remove (75) (means canceling a message)</p> <p>Resubmit (A4) (means restarting a message)</p> <p>General overview (GL) (means starting external monitoring like XML monitoring for PI messages or WE02 for IDocs)</p>
/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

## 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.

## 13.10.1.1.2.4 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.

## 13.10.1.1.2.5 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	<p>You can enter the following activities (see description for authorization object /AIF/ERR for details):</p> <p>Execute (16)</p> <p>Read (33)</p> <p>Write (34)</p> <p>Administer (70)</p> <p>Analyze (71)</p> <p>Remove (75)</p> <p>Resubmit (A4)</p> <p>General overview (GL)</p>
/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.

## 13.10.1.1.2.6 Authorization Objects for Custom Functions

### Definition

The authorization object /AIF/CFUNC is 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 <a href="#">Monitoring and Error Handling</a> 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:  <b>A</b> means "Just for current user"  <b>B</b> means "For a list of users" (maintained in transaction <a href="#">/AIF/CUST_FUNC</a> <a href="#">▶ Define Custom Functions</a> <a href="#">▶ Assign Users</a> <a href="#">▶</a> )  <b>C</b> 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.

## 13.10.1.1.2.7 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: <b>A</b> means "Just for current user" <b>B</b> means "For a list of users" (not used at the moment) <b>C</b> 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 hints in the *Monitoring and Error Handling* transaction and the corresponding maintenance views of the custom hints.



## 13.10.1.1.2.8 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
<code>/AIF/IDTY</code>	Application Engine Identifier	Type of application engine: 000: Proxy 001: IDoc 002: XML 003: Test File 004: ECH
<code>/AIF/NS</code>	Namespace	Namespace of a customer-specific engine
<code>/AIF/IDCTY</code>	Identifier for a Customer-Specific AIF Interface Type	Identifier of a customer-specific engine
<code>/AIF/IDN1</code>	Name 1 of Interface Type	First key field of an engine
<code>/AIF/IDN2</code>	Name 2 of Interface Type	Second key field of an engine
<code>ACTVT</code>	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.

## 13.10.1.1.2.9 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.

## 13.10.1.1.2.10 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).

## 13.10.1.1.2.11 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.

## 13.10.1.1.2.12 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 <i>Modified By</i> field

## Use

The authorization object protects the access to the user name of log entry in the [Error Handling Change Log](#).

## 13.10.1.1.2.13 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
/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: <b>A</b> means "Just for current user" <b>B</b> means "For a list of users" (not used at the moment) <b>C</b> 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 Handling](#) transaction and the corresponding maintenance views for custom message texts.

## 13.10.1.1.2.14 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: <b>A</b> means "Just for current user" <b>B</b> means "For a list of users" (not used at the moment) <b>C</b> 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.

## 13.10.1.1.3 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 \[page 185\]](#)
- SAP\_AIF\_ALL: [AIF All Authorizations \[page 189\]](#)
- SAP\_AIF\_ARCHITECT: [AIF Architect \[page 189\]](#)
- SAP\_AIF\_DEVELOPER: [AIF Developer \[page 193\]](#)
- SAP\_AIF\_USER: [AIF Business User \[page 198\]](#)
- SAP\_AIF\_POWER\_USER: [AIF Power User \[page 199\]](#)
- SAP\_AIF\_PROCESSING: [AIF Processing \[page 203\]](#)
- SAP\_AIF\_TEST\_TEMPL: [AIF Test Template \(Non-Productive\) \[page 204\]](#)

#### 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 `PF03`) 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

### 13.10.1.1.3.1 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

Authorization Object	Activity	Activity Description
/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
/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:

<b>Transaction Code</b>	<b>Description</b>
/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/DISPMGSSNAP	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_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

Transaction Code	Description
/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
/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

View/View Cluster	Description
/AIF/V_FINE_TL	Define Trace Level
/AIF/V_HINTS	Define Custom Hints
/AIF/V_PERS_RTCG	Define Runtime Configuration Group

### 13.10.1.1.3.2 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.

### 13.10.1.1.3.3 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

Authorization Object	Activity	Activity Description
/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
/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

Authorization Object	Activity	Activity Description
/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
/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/DISPMGSNAP	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

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

### 13.10.1.1.3.4 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

Authorization Object	Activity	Activity Description
/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
/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

Authorization Object	Activity	Activity Description
/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 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

Transaction Code	Description
/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/IFTTEST	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:

<b>View/View Cluster</b>	<b>Description</b>
/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
/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-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_IFKEY	Define Interface Key Fields for Variants
/AIF/V_PERS_RTGC	Define Runtime Configuration Group

## 13.10.1.1.3.5 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
/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

Authorization Object	Activity	Activity Description
/AIF/HINTS	3	Display
/AIF/HINTS	6	Delete
/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	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

### 13.10.1.1.3.6 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



Authorization Object	Activity	Activity Description
/AIF/HINTS	2	Change
/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

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/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

View/View Cluster	Description
/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
/AIF/V_VALID_PER	Define Validity Period

### 13.10.1.1.3.7 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

### 13.10.1.1.3.8 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.

### 13.10.1.1.4 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 from SYSTEM02. The interface-specific authorization is used, for example, to ensure that USER01 is not able to change data received from SYSTEM02.

# 14 SAP S/4HANA LoB Products for specific Industries

## 14.1 Automotive

### 14.1.1 Vehicle processes for Wholesale and Retail

#### 14.1.1.1 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

## 14.2 Banking

### 14.2.1 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](https://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*. ▶

#### 14.2.1.1 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).

#### 14.2.1.2 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).

## 14.2.1.2.1 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).

## 14.2.1.3 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).

## 14.2.2 Bank Customer Accounts (BCA)

### 14.2.2.1 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



Business Transaction Event	Name
SAMPLE_INTERFACE_00010950	Check management
SAMPLE_INTERFACE_00010210	Payment item dialog
SAMPLE_INTERFACE_00010410	Payment order dialog
SAMPLE_INTERFACE_00010411	Standing order dialog

## 14.2.2.2 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).

## 14.2.2.3 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 an 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.

## 14.2.3 Loans Management (FS-CML)

### 14.2.3.1 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	<ul style="list-style-type: none"> <li>• Create, change, display, delete business partner</li> <li>• Collateral value calculation, credit standing calculation and decision-making</li> <li>• Maintain objects and securities</li> <li>• Create contracts, or transfer from application or offer</li> <li>• Enter disbursements</li> <li>• Process correspondence</li> <li>• Release loan (colleague or superior)</li> <li>• Process business operations (such as charges, individual posting, pay-off)</li> </ul>
Credit Analyst	SAP_CML_CREDIT_ANALYST	<ul style="list-style-type: none"> <li>• Create, change, display, delete business partner</li> <li>• Maintain loan enquiries, applications and offers</li> <li>• Calculate credit standing</li> <li>• Decision-making</li> <li>• Maintain limits</li> <li>• Calculate the collateral value</li> <li>• Maintain objects and securities</li> </ul>
Rollover Officer	SAP_CML_ROLLOVER_OFFICER	<ul style="list-style-type: none"> <li>• Loan rollover (individual and mass)</li> <li>• Process correspondence</li> <li>• Management of rollover file</li> <li>• Maintain condition tables</li> </ul>

Role	Name	Scope
Staff Accountant for Loans	SAP_CML_STAFF_ACCOUNTANT	<ul style="list-style-type: none"> <li>• Post transactions</li> <li>• Clearing</li> <li>• Create payments</li> <li>• Post and monitor incoming payments</li> <li>• Process waivers and write-offs</li> <li>• Cancellation</li> <li>• Accrual/deferral</li> <li>• Valuation</li> <li>• Generating accounting reports</li> </ul>
Manager of Loans Department	SAP_CML_DEPARTM_MANAGER	<ul style="list-style-type: none"> <li>• Release</li> <li>• Maintain condition tables</li> <li>• Change limits</li> <li>• Risk analysis</li> <li>• Monitor file (rollover or process management)</li> <li>• Monitor portfolio and portfolio trend using reports; reports and queries</li> </ul>
Product Administrator	SAP_CML_PRODUCT_ADMIN	<ul style="list-style-type: none"> <li>• Update reference interest rates</li> <li>• Maintain condition tables</li> <li>• Maintain new business tables</li> </ul>
Technical Administrator	SAP_CML_TECHNICAL_ADMIN	<ul style="list-style-type: none"> <li>• Perform mass runs (such as mass print run), set status of plan to completed, post planned records</li> <li>• Currency conversion</li> <li>• Update reference interest rates and currency rates</li> <li>• Reorganization and data archiving</li> <li>• Define queries, drilldown reporting forms and reports</li> <li>• Maintain performance parameters</li> <li>• Analyze change pointers</li> <li>• Define export interfaces</li> </ul>

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.

## 14.2.3.2 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.

## 14.2.3.3 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](https://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 an error message.

The following lists the logical file names and paths used by *Loans Management (FS CML)* and the programs for which these file names and paths apply:

### Logical File Names Used in This Application

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

- CML\_PAYMENT\_US
- Program using this logical file name:
- RFVD\_AUTODRAFT\_PROCESS
- RFVD\_PAY\_STOP
- Parameters used in this context: None
- CML\_CREDIT\_BUREAU
- Program using this logical file name:
- RFVD\_CBR\_PROCESS
- Parameters used in this context: None
- CML\_MIGRATION\_OBJECTS\_LOGFILE\_IN
- Program using this logical file name:
- RFVOBJ01
- Parameters used in this context: None
- CML\_MIGRATION\_OBJECTS\_LOGFILE\_OUT
- Program using this logical file name:
- RFVOBJ01
- RFVOBJ01\_CREATE\_STRUCTURE
- Parameters used in this context: None
- CML\_MIGRATION\_OBJECTS\_PHYSFILE\_IN
- Program using this logical file name:
- RFVOBJ01
- Parameters used in this context: None
- CML\_MIGRATION\_OBJECTS\_PHYSFILE\_OUT
- Program using this logical file name:
- RFVOBJ01
- 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.

## 14.2.4 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](http://service.sap.com) ) that describes the basic security aspects and measures for SAP systems.

### 14.2.4.1 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 <i>CM</i> .

Role	Purpose
SAP_FS_CMS_MAINTAIN_ALL	Maintaining (Create, change and display only) all entity objects.
SAP_FS_CMS_MAINTAIN_ALL_PRC	Executing all the process related activities in addition to maintenance of objects
SAP_FS_CMS_CUST_ALL	Customizing
SAP_FS_CMS_ADMIN	CM administrator role
SAP_FS_CMS_COL_AUDITOR	Maintaining all the entity objects and the access to run all the reports in CM.
SAP_FS_CMS_CREDIT_MANAGER	Displaying collateral objects and collateral agreements.
SAP_FS_CMS_CREDIT_RISK_MANAGER	Maintaining collateral objects and collateral agreements and displaying receivables.
SAP_FS_CMS_LIQUIDATION_OFFICER	Maintaining liquidation measures.

### Authorization Objects in CM

Technical name	Name
CMS_PCN_02	Authorization for activities (change request mode)
CMS_PCN_01	Authorization for activities (normal mode)
CMS_OMS1	Authorization for all collateral objects other than real estate (replace CMS_OMS from ECC 6.0 onwards)
CMS_OMS	Authorization for all collateral objects other than real estate (obsolete from ECC 6.0 onwards)
CMS_CAG	Authorization object for collateral agreements
CMS_RE	Authorization object for real estate objects in CM.
CMS_RBL	Authorization object for receivable in CM.

### Characteristic Based Authorizations

In the Collateral Management, all the objects must belong to an administration organizational unit. The authorization objects for collateral objects (real estate and other collateral objects) and collateral agreements are based on a combination of the administration organizational unit and the entity type (assigned using a process control key). For receivables, the authorizations are based on the receivable organizational unit, the receivable status and the product. Authorizations for receivables is valid only for the receivables created in the CM or even the local copies of the receivables in external credit systems.



### i Note

For example, you can use the attribute administration organization unit to differentiate between employee ,VIP and normal customers objects. You can also create objects in these organizational units as characteristics, which can then also be used to protect application data.

## 14.2.4.2 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	
SAP Business Information Warehouse (BIW)	IDoc and RFC	Collateral agreements, collateral objects, charges, collateral agreement – receivable assignment and calculations data	
SAP Bank Analyzer ( Basel II)	IDoc and RFC	Collateral agreements, collateral objects, charges, collateral agreement – receivable assignment and calculations data	

The following RFC connections have to be set up for operating the *CM* . You are advised not to create the users belonging to these as dialog users.

- RFC communication with the Tool BW
- RFC communication within the Tool BW
- RFC communication in the context of import methods for the client copy. The relevant authorization objects are:
- S\_TABU\_DIS; S\_RS\_ICUBE; S\_RS\_ADMWB; S\_RS\_ISOURL; S\_BTCH\_ADM; S\_ADMI\_FCD; S\_BTCH\_JOB; S\_RS\_ODSO; S\_RS\_ISET

*CM* provides the following business application programming interfaces (BAPIs) for allowing external systems to connect to it:

- BAPI\_CM\_AST\_GET\_MULTI

- BAPI\_CM\_CAG\_CREATE
- BAPI\_CM\_CAG\_GETDETAIL\_MULTI
- BAPI\_CM\_CAG\_GET\_BY\_RBL
- BAPI\_CM\_GENLNK\_RBL\_ON\_RBL\_01
- BAPI\_CM\_GENLNK\_RBL\_ON\_RBL\_02
- BAPI\_CM\_SEC\_GETDETAIL\_MULTI
- BAPI\_CM\_RE\_GETDETAIL\_MULTI
- BAPI\_CM\_RIG\_GETDETAIL\_MULTI
- BAPI\_CM\_MOV\_GETDETAIL\_MULTI

B APIs are standard SAP interfaces and are important in the technical integration and in exchange of business data between SAP components and between the SAP and non-SAP components. B APIs enable you to integrate these components. They are therefore an important part of developing integration scenarios where multiple components are connected to each other, either on a local network or on the internet.

B APIs allow integration at the business level and not at the technical level. This provides for greater stability of the linkage and independence from the underlying communication technology.

The current requirement for B APIs in *CM* caters mainly to the migration scenarios. Hence these B APIs are not protected by special authorizations. Authorization checks for B APIs can be provided (in the future releases), if there are requirements for them.

*CM* also provides an extensive enhancement concept that offers user exits in the form of Business Add-Ins (BADIs).

## Network Security and Communication Channels

*Collateral Management* (*CM*) uses the same communication channels that are described in the SAP NetWeaver AS security guide. No further customer-specific communication channels are provided. Hence the aspects and actions described in the SAP NetWeaver AS security guide (such as use of SAPRouter in combination with Firewall, use of Secure Network Communication (SNC), Communication Front-End-Application Server, connection to the database) also apply for *CM*.

## 14.2.5 Reserve for Bad Debt (FS-RBD)

### 14.2.5.1 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:

- Activity  
You use the activity to control what a user is permitted to do.

- Organization

At the level of the RBD-specific objects *RBD Area* or *Organizational Unit*, you specify which data the user is permitted to display or edit in accordance with the activity.

## Standard Profiles

Preconfigured standard roles are not shipped with RBD. The following standard profiles are shipped with the SAP system:

Standard Profiles

Role	Description
S_A.SYSTEM	Access authorizations for the basis system only
S_A.ADMIN	Access authorizations for administration of the operational SAP system, but <b>without</b> access authorization for the following areas: <ul style="list-style-type: none"> <li>• ABAP/4 Development Workbench</li> <li>• Maintenance of super users</li> <li>• Maintenance of standard profiles beginning with "S_A"</li> </ul>
S_A.DEVELOP	Access authorizations for users who work with ABAP/4 Development Workbench
S_A.CUSTOMIZ	Access authorizations for basis settings in the Customizing system
S_A.USER	Access authorizations for end users (without access authorization for SAP work areas)

## Authorization Objects

The following authorization objects are shipped with *Reserve for Bad Debt (RBD)*.

RBD Authorization Objects

Object	Description	Authorization Field <i>Activity</i>	Authorization Field <i>RBD Area</i>	Authorization Field <i>Organizational Unit</i>
RBD_CUST	RBD: Customizing	16( <i>Execute</i> )	Not relevant	Not relevant

Object	Description	Authorization Field <i>Activity</i>	Authorization Field <i>RBD Area</i>	Authorization Field <i>Organizational Unit</i>
RBD_EDIT	RBD: Dialog & Batch	01 ( <i>Add or Create</i> ) 02 ( <i>Change</i> ) 03 ( <i>Display</i> ) 05 ( <i>Lock</i> ) 10 ( <i>Post</i> ) 66 ( <i>Update</i> ) 85 ( <i>Reverse</i> ) 86 ( <i>Transfer Post</i> ) 91 ( <i>Reactivate</i> ) 95 ( <i>Unlock</i> ) H1 ( <i>Deactivate</i> )	According to Customizing (table / IBS / CRB_RBD_P)	According to Customizing (table / IBS / CRB_ORGEIN)
RBD_REPO	RBD: Reporting	Not relevant	According to Customizing (table / IBS / CRB_RBD_P)	According to Customizing (table / IBS / CRB_ORGEIN)

### ⚠ Caution

For the *RBD Area* and *Organizational Unit* authorization fields, you can use the wildcard symbol “\*”. If you use the wildcard symbol, the relevant authorization field is not used to check access authorization.

### 🔗 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 “Tokio”.
- The assignment of authorization object RBD\_EDIT with *activities* 02 and 10 and RBD area 0003 enables a user to create and post planned records for an RBD account in RBD area 0003.  
However, a prerequisite for this is that the principle of multiple control for posting planned records (risk provision proposals) has **not** been activated in Customizing for RBD.

- The assignment of authorization object RBD\_REPO with *RBD area* "\*" and *organizational unit* "\*" allows a user to display the RBD data for all RBD areas using the RBD standard reports of the RBD information system, regardless of the organizational units assigned.

## 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 Manage- ment / IBS/RB_MANCON	RBD_EDIT (01, 02, 03)	Relevant +Not relevant

RBD Area Menu, Information System Folder

Transaction	Object (Activity)	RBD Area + Organizational Unit
Worklist - Processor / IBS/ RB_WORKLIST and / IBS/ RB_WORKLIST_SEL	RBD_REPO (Not relevant) RBD_EDIT (Not relevant)	Relevant + Relevant Not relevant+Not relevant
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 Analy- sis / IBS/RB_PROPRES_HGB	RBD_REPO (Not relevant) S_GUI (61)	Not relevant+Not relevant Not relevant+Not relevant

Transaction	Object (Activity)	RBD Area + Organizational Unit
Decision Template for Future Analysis / IBS/RB_PROPRES_IAS	RBD_REPO (Not relevant)	Not relevant+Not relevant
	S_GUI (61)	Not relevant+Not relevant
Decision Template for ECF Procedure / IBS/RB_PROPRES_HGB	RBD_REPO (Not relevant)	Not relevant+Not relevant
	S_GUI (61)	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)	Relevant +Not relevant
	S_APPL_LOG (03)	
Drilldown Reporting with References / IBS/RB_REF	RBD_REPO (Not relevant)	Relevant +Not relevant
IVA: List of Notes for FS-CML / IBS/RB_HINT	RBD_REPO (Not relevant)	Relevant +Not relevant
IVA: List of Notes for Multiple Source Systems / IBS/RB_HINTM	RBD_REPO (Not relevant)	Relevant +Not relevant

RBD Area Menu, Flat-Rate Value Adjustment Procedure Folder

Transaction	Object (Activity)	RBD Area + Organizational Unit
FVA: Fill RBD Gate for FS-CML / IBS/RB_FILL_GATE	Not relevant	Not relevant+Not relevant
FVA: Enrich RBD Gate / IBS/RB_GATE_MODIFY	RBD_REPO (Not relevant)	Relevant +Not relevant
FVA: Update Run / IBS/RB_PWV_UPD	RBD_EDIT (10)	Relevant +Not relevant
FVA: Update Run (PPF) / IBS/RB_PWV_UPD	RBD_EDIT (10)	Relevant +Not relevant

RBD Area Menu, Periodic Processing Folder

Transaction	Object (Activity)	RBD Area + Organizational Unit
<ul style="list-style-type: none"> <li>IVA: Update Run - Past Analysis / IBS/RB_EWB_UPD</li> <li>IVA: Update Run - Past Analysis / IBS/RB_EWB_UPD</li> </ul>	RBD_EDIT (10)	Relevant + Relevant
IVA: Update Run - Past Analysis / IBS/RB_EWB_UPD	RBD_EDIT (10)	Relevant + Relevant
<ul style="list-style-type: none"> <li>IVA: Update Run - Future Analysis / IBS/RB_IAS_UPD</li> <li>IVA: Update Run - Future Analysis (PPF) / IBS/RB_IAS_UPD_PPF</li> <li>IVA: Unwinding Run - Future Analysis / IBS/RB_IAS_UPD_UNW</li> </ul>	RBD_EDIT (02)	Relevant + Relevant
<ul style="list-style-type: none"> <li>IVA: Posting Run - Future Analysis / IBS/RB_IAS_POST</li> <li>IVA: Posting Run - Future Analysis (PPF) / IBS/RB_IAS_POST_PPF</li> <li>IVA: Unwinding Posting Run - Future Analysis / IBS/RB_IAS_POST_UNW</li> </ul>	RBD_EDIT (10)	Relevant + Relevant
<ul style="list-style-type: none"> <li>IRP: Filling Report for ECF Gate / IBS/RB_ECF_FILL</li> <li>IRP: Deletion Report for ECF Gate / IBS/RB_ECF_CLEAR</li> </ul>	Not relevant	Not relevant+Not relevant
<ul style="list-style-type: none"> <li>IRP: ECF Update Run / IBS/RB_IAS_POST</li> <li>IRP: ECF Update Run (PPF) / IBS/RB_IAS_POST_PPF</li> <li>IRP: ECF Unwinding Run / IBS/RB_IAS_POST_UNW</li> <li>IRP: ECF Unwinding Run (PPF) / IBS/RB_IAS_POST_UNW</li> </ul>	RBD_EDIT (02, 10)	Relevant +Not relevant
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

Transaction	Object (Activity)	RBD Area + Organizational Unit
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

## 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.

### 14.2.5.2 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).



## 14.2.5.2.1 Communication Destinations

For Remote Function Call (RFC) connections to *SAP Deposits Management for Banking* (FS-AM), technical users are required.

These technical users require read authorization, for example, to read balances and account master data.

## 14.2.5.3 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.

## 14.3 Public Sector

### 14.3.1 Finance

#### 14.3.1.1 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 RFEXBLKO 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.

## 14.3.1.1.1 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

Role	Name
SAP_IS_PS_CF_OI_PREPARE	Prepare Carryforward of Consumable Budget
SAP_IS_PS_MD_DISPLAY	Funds Management Master Data: Display Functions
SAP_IS_PS_MD_ZUOB	Funds Management Master Data: Assignment to CO Structures
SAP_IS_PS_PO_COMMITMENTS	Postings: Commit Funds
SAP_IS_PS_PO_CONSUMPTION_DISP	Postings: Consumed Funds Display
SAP_IS_PS_PO_FOR	Postings: Forecast of Revenue
SAP_IS_PS_PO_TRANSFERS	Postings: Transfer Consumable Budget
SAP_FI_GL_REORG_MANAGER	Reorganization Manager
SAP_FI_GL_REORG_OBJLIST_OWNER	Object List Owner

## Authorization objects for Funds Management (PSM-FM)

Authorization Object	Name
F_FICB_FKR	Cash Budget Management/Funds Management FM Area
F_FICB_VER	Cash Budget Management/Funds Management Version
F_FICA_FOG	Funds Management: Authorization Group of Fund
F_FICA_FSG	Funds Management: Authorization Group for Funds Center
F_FICA_SEG	Funds Management: Authorization Group for All Funds Centers
F_FICA_SIG	Funds Management: Authorization Group Internal Funds Centers
F_FICA_FPG	Funds Management: Authorization Group for Commitment Item
F_FICA_TRG	Funds Management: Authorization Groups of FM Acct Assignment
F_FMMD_FAR	Funds Management: Functional Area (Authorization Group)
F_FMMD_MES	Funds Management: Funded Program (Authorization Group)

Authorization Object	Name
F_FMMD_BPG	F_FMMD_BPG
F_FMMD_FPG	Funds Management: Funded Program Sets
F_FICA_FNG	Funds Management: Fund Groups
F_FICA_FAG	Funds Management: Function Groups
F_FICA_CIG	Funds Management: Commitment Item Group
F_FICA_FCG	Funds Management: Funds Center Groups
F_FMCA_SHE	Clarification Worklist (FMSHERLOCK)

See also the documentation for Funds Management on the [SAP Help Portal](https://help.sap.com) at [help.sap.com](https://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

### 14.3.1.1.2 Grants Management

#### Standard roles for Grants Management (PSM-GM)

Function	Name	Function
SAP_FI_GM_GRANT_ANALYST	Grants Management: Grant Analyst	Master data maintenance, execution of reports
SAP_FI_GM_GRANT_MANAGER	Grants Management: Grant Manager	New entry, check, and approval of master data, execution of billing program
SAP_FI_GM_PROGRAM_ANALYST	Grants Management: Program Analyst	Creation of master data, processing of proposals and budget
SAP_FI_GM_PROGRAM_MANAGER	Grants Management: Program Manager	Check and approval of proposals and budget
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

BAdI	Name
GM_POST_AUTHORITY	Grants Management Coding Block Authority Check

### 14.3.1.1.3 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](https://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.

### 14.3.1.1.4 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](https://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](#)

## 14.4 Utilities

### 14.4.1 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_NBSERV12	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_PRFF2	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_PRESCCL	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_ISSUEBPP	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.**

## 14.4.2 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`.

## 14.4.3 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.

# 15 SAP S/4HANA LOB Products

## 15.1 Asset Management

### 15.1.1 Maintenance Operations

#### 15.1.1.1 Authorizations in Plant Maintenance

Plant Maintenance 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 `PF03`) 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	<p><i>Maintenance Worker 2</i></p> <p>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.</p>
SAP_COCKPIT_EAMS_GENERIC_FUNC2	<p><i>Generic EAM Functions 2</i></p> <p>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.</p>

## 15.1.2 Environment, Health and Safety

### 15.1.2.1 User Administration and Authentication

*Environment, Health, and Safety* 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 \[page 10\]](#) in the *Introduction* section

#### 15.1.2.1.1 User Management

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

User ID	Type	Password	Description
Business processing user	Dialog user	To be entered	Business user of <i>EHS</i>

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

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

### i Note

Several business processes within *Environment, Health, and Safety* 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).

## 15.1.2.1.2 Standard Roles

In *Environment, Health, and Safety*, 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 \[page 241\]](#)
- [Roles for Managing Incidents \[page 242\]](#)
- [Roles for Managing Health and Safety Processes \[page 242\]](#)

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 *Environment, Health, and Safety* 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.

For more information about roles for *Environment, Health, and Safety*, go to [http://help.sap.com/s4hana\\_op\\_1511](http://help.sap.com/s4hana_op_1511), enter *Foundation for EHS* into the search bar, press , and open the search result with that title.



## 15.1.2.1.2.1 Roles for Foundation Processes

Role	Description
SAP_EHSM_MASTER	<p>Master PFCG role for all incident management, risk assessment and product safety and stewardship functionality. This role is intended for use as a copy template for the menu structures of the end user roles that are currently assigned.</p>
SAP_EHSM_PROCESS_ADMIN	<p>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 SAP S/4HANA system.</p> <p>This role can receive workflow items.</p>
SAP_EHSM_FND_WF_PERMISSION	<p>System user role for the Workflow Engine. This role contains the additional authorization profiles needed to process the workflows in the background.</p> <p>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.</p> <p>For processing incident management workflows, the users should also receive the same authorizations as the SAP_EHSM_HSS_INCIDENT_MANAGER role.</p> <p>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.</p>
SAP_EHSM_HSS_EML_REC	<p>System user role for the e-mail recipient. This role contains the authorization profiles needed to receive and process e-mails.</p>
SAP_EHSM_FND_MIGRATION	<p>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).</p> <p>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).</p>

## 15.1.2.1.2.2 Roles for Managing Incidents

Role	Description
SAP_EHSM_HSS_INCIDENT_MANAGER	<p>End user role for the incident manager. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the S/4HANA system.</p> <p>This role can receive workflow items.</p>
SAP_EHSM_HSS_INCIDENT_REPORTER	<p>End user role for the incident reporter. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the S/4HANA system.</p>
SAP_EHSM_HSS_INCIDENT_NOTIFIED	<p>End user role for a person who is notified during the processing of an incident. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the S/4HANA system.</p> <p>This role can receive workflow items.</p>

## 15.1.2.1.2.3 Roles for Managing Health and Safety Processes

Role	Description
SAP_EHSM_HSS_CHEMAPPR	<p>End user role for the chemical approver. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.</p>
SAP_EHSM_HSS_CHEMREQ	<p>End user role for the chemical requestor. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.</p>
SAP_EHSM_HSS_HSMGRCORP	<p>End user role for the corporate health and safety manager. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.</p>
SAP_EHSM_HSS_ENVMGR	<p>End user role for the environmental manager. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.</p>
SAP_EHSM_HSS_HAZSUBMGR	<p>End user role for the hazardous substance manager. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.</p>

Role	Description
SAP_EHSM_HSS_HYGIENIST	End user role for the industrial hygienist. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.
SAP_EHSM_HSS_LINEMGR	End user role for the line manager. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.
SAP_EHSM_HSS_SAFEMGR	End user role for the safety manager. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.
SAP_EHSM_HSS_SDSCLERK	End user role for the safety data sheet clerk. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.
SAP_EHSM_HSS_SMPLTECH	End user role for the sampling technician. This role assigns the menu structure in NWBC to the end user and the necessary authorizations in the SAP S/4HANA system.

### 15.1.2.1.3 Standard Authorization Objects

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

- [Authorization Objects for Foundation Processes \[page 243\]](#)
- [Authorization Objects for Managing Incidents \[page 249\]](#)
- [Authorization Objects for Managing Health and Safety Processes \[page 252\]](#)
- [Authorization Objects for Integration \[page 255\]](#)

#### 15.1.2.1.3.1 Authorization Objects for Foundation Processes

Authorization Object	Field	Value	Description
EHFND_CHDC (Change Document)	ACTVT	03 (Display)	Activity

Authorization Object	Field	Value	Description
	BO_NAME	EHFND_LOCATION (Location) 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)	Business Object Name
EHFND_LOC (Location)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete) A3 (Change status)	Activity
	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

Authorization Object	Field	Value	Description
EHFND_DCTR (Default Controls)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
S_PB_CHIP (Chips for side panel)	ACTVT	01 (Create or generate)	Activity (03 and 16 are needed for displaying the information in the side panel)
		02 (Change)	
		03 (Display)	
		06 (Delete)	
		16 (Execute)	

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_IN STR_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 pa- ges)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
	CONFIG_ID	EHFND_LOC_OIF_SIDE_PAN EL EHFND_CHM_SIDE_PANEL EHSS_HAZ- SUBMGR_HOMEPAGE EHSS_HYGIENIST_HOME- PAGE EHSS_INC_MANAGER _HOMEPAGE EHSS_HSMGRCORP_HOM EPAGE EHSS_SMPLTECH_HOME- PAGE	Configuration Identification
	PERS_SCOPE	0 (No Personalization 1 (User)) 2 (View Handle) 4 (All) 5 (Configuration)	Web Dynpro: Personalization

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)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
EHFND_REGL (Regulatory List Content)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	



## 15.1.2.1.3.2 Authorization Objects for Managing Incidents

Authorization Object	Field	Value	Description
EHHSS_INC1 (Incident)	ACCESS_LEV	000 (Basic Information / Standard Data)	Incident Access Level
		001 (Person Involved Access)	For more information about creating and assigning access levels to tabs, see Customizing the following activities for <i>Environment, Health, and Safety</i> under <a href="#">Incident Management</a> > <a href="#">General Information</a> >:
		002 (Injury / Illness Access)	
		003 (Confidential Access)	
		004 (Date of Birth Access)	<ul style="list-style-type: none"> <li>• <a href="#">Create Incident Access Levels</a></li> <li>• <a href="#">Assign Access Levels to Tabs</a></li> </ul>
ACTVT		01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
		C5 (Reopen)	
INC_CATEG		001 (Incident)	Incident Category
		002 (Near Miss)	
		003 (Safety Observation)	
INC_STATUS		00 (Void)	Incident Record Status
		01 (New)	
		02 (In Progress)	
		03 (Closed)	
		04 (Re-opened)	
	ORGUNIT_ID		Organizational Unit ID
	PLANT_ID		Plant ID
EHHSS_INC2 (Incident Report)	ACTVT	02 (Change)	Activity
		03 (Display)	
		06 (Delete)	

Authorization Object	Field	Value	Description
	NM_GROUP	Entries in Customizing activity <i>Specify Near Miss Groups</i> under <b>Environment, Health, and Safety</b> > <i>Incident Management</i> > <i>Incident Recording</i> >	Near Miss Group
	SO_GROUP	Entries in Customizing activity <i>Specify Safety Observation Groups</i> under <b>Environment, Health, and Safety</b> > <i>Incident Management</i> > <i>Incident Recording</i> >	Safety Observation Group
	INC_GROUP	Entries in Customizing activity <i>Specify Incident Groups</i> under <b>Environment, Health, and Safety</b> > <i>Incident Management</i> > <i>Incident Recording</i> >	Incident Group
	INC_NO_GRP	1 (Incident) 2 (Near Miss) 3 (Safety Observation)	Incident Category
EHHSS_INC5 (Incident by Location)	ACTVT	01 (Create or generate) 02 (Change) 03 (Display) 06 (Delete)	Activity
	LOCTYPE	Business Unit Equipment Production Unit Site Work Center	Location Type

Authorization Object	Field	Value	Description
	LOCSTATUS	01 (New) 02 (Active) 03 (Inactive) 04 (Historic)	Location Status
	LOCAUTHGRP		Location Authorization Group
	LOCPLANT		Plant ID
	LOCCOST		Cost Center
	LOCCOMP		Company Code
	LOCBUSAREA		Business Area
	LOCCOUNTRY		Country
	LOCREGION		Region
S_TABU_DIS	DICBERCL	EHMI (Incident) EHMF (Foundation)	Authorization Group
	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

### 15.1.2.1.3.3 Authorization Objects for Managing Health and Safety Processes

Authorization Object	Field	Value	Description
EHHSS_AGT (Agent)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
EHFND_CTRL (Control Master Data)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
EHHSS_JOB (Job)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
EHHSS_PEP (Personal Exposure Profile)	ACTVT	03 (Display)	Activity
	PERSA		Personnel Area
	BTRTL		Personnel Subarea
EHHSS_RAS (Risk Assessment, Risks, Controls on Risks and Control Inspections)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
		A8 (Process mass data)	
	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

Authorization Object	Field	Value	Description
	LOCPLANT		Plant ID
	LOCCOST		Cost Center
	LOCCOMP		Company Code
	LOCBUSAREA		Business Area
EHHSS_RASP (Proposal of Health Surveillance Protocol)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
	HSP_TYPE		Health Surveillance Protocol Type
EHHSS_HSP (Health Surveillance Protocol Master Data)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
	HSP_TYPE		Health Surveillance Protocol Type
	COUNTRY		Country Key
	REGIO		Region (State, Province, County)
EHFND_CHM (Chemical)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
EHFND_CHA (Chemical Approval)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	

Authorization Object	Field	Value	Description	
EHFND_DCTR (Default Controls)	ACTVT	01 (Create or generate)	Activity	
		02 (Change)		
		03 (Display)		
		06 (Delete)		
EHFND_DSC (Dynamic Statement Creation)	EHFND_DSCC	Entries in Customizing activity <i>Enable BO Fields for Dynamic Creation of Statements</i> under ► <i>Environment, Health, and Safety</i> ► <i>Foundation for EHS</i> ► <i>General Configuration</i> ►	Dynamic Statement Creation enabled fields	
EHFND_RCH (Request Chemical)	ACTVT	01 (Create or generate)	Activity	
		02 (Change)		(01 and 02 are needed for using the service "request chemical approval")
		03 (Display)		
		06 (Delete)		
EHFND_VEN (Vendor)	ACTVT	01 (Create or generate)	Activity	
		02 (Change)		
		03 (Display)		
		06 (Delete)		
EHHSS_SI (Safety Instruction)	ACTVT	01 (Create or generate)	Activity	
		02 (Change)		
		03 (Display)		
		06 (Delete)		
EHFND_SPL (Sample Management)	ACTVT	03 (Display)	Activity	
		16 (Execute)		
		23 (Maintain)		
	EHSM_COMP	HSS	Component	
	LOCAUTHGRP		Location Authorization Group	
	LOCPLANT		Plant ID	
LOCCOST		Cost Center		

Authorization Object	Field	Value	Description
	LOCCOMP		Company Code
	LOCBUSAREA		Business Area
EHFND_SPLM (Sampling Method)	ACTVT	01 (Create or generate)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	
S_TABU_DIS	DICBERCL	EHMR (Risk Assessment)	Authorization Group
S_PROGRAM	P_GROUP	EHFNDPRG (Foundation program authorization)	Authorization group ABAP/4 program
		EHFNDWFT (Workflow tools)	
		EHHSSRAS (Risk Assessment)	
	P_ACTION	SUBMIT	User action ABAP/4 program

### 15.1.2.1.3.4 Authorization Objects for Integration

Authorization Object	General Settings	Further Information
P_ORGIN (HR: Master data)	Display authorizations are required for specific infotypes.	See Customizing for <a href="#">Environment, Health, and Safety</a> under <a href="#">▶ Foundation for EHS ▶ Integration ▶ Human Resources Integration ▶ Check Authorizations for Person Information ▶</a>
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.	

Authorization Object	General Settings	Further Information
B_BUPA_RLT (Business partner: BP roles)	<p>Authorizations are required for the following BP roles:</p> <p>CBIH10 - External person</p> <p>HEA010 - Physician</p> <p>HEA030 - Health center (hospital)</p>	
B_BUPA_FDG (Business partner: field groups)	<p>Special authorization check for individual field groups in the business partner dialog box.</p>	

## 15.1.2.1.4 Communication Destinations

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

Destination	Delivered	Type	Description
<HR system>	No	RFC	Connection to human resource system
<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
<MOC system>	No	RFC (3, H)	Connection to <i>SAP Management of Changes</i> system (ABAP/3- and HTTP/H-Connection)
<EHS system>	No	RFC	Connection to <i>SAP EHS Management</i> as part of <i>SAP ERP</i> system

### i Note

The user in the remote HR and AC systems need to have all authorizations as proposed by the respective EHS user roles.

For *SAP Management of Changes* and *SAP EHS Management* as part of *SAP ERP*, EHS 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* ►.



## 15.1.2.2 Data Storage Security

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

In *Environment, Health, and Safety*, 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 *Environment, Health, and Safety* 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
  - The 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, see about data storage security, see the respective chapter in the SAP NetWeaver Security Guide.

## 15.1.2.3 Data Protection

Data protection is very important in the following examples:

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

*Environment, Health, and Safety* 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 \[page 25\]](#) in the *Introduction* section.

### 15.1.2.3.1 Read Access Logging of Personal Data

If you record incidents involving illnesses or injuries, you enter personal health data into the system. Since this information is potentially sensitive and access to this information is in some cases legally regulated, your organization can log information about when the data was accessed and by whom.

You can configure *Read Access Logging* to log read access to sensitive data of *Environment, Health, and Safety*. For more information, see *Read Access Logging (RAL)* in the documentation for SAP NetWeaver on the [SAP Help Portal](#).

## 15.1.2.4 Virus Scanning

The interactive forms of *Environment, Health, and Safety* 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 \[page 18\]](#) in the *Introduction* section.

## 15.1.2.5 Other Security-Relevant Information

The following information is relevant for the security of *Environment, Health, and Safety*:

### 15.1.2.5.1 Dispensable Functions with Impacts on Security

*Environment, Health, and Safety* 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.

## 15.2 Commerce

### 15.2.1 Commerce Management

#### 15.2.1.1 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).

##### 15.2.1.1.1 Authorizations

###### Business Roles

The following business roles are provided:

- SAP\_BR\_APR\_MANAGER\_FICA (Accounts Payable and Receivable Manager (FI-CA))
- SAP\_BR\_APR\_ACCOUNTANT\_FICA (Accounts Payable and Receivable Accountant (FI-CA))
- SAP\_BR\_INVOICING\_SPEC\_CINV (Invoicing Specialist (Convergent Invoicing))
- SAP\_BR\_INVOICING\_MANAGER\_CINV (Description: Invoicing Manager (Convergent Invoicing))

###### 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).

## 15.2.1.1.2 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.

### 15.2.1.1.3 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.

## 15.2.1.1.4 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.

## 15.3 Finance

### 15.3.1 Treasury and Financial Risk Management

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

##### About this Document

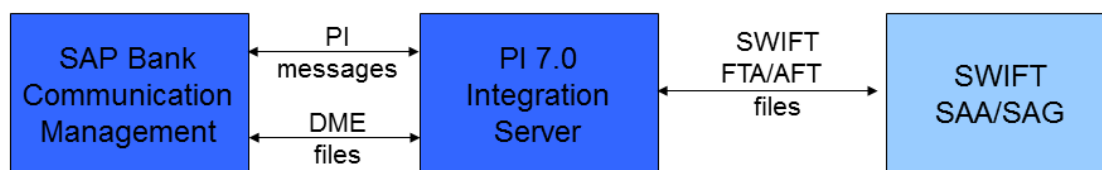
The Security Guide provides an overview of the specific security-relevant information that applies to the SAP *Bank Communication Management* including the SAP *Integration Package for SWIFT*.

##### 15.3.1.1.1 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](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	<i>Master Guide</i>	<a href="http://service.sap.com/instguides">http://service.sap.com/instguides</a>
High availability	<i>High Availability for SAP Solutions</i>	<a href="http://sdn.sap.com/irj/sdn/ha">http://sdn.sap.com/irj/sdn/ha</a>
Technical landscape design	See applicable documents	<a href="http://sdn.sap.com/irj/sdn/landscapedesign">http://sdn.sap.com/irj/sdn/landscapedesign</a>
Security	See applicable documents	<a href="http://sdn.sap.com/irj/sdn/security">http://sdn.sap.com/irj/sdn/security</a>

## 15.3.1.1.2 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 <a href="#">SAP Integration Package for SWIFT Configuration Guide</a> .

You need to create these users before XI configuration.

Assign role SAP\_XI\_IS\_SERV\_USER to user BRMXIUSER and role SWIFT\_ADMINISTRATOR to user SWIFTADMIN.

Creation of role SWIFT\_ADMINISTRATOR is described in the [SAP Integration Package for SWIFT Configuration Guide](#) .

### 15.3.1.1.3 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_ADMINISTRATOR	Operating SWIFT interface. See Integration Package for SWIFT Configuration Guide (attached in SAP Note <b>1064419</b> )
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

### 15.3.1.1.4 Communication Destinations

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

Destination	Delivered	Type	User, Authorizations	Description
INTEGRA- TION_SERVER	No	RFC	XIAPPLUSER Role SAP_XI_APPL_SERV_ USER	▶ <a href="https://service.sap.com/instguides">service.sap.com/instguides</a> ▶ <a href="#">SAP NetWeaver Configuration Guide</a> <a href="#">SAP XI</a> ▶
LCRSAPRFC	No	RFC		▶ <a href="https://service.sap.com/instguides">service.sap.com/instguides</a> ▶ <a href="#">SAP NetWeaver Configuration Guide</a> <a href="#">SAP XI</a> ▶
SAPSLDAPI	No	RFC		▶ <a href="https://service.sap.com/instguides">service.sap.com/instguides</a> ▶ <a href="#">SAP NetWeaver Configuration Guide</a> <a href="#">SAP XI</a> ▶

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

### 15.3.1.1.5 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\_RFEBKATO\_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBKATO
- FI\_RFEBKATX\_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBKATX
- FI\_RFEBKAT1\_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBKAT1
- FI\_RFEBESTO\_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBESTO
- FI\_RFEBLBT1\_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBLBT1
- FI\_RFEBLBT2\_FILE
  - Program using this logical file name and parameters used in this context:
    - RFEBLBT2

Parameters used in this context: <PARAM\_1> Program name

### Logical Path Name Used in SAP Bank Communication Management

The logical file names listed above all use the logical file path FI\_FTE\_TEST\_FILES .

## 15.3.1.2 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 208]

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 53]

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 at <http://service.sap.com/ibc>

### 15.3.1.2.1 Security Aspects of Data, Data Flow and Processes

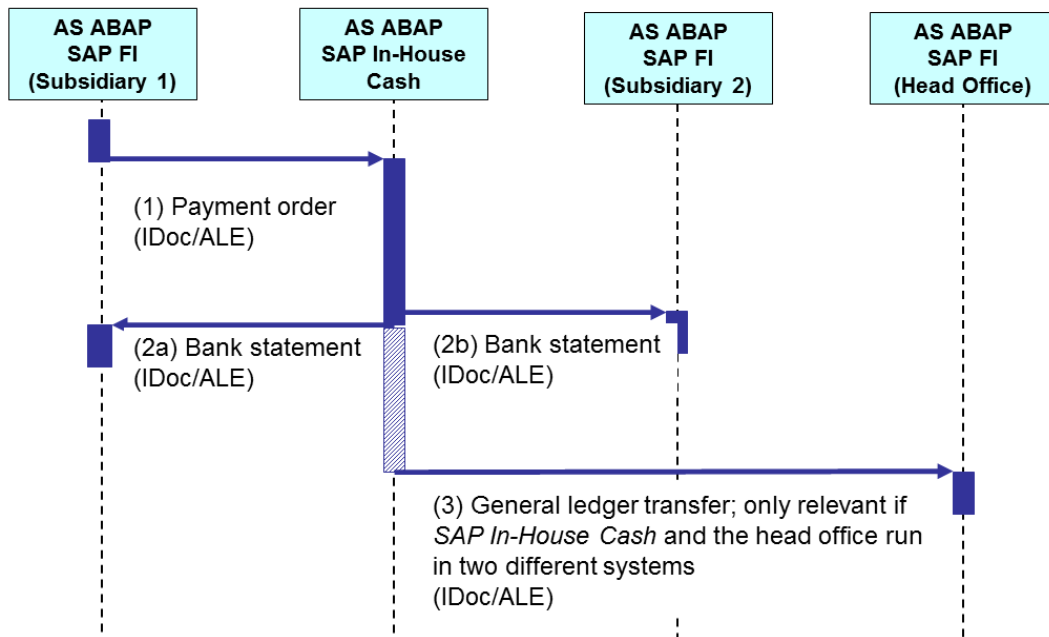
The following sections show an overview of the data flow in the processes of *SAP In-House Cash*.

#### i Note

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

#### 15.3.1.2.1.1 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.

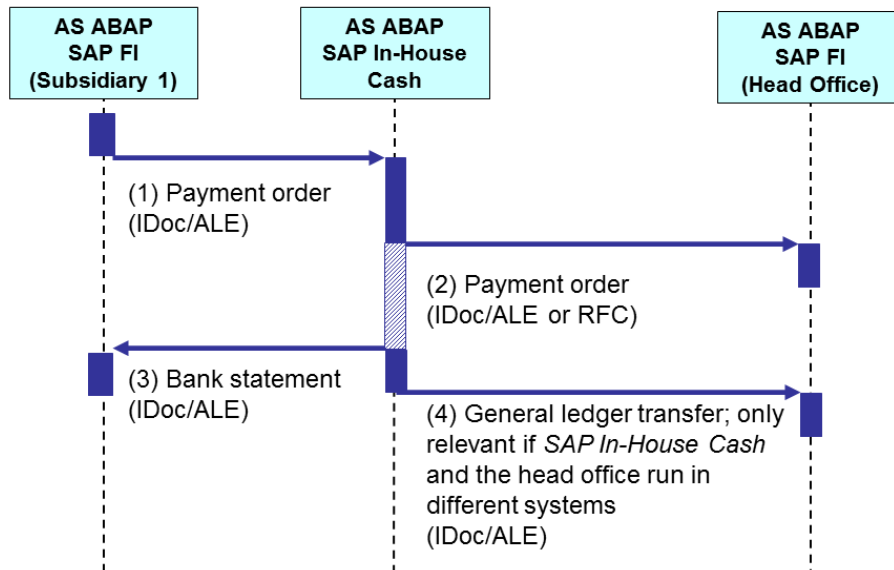


The table below shows the security aspect to be considered for the process step and what mechanism applies.

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

## 15.3.1.2.1.2 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.

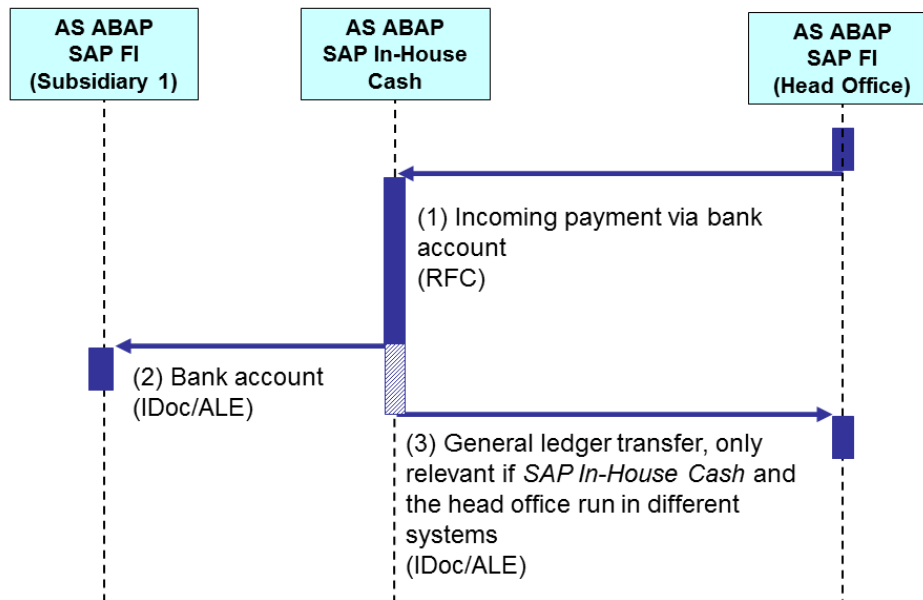
Step	Description	Security Measure
1	Payment order (IDoc/ ALE )	User type: dialog user or technical user
2	Payment order (IDoc/ ALE or RFC)	User type: dialog user or technical user
3	Bank statement (IDoc/ ALE )	User type: dialog user or technical user
4	General ledger transfer; only relevant if <i>SAP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

## i Note

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

### 15.3.1.2.1.3 Central Incoming Payments

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



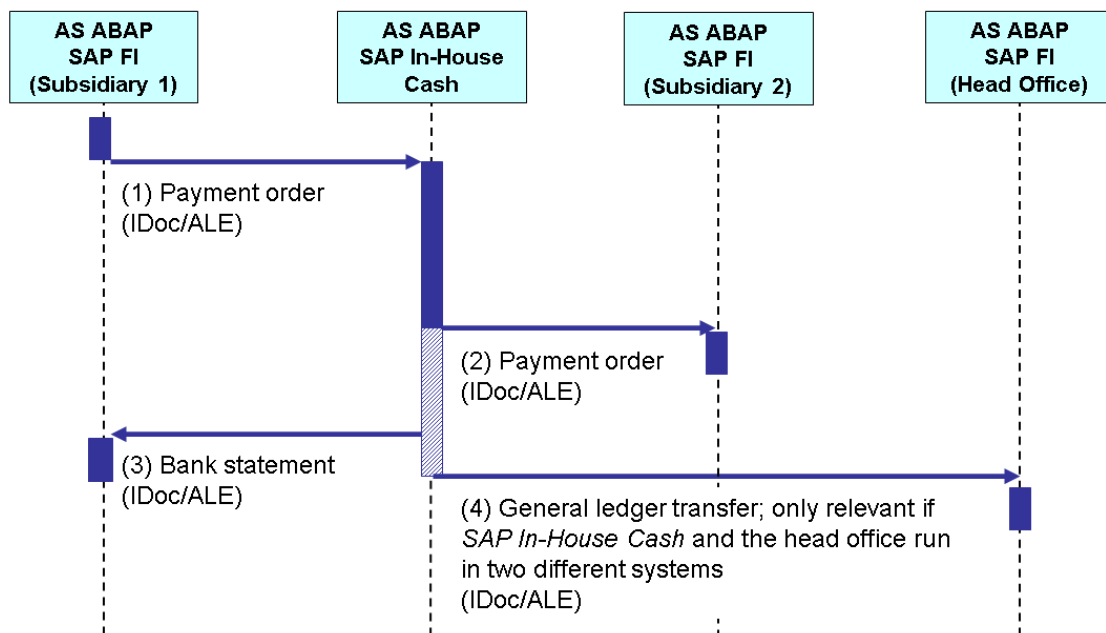
The table below shows the security aspect to be considered for the process step and what mechanism applies.

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

### 15.3.1.2.1.4 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 \[page 270\]](#) .



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

## 15.3.1.2.2 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. ▶](#)

## 15.3.1.3 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 \[page 274\]](#).

#### 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 \(ICF\) \[page 278\]](#).

#### 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 \[page 279\]](#).

### 15.3.1.3.1 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

## Standard Authorization Objects

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

Authorization Object	Permitted Activities	Description
B_BUPA_RLT	<ul style="list-style-type: none"> <li>01 Create or generate</li> <li>02 Change</li> <li>03 Display</li> </ul>	With this authorization object, you define which BP roles can be edited.
B_BUPA_GRP	<ul style="list-style-type: none"> <li>01 Create or generate</li> <li>02 Change</li> <li>03 Display</li> <li>06 Delete</li> </ul>	With this authorization object, you define which business partners can be edited on the basis of the authorization group.
B_BUPR_BZT	<ul style="list-style-type: none"> <li>01 Create or generate</li> <li>02 Change</li> <li>03 Display</li> <li>06 Delete</li> </ul>	With this authorization object, you establish which relationship categories can be processed.
CA_POWL	Not applicable	With this authorization object, you define the authorizations for the Personal Object Worklist (POWL) iViews.
F_BNKA_MAN	<ul style="list-style-type: none"> <li>01 Create or generate</li> <li>02 Change</li> <li>03 Display</li> <li>08 Display change documents</li> <li>11 Change number range status</li> </ul>	This object controls the authorizations for maintaining bank master data.

F_CLM_BAM	<ul style="list-style-type: none"> <li>• 01 Create or generate: Create new bank account master records</li> <li>• 02 Change: Change bank account master records</li> <li>• 03 Display: Display bank account master records</li> <li>• 06 Delete: Delete inactive bank account master records</li> <li>• 31 Confirm: Review bank account master records</li> <li>• 69 Discard: Close bank accounts</li> </ul>	<p>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.</p>
F_CLM_BAH2	<ul style="list-style-type: none"> <li>• 01 Create or generate</li> <li>• 02 Change</li> <li>• 03 Display</li> <li>• 06 Delete</li> </ul>	<p>This authorization object is used for controlling the authorizations of bank hierarchy and bank account group maintenance.</p>
F_CLM_UP	<p>01 Create or generate: Create or update bank account master data</p>	<p>This authorization object controls the authorization of using the <i>Import and Export Bank Accounts</i> tool to create or update bank account master data by importing bank accounts from an XML file.</p>
F_FEBS_BUK	<ul style="list-style-type: none"> <li>• 01 Create or generate</li> <li>• 02 Change</li> <li>• 03 Display</li> </ul>	<p>This authorization object controls the authorizations for maintaining bank statements in a company code. The permitted activities of this object include Create, Change, and Display. A user who would like to display Bank Statement reports using SAP Cash Management should have Bank Statement display authorization. This authorization object is assigned to the standard role Cash Manager by default.</p>
<p>F_FDES_BUK Cash Management and Forecast: Company Code Memo Records</p>	<ul style="list-style-type: none"> <li>• 01 Create or generate</li> <li>• 02 Change</li> <li>• 03 Display</li> </ul>	<p>With this authorization object, you can check the authorizations to maintain Cash Management and Forecast payment advices and planned items in a company code.</p>
<p>F_FDES_GSB Cash Management and Forecast: Business Area Memo Records</p>	<ul style="list-style-type: none"> <li>• 01 Create or generate</li> <li>• 02 Change</li> <li>• 03 Display</li> </ul>	<p>With this authorization object, you can check the authorizations to maintain Cash Management and Forecast payment advices and planned items in a business area.</p>

F_LFA1_BUK	<ul style="list-style-type: none"> <li>• 01 Create or generate</li> <li>• 02 Change</li> <li>• 03 Display</li> <li>• 05 Lock</li> <li>• 06 Delete</li> <li>• 08 Display change documents</li> <li>• C8 Confirm change</li> </ul>	With this authorization object, you can specify which activities are allowed in the company code-dependent area of the vendor master record.
S_ALM_ROLE	<ul style="list-style-type: none"> <li>• 02 Change</li> <li>• 03 Display</li> </ul>	Whenever a user tries to manipulate or to display the alerts of another user, the corresponding activities of authorization object S_ALM_ROLE are checked.
S_OC_SEND	Not applicable	With this authorization object, you define the communication method for incoming and outgoing communication, as well as the maximum number of recipients.
S_START	Not applicable	This authorization object is used during the start authorization check for particular TADIR objects, such as Web Dynpro applications.
S_TCODE	Not applicable	Whenever a transaction is started, the kernel uses the transaction code as the value to check against the authorization object.
S_USER_AGR Authorization: Role Check	<ul style="list-style-type: none"> <li>• 01 Create or generate</li> <li>• 02 Change</li> <li>• 03 Display</li> <li>• 06 Delete</li> <li>• 08 Display change documents</li> <li>• 21 Transport</li> <li>• 22 Enter, Include, Assign</li> <li>• 36 Extended maintenance</li> <li>• 59 Distribute</li> <li>• 64 Generate</li> <li>• 68 Model</li> <li>• 78 Assign</li> <li>• 79 Assign Role to Composite Role</li> <li>• Download</li> <li>• Upload</li> </ul>	This authorization object is used to protect the roles. Roles are used to combine users into groups and to assign them different attributes, in particular transactions and authorization profiles.

S\_WF\_WI

Not applicable

With this authorization object, you can check whether certain actions can be performed on specific work items.

---

## 15.3.1.3.2 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
- 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 **SIICF** 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.

### 15.3.1.3.3 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.

## 15.3.1.4 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 \[page 280\]](#) section.
- [Using Logical Path and Filenames to Protect Access to the File System \[page 302\]](#)

- **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.

### 15.3.1.4.1 Authorizations

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

The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction `PF03`) on the AS ABAP.

#### i Note

For more information about how to create roles, see *Role Maintenance*.

### Standard Roles

The table below shows the standard roles that are used by the *SAP Treasury and Risk Management*.

Standard Roles

Role	Description
SAP_TRM_ADMINISTRATOR	Treasury Administrator
SAP_TRM_DEALER	Trader
SAP_TRM_LIMIT_MANAGER	Limit Manager



Role	Description
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 <i>Treasury</i> 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)).
SAP_AUDITOR_TAX_TR (AIS Audit Information System Transaction Role)	Provides the collection, structuring, and presetting of evaluations in <i>Treasury</i> 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
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 TRM/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 TRM/Banking Analysis (e.g. evaluation type, scenario, portfolio hierarchy).
T_POS_ASS Assign Attributes to Positions	01 Create or generate 02 Change 03 Display	<p>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.</p> <p>You can control the authorization for each Accounting code, valuation area, and product type.</p> <p>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.</p>
FTR_COEX Authorization Object for Commodity Price Exposures	03 Display	The authorization object controls which activities are permitted for commodity exposures.

Authorization Object	Permitted Activities	Description
T_HREL_AUT Authorization for Hedging Relationship (P-HA)	01 Create or generate 02 Change 03 Display 06 Delete 43 Release 91 Reactivate 98 Mark for release	With this authorization object, you determine which activities are allowed for a hedging relationship within <i>Hedge Accounting for Positions</i> (P-HA) in a company code and valuation area.  Use in function:  Manage Hedging Relationships (transaction TPM100)
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: <ul style="list-style-type: none"> <li>• Trade Repository Monitor (transaction FTR_TARO_MONITOR)</li> <li>• Update Trade Repository Objects (transaction FTR_TARO_PROCESS)</li> <li>• Send Trade Repository Objects (transaction FTR_TARO_SEND)</li> <li>• Import Incoming Messages (transaction FTR_TARO_IMPORT)</li> <li>• Report R_TLR_TARO_STATUS_REMARK <i>Update the Status or the Text in the Field Remark of TAROs</i></li> </ul>

Authorization Object	Permitted Activities	Description
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 85Reverse 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 <i>Transaction Manager</i> (FSCM-TRM-TM) which create or maintain financial transactions including the BAPIs.
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 Intra-group transactions [within <i>Edit Intragroup Transactions</i> (transaction TRIG_IGT)].

Authorization Object	Permitted Activities	Description
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: <ul style="list-style-type: none"> <li>• TRS_SEC_ACC – Edit Securities Account</li> <li>• FWDP – Securities Account List</li> <li>• TS09 – Define Default Values</li> </ul>
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 <ul style="list-style-type: none"> <li>• T_DEAL_DP</li> <li>• T_DEAL_PF</li> <li>• T_DEAL_PD</li> </ul> Application examples: <ul style="list-style-type: none"> <li>• A trader should only be allowed to display/process department-related orders.</li> <li>• A clerk should not be allowed to display/process an employee loan.</li> </ul>
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
T_TRCO_FUT Authorization object for Commodity Futures Dialog	03 Display	Authorization object for displaying Commodity Futures market data  Use in functions:  <a href="#">Commodity Curve Futures Market Data</a> (transaction TPM_TRCO_FUTMD)

Authorization Object	Permitted Activities	Description
T_TRCO_FWD Authorization object for Commodity Forward data	01 Create or generate 02 Change 03 Display 06 Delete	Authorization object for maintaining the commodity forward market data dialog. Use in functions: <a href="#">Enter Commodity Forward Market Data</a> (transaction TPM_TRCO_FWDMD)
T_TRCO_CTY Authorization object for Commodity master data	01 Create or generate 02 Change 03 Display 06 Delete	Authorization for maintaining the Commodity master data information Use in functions <ul style="list-style-type: none"> <li>• BAPIs for BUS5120 Commodity-MasterData</li> <li>• Maintain Commodity Master Data (transaction FCZZ)</li> <li>• Commodity Overview (transaction TPM_CTY11)</li> </ul>
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: <a href="#">Transaction Manager</a> > <a href="#">Securities</a> > <a href="#">Trading</a> > <a href="#">Security Right</a> > <a href="#">Exercise / Reverse</a> >).

Authorization Object	Permitted Activities	Description
T_BP_USED Business Partner: Authorization for Where-Used List		<p>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.</p> <p>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.</p>
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.
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.

Authorization Object	Permitted Activities	Description
<p>T_RMCHAR_V</p> <p>Characteristic Values in Risk Management Reports</p>		<p>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.</p> <p>Defined fields</p> <ul style="list-style-type: none"> <li>• Report Category <p>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.</p> </li> <li>• Characteristic</li> <li>• Value <p>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.</p> <p>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.</p> </li> </ul>



Authorization Object	Permitted Activities	Description
T_TCC_CCUR Commodity Curve	01 Create or generate 02 Change 03 Display 06 Delete	<p>Authorization object for commodity curve maintenance</p> <p>Note:</p> <p>To edit or delete the line item data, <a href="#">Delete</a> authorization is a must.</p> <p>Use in functions</p> <ul style="list-style-type: none"> <li>• Maintain Commodity Curves (transaction TANCCMASTER)</li> <li>• Compare Commodity Curves (transaction TANCC_COMPARE)</li> </ul>
T_KAPM_1 Corporate Actions I	01 Create or generate 02 Change 03 Display 63 Activate	<p>You use this object to define the user authorizations for:</p> <ul style="list-style-type: none"> <li>• Corporate action types</li> <li>• Activities</li> </ul> <p>Use in functions</p> <p>The object T_KAPM_1 is checked in the following application functions:</p> <p>▶ <a href="#">Securities</a> ▶ <a href="#">Back Office</a> ▶ <a href="#">Corporate Actions</a> ▶ for <a href="#">Corporate action category</a>: Manually generated</p>
T_KAPM_2 Corporate Actions II	10 Post 48 Simulate 85 Reverse	<p>With this authorization object, you define at the company code level, for which corporate actions postings or simulation runs may be carried out.</p> <p>Use in functions</p> <p>Object T_KAPM_2 is checked in the following application function:</p> <p>Securities – Processing: Post other corporate actions</p>

Authorization Object	Permitted Activities	Description
T_THXE_ET Effectiveness Tests	01 Create or generate 02 Change 03 Display 06 Delete 94 Override	<p>You can use this authorization object to manage the access in the effectiveness test part of the <i>Hedge Accounting for Positions</i>.</p> <p>Use in functions:</p> <p>The system checks whether the user is authorized to execute the function based on <i>Company Code</i>, <i>Valuation Area</i>, <i>Hedging Relationship Category</i>, <i>Hedging Relationship Profile</i> and <i>Activity</i> within the following functions:</p> <ul style="list-style-type: none"> <li>• <i>Manage Hedging Relationships</i> (transaction TPM100)</li> <li>• <i>Run Effectiveness Test</i> (transaction TPM110)</li> </ul>
T_TREA_EVA Execute or Display Evaluation Data on External Accounts	01 Create or generate 03 Display	<p>With this authorization object, you determine which activities for evaluations on external accounts can be performed by which users.</p> <p>Use in functions:</p> <ul style="list-style-type: none"> <li>• NPV Calculation for External Account Transactions (transaction: TREA_EVAL)</li> <li>• Show Results of Key Figure calculation for External Accounts (transaction: TREA_EVAL_SHOW)</li> </ul>
T_RIGHTS_D Exercise Rights for Listed Options or Futures	03 Display 38 Perform 48 Simulate 85 Reverse	

Authorization Object	Permitted Activities	Description
TEM_ANALYZ	01 Create or generate	<p>You can use this authorization object in <a href="#">Exposure Management 1.0</a> for analyzing exposures.</p> <p>Use in functions:</p> <p>When the following function are called, the system checks whether the user is authorized to execute the function based on the exposure planning profile and the activity:</p> <ul style="list-style-type: none"> <li>• Maintain Exposure Planning Profile (transaction TEM1)</li> <li>• Execute Exposure Analysis (transaction TEM20)</li> <li>• Generate Version (transaction TEM15)</li> <li>• Versions Display (transaction TEM19)</li> </ul>
ExpMgt: Analysis Process: Png Profile, Version and Analysis	02 Change	
	03 Display	
	06 Delete	
TEM_EXPOS	01 Create or generate	<p>You can use this authorization object in <a href="#">Exposure Management 1.0</a> for analyzing exposures.</p> <p>Use in functions:</p> <p>When the following function are called, the system checks whether the user is authorized to execute the function based on Exposure Origin, Activity, Company code, Country and Transaction category:</p> <ul style="list-style-type: none"> <li>• Maintain Raw Exposures (transaction TEM10)</li> <li>• Display Raw Exposures (transaction TEM11)</li> <li>• Generate Version (transaction TEM15)</li> </ul>
Exposure Management: Raw Exposure Maintenance	02 Change	
	03 Display	
	06 Delete	

Authorization Object	Permitted Activities	Description
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 <i>Exposure Management 2.0</i> .
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: <ul style="list-style-type: none"> <li>Maintain External Accounts (transaction TREA_ACC_MNT)</li> <li>Create Net Payment (transaction TREA_PAY)</li> </ul>
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: <ul style="list-style-type: none"> <li>Maintain External Account Statements (transaction TREA_STA_MNT)</li> <li>Upload External Account Statements (transaction TREA_STA_UPL)</li> <li>Release Line Items (transaction TREA_RELEASE)</li> </ul>

Authorization Object	Permitted Activities	Description
T_BP_DEAL	01 Create or generate	<p>The system checks against the authorization object <i>Treasury Business Partner: Standing Instructions</i> when the user calls up the standing instructions function. The system only displays the standing instructions for which the user is authorized.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
FS Business Partner: Standing Instructions	02 Change	
	03 Display	

Authorization Object	Permitted Activities	Description
T_FGDT_ART	01 Create or generate	<p>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.</p> <p>Note:</p> <p>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.</p> <p>Procedure</p> <p>If you want to use this authorization object, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Decide for which fields in the generic transaction you want to assign authorizations.</li> <li>• In the Customizing for the generic transaction, create an authorization type for these fields.</li> <li>• 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.</li> <li>• Assign the authorizations you have created to the selected employees by using the relevant profile.</li> </ul>
Generic Transaction: Authorization Types	02 Change	
	03 Display	
T_HM_BUK	01 Create or generate	<p>Authorization object for the functions of hedge accounting (E-HA) in the company code.</p>
Hedge Accounting (E-HA) in Company Code	02 Change	
	03 Display	
	06 Delete	

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_VTBLLR 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	
F_T_VTBMA Master Agreement	01 Create or generate 02 Change 03 Display	With this authorization object, you define which master agreements can be edited.
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 <code>FWZZ</code> )

Authorization Object	Permitted Activities	Description
T_DEAL_PF	01 Create or generate	With this authorization object, you determine which functions and activities are allowed for a portfolio in a company code.
Portfolio Authorization	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	



Authorization Object	Permitted Activities	Description
T_PACC_POS Position in Futures Account	10 Post 85 Reverse	<p>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.</p> <p>You use the authorization object for the following transactions or functions:</p> <ul style="list-style-type: none"> <li>• Post Variation Margin: Function A, Activity 10</li> <li>• Post Close Margin: Function A, Activity 10</li> <li>• Reverse Margin Flows: Function A, Activity 85</li> <li>• Manual Posting: Function B, Activity 10</li> <li>• Reverse Manual Posting: Function B, Activity 85</li> <li>• Execute Matching: Function C, Activity 10</li> <li>• Reverse Matching: Function C, Activity 85</li> </ul>
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	<p>The authorization object controls, which activities are allowed for raw exposures within <a href="#">Exposure Management 2.0</a>.</p>

Authorization Object	Permitted Activities	Description
T_RDB_CVKE Results Database: Characteristic Value and Key Figure		<p>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.</p> <p>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).</p>
T_RDB_RDEL Results Database: Delete Single Records		<p>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.</p>
F_TR_MRM_S Scenario Maintenance	01 Create or generate 02 Change 03 Display 06 Delete	<p>Object F_TR_MRM_S (<i>Scenario maintenance</i>) 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.</p>

Authorization Object	Permitted Activities	Description
T_DEPOT	01 Create or generate	<p>With this authorization object, you define which position-changing measures may be carried out for the following:</p> <ul style="list-style-type: none"> <li>• company code</li> <li>• product category</li> <li>• securities account</li> </ul> <p>Defined fields</p> <ul style="list-style-type: none"> <li>• Company code</li> <li>• Product type</li> <li>• Function (D4= Disposition block, D5= securities account transfer, D6= securities account cash flow)</li> <li>• Securities account</li> <li>• Activity (create, change, display, delete, reverse)</li> </ul> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>i Note</b></p> <ul style="list-style-type: none"> <li>• Necessary authorization for <i>Unblock: 06 (delete)</i></li> <li>• Necessary authorization for <i>Manual posting or debit position:</i> <ul style="list-style-type: none"> <li>◦ Function: Securities account cash flow (D6)</li> <li>◦ Activity: change (02)</li> </ul> </li> <li>• Necessary authorization for <i>Update securities account position</i> <ul style="list-style-type: none"> <li>◦ Function: Securities account cash flow (D6)</li> <li>◦ Activity: change (02)</li> </ul> </li> </ul> </div> <p>Use in functions</p> <p>Object T_DEPOT is checked in the following functions:</p> <ul style="list-style-type: none"> <li>• Securities account transfer</li> <li>• Securities account position overview</li> <li>• Manual posting</li> <li>• Debit position</li> <li>• Reversal of debit position / manual posting</li> </ul>
Securities Account Position	02 Change	
	03 Display	
	06 Delete	

Authorization Object	Permitted Activities	Description
		<ul style="list-style-type: none"> <li>• Update securities account position</li> <li>• Posting journal</li> </ul>
T_SEC_PRIC Security Price Maintenance – Price Type	<ul style="list-style-type: none"> <li>• 03 Display Display Security Price</li> <li>• 23 Maintain Create/Change/Delete Security Prices</li> </ul>	<p>With this authorization object you can control, for which price types a user has the authorization to display or maintain security prices.</p> <p>Defined fields</p> <p>The authorization object has the following fields:</p> <ul style="list-style-type: none"> <li>• S_KURSART Rate/Price Type – Treasury Instruments</li> <li>• ACTVT Activity (Display, Maintain) Use When you have activated the security price check in the customizing under <a href="#">Treasury and Risk Management &gt; Transaction Manager &gt; General Settings &gt; Organization &gt; Activate Authority Check for Security Price Type</a> the authorization object T_SEC_PRIC is checked in the following functions: <ul style="list-style-type: none"> <li>◦ Display security price (transaction FW17)</li> <li>◦ Maintain security price (transaction FW18)</li> <li>◦ Class Master Data (transaction FWZZ)</li> </ul> </li> </ul>
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 <i>SAP Treasury and Risk Management</i> .
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: <ul style="list-style-type: none"> <li>Maintain External Accounts (transaction TREA_ACC_MNT)</li> <li>Create Net Payment (transaction TREA_PAY)</li> </ul>
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: <ul style="list-style-type: none"> <li>Maintain External Account Statements (transaction TREA_STA_MNT)</li> <li>Upload External Account Statements (transaction TREA_STA_UPL)</li> <li>Release Line Items (transaction TREA_RELEASE)</li> </ul>

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	<ul style="list-style-type: none"> <li>• Create and change to bring the data into the system,</li> <li>• Lock and release, to control usability,</li> <li>• Display, to enable the user to use the function,</li> <li>• Display change documents, to enable you to display the master data changes.</li> </ul>	<p>Repetitive codes are used to simplify processing of recurring payments. Such usage is agreed between the user and the bank.</p> <p>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.</p> <p>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).</p> <p>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).</p> <p>When you display change documents you can only restrict to company code.</p>

## 15.3.1.4.2 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 MJBHF01
  - No parameters are used in this context.
  - The logical file name uses the logical file path FTRM\_AN\_BATCH\_INPUT\_ERR\_FILE.
- FTRM\_TARO\_SEND
  - Programs using this logical file name:
    - R\_TLR\_TARO\_SEND
  - No parameters are used in this context:
  - The logical file name uses the logical file path FTRM\_TARO\_SEND (this is where the send program puts the files to be sent to the repository)
- FTRM\_TARO\_IMPORT
  - Programs using this logical file name:
    - R\_TLR\_TARO\_IMPORT and R\_TLR\_TARO\_IMPORT\_REPORTS
  - No parameters are used in this context:
  - The logical file name uses the logical file path FTRM\_TARO\_IMPORT (this is where the system expects files sent by the repository)
- FTRM\_TARO\_ARCHIVE
  - Programs using this logical file name:
    - R\_TLR\_TARO\_IMPORT and R\_TLR\_TARO\_IMPORT\_REPORTS
  - No parameters are used in this context:
  - The logical file name uses the logical file path FTRM\_TARO\_ARCHIVE (this is where imported files are stored if they were successfully imported)
- FTRM\_TARO\_ERROR
  - Programs using this logical file name:
    - R\_TLR\_TARO\_IMPORT and R\_TLR\_TARO\_IMPORT\_REPORTS
  - No parameters are used in this context:
  - The logical file name uses the logical file path FTRM\_TARO\_ERROR (this is where imported files are stored if they were NOT successfully imported but caused an error)

### Activating the Validation of Logical Path and File Names

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

## 15.3.2 Financial Operations

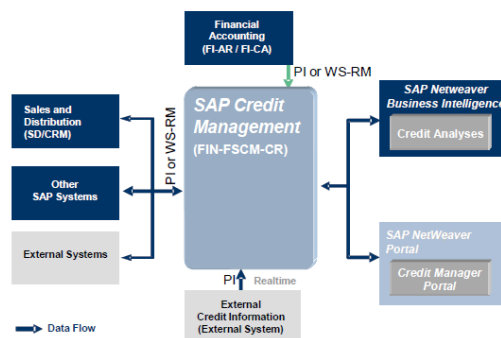
## 15.3.2.1 Receivables Management

### 15.3.2.1.1 SAP Credit Management

#### 15.3.2.1.1.1 Technical System Landscape

##### Use

This figure shows an overview of the technical system landscape for *SAP Credit Management*.



#### Technical System Landscape

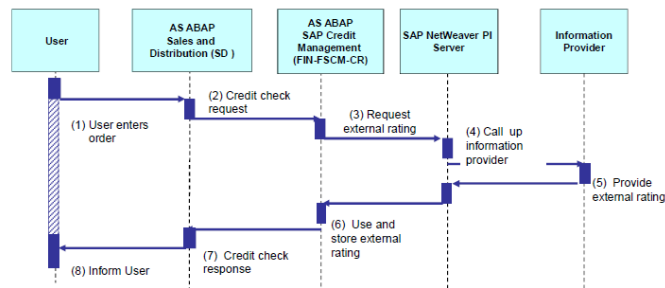
To exchange messages with external information providers, you have to use the Integration Server. For accounting systems as well as Sales and Distribution (SD) systems, you can configure the communication either via the Integration Server or via a point to point connection using Web Services Reliable 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.

## 15.3.2.1.1.2 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

## 15.3.2.1.1.3 User Management

### Standard Users

This table shows the standard users that are necessary for operating *SAP Credit Management*.

System	User ID	Type	Password	Description
<i>SAP Credit Management</i> , 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 <i>SAP Credit Management</i> and client systems using the XI channel.

You need to create this user before XI configuration. Assign both roles `SAP_FIN_FSCM_CR_USER` and `SAP_XI_IS_SERV_USER` to the user. The user and password are added to the XI channel logon data that you create when you configure your exchange server.

## 15.3.2.1.1.4 Authorizations

### Standard Roles

This table shows the standard roles that are used by *SAP Credit Management*.

Role	Description
<code>SAP_FIN_FSCM_CR_USER</code>	SAP Credit Management - Credit Analyst
<code>SAP_XI_IS_SERV_USER</code>	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	Subject	Meaning
FIN-FSCM-CR-MASS	ERROR	Logs of mass changes, can be differentiated by the severity of the error
	ERROR_BIG	
	ERROR_PROG	
	ERROR_UPD	
	INFO	
	STATISTICS	
	SUCCESS	
	WARNING	

## 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 <i>SAP Credit Management</i>	B_BUPA_RLT with the business partner role UKM000	
Display and/or delete application logs of <i>SAP Credit Management</i>	S_APPL_LOG with the object names and subobjects listed above	03
		06

## 15.3.2.1.1.5 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.

## 15.3.2.1.1.6 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.

## 15.3.2.1.1.7 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.

## 15.3.2.1.2 SAP Dispute Management

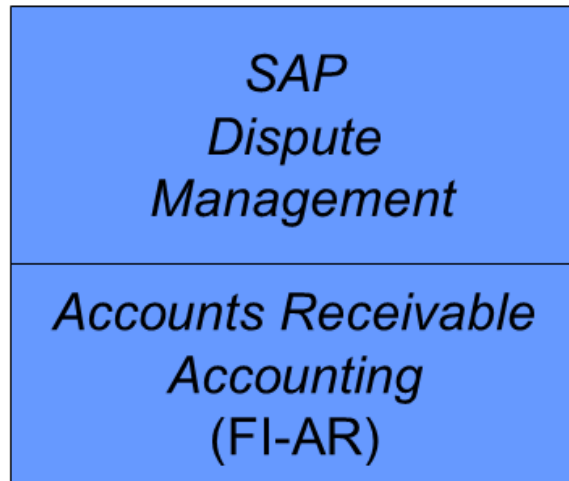
### 15.3.2.1.2.1 Technical System Landscape

#### Use

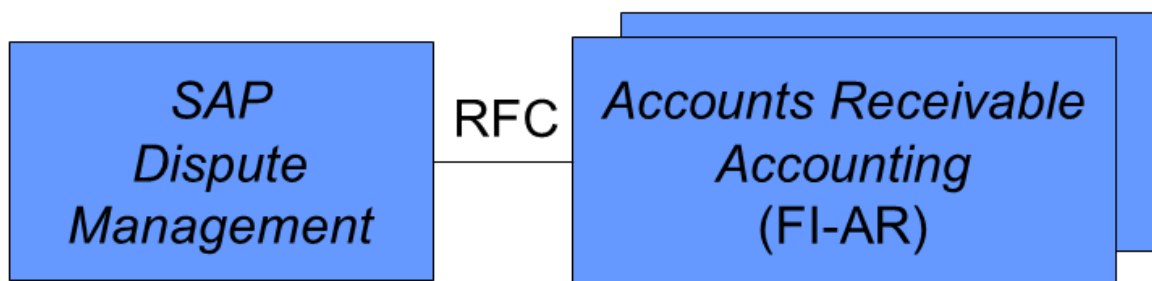
You can use *SAPDisputeManagement* as a **one-system** or as a **multiple-system scenario**. If you use *SAPDisputeManagement* in a one-system scenario, this means that you use *SAP Dispute Management* in the same system as Accounts Receivable. In a multiple-system scenario, you run *SAPDisputeManagement* 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.

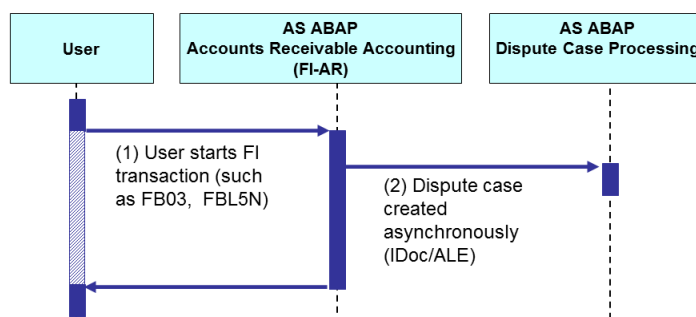
Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for <i>SAP Dispute Management</i> and the underlying components such as <i>SAP NetWeaver</i>	<i>Master Guide</i>	<a href="http://service.sap.com/instguides">http://service.sap.com/instguides</a>
High Availability	<i>High Availability for SAP Solutions</i>	<a href="http://sdn.sap.com/irj/sdn/ha">http://sdn.sap.com/irj/sdn/ha</a>

Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Design of the technical landscape	See applicable documents	<a href="http://sdn.sap.com/irj/sdn/landscape-design">http://sdn.sap.com/irj/sdn/landscape-design</a>
Security	See applicable documents	<a href="http://sdn.sap.com/irj/sdn/security">http://sdn.sap.com/irj/sdn/security</a>

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.

## 15.3.2.1.2.2 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 or FBL5N 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 <a href="#">User Management [page 315]</a> )

As already mentioned under [Technical System Landscape \[page 312\]](#) , *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.

## 15.3.2.1.2.3 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 <a href="#">SAPNetWeaver AS ABAP</a> (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: ALERE-MOTE1_COM	Communication users	The user ID and password are stored in the RFC destination for the connection.	These users are used when synchronous or asynchronous BAPI methods are called from the Accounts Receivable system in the Dispute Case Processing system.
System for Dispute Case Processing	Example: ALERE-MOTE1_DIA	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Accounts Receivable Accounting system in the Dispute Case Processing system.

System	User ID	Type	Password	Description
Accounts Receivable Accounting system	Example: ALERE-MOTE2_COM	Communication users	The user ID and password are stored in the RFC destination for the connection.	These users are used when synchronous or asynchronous BAPI methods are called from the Dispute Case Processing system in the Accounts Receivable system.
Accounts Receivable Accounting system	Example:ALERE-MOTE2_DIA	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Dispute Case Processing system in the Accounts Receivable Accounting system.

Create the users and enter them in the corresponding RFC destinations. You can assign user IDs as required. The user IDs above are merely examples.

## 15.3.2.1.2.4 Authorizations

### Standard Roles:

The table below shows the standard roles used by *SAP Dispute Management*.

Role	Description
SAP_FIN_FSCM_DM_USER	<i>FSCM Dispute Management - Processor</i>
<ul style="list-style-type: none"> <li>One-system and multiple-system scenario</li> </ul>	Contains the authorizations that an end user requires in Dispute Case Processing.
SAP_FIN_FSCM_DM_RFC_COMM	<i>RFC user (communication) in Dispute Case Processing</i>
<ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p>Contains the authorizations required by a user to call synchronous and asynchronous BAPI methods from the Accounts Receivable system in the Dispute Case Processing system.</p> <p>Examples of such methods are creating dispute cases from Accounts Receivable and automatically changing dispute cases using clearing transactions in Accounts Receivable.</p>

Role	Description
SAP_FIN_FSCM_DM_RFC_DIALOG <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (dialog) in Dispute Case Processing</i></p> <p>Contains the authorizations for a user with which the DISPLAY method is called in the Dispute Case Processing system from the Accounts Receivable system by RFC. The role contains the authorizations necessary for displaying the dispute case.</p>
SAP_FIN_FSCM_DM_AR_DIALOG <ul style="list-style-type: none"> <li>One-system scenario</li> </ul>	<p><i>Role for Functions of Accounts Receivable</i></p> <p>Contains authorizations required by end users in Dispute Case Processing so that they can call Accounts Receivable functions in Dispute Case Processing.</p> <p>Examples of such functions are including open items in a dispute case and navigating from a dispute case to a linked line item.</p>
SAP_FIN_FSCM_DM_AR_RFC_DIALOG <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (dialog) in Accounts Receivable</i></p> <p>Contains the authorizations required by a user to call <i>SAP Dispute Management</i> dialog methods using RFC from the Dispute Case Processing system in the Accounts Receivable system.</p> <p>Examples of such methods are including open items in a dispute case and navigating from a dispute case to a linked line item.</p>
SAP_FIN_FSCM_DM_AR_RFC_COMM <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (communication) in Accounts Receivable</i></p> <p>Contains the authorizations required by a user to call <i>SAP Dispute Management</i> synchronous and asynchronous BAPI methods from the Dispute Case Processing system in the Accounts Receivable system.</p> <p>Examples of such methods are the automatic write off of dispute cases and automatic notification of Accounts Receivable when confirming and voiding cases.</p>
SAP_FIN_FSCM_DM_DIALOG <ul style="list-style-type: none"> <li>One-system scenario</li> </ul>	<p><i>Role for functions of Dispute Case Processing</i></p> <p>Contains authorizations required by end users in Accounts Receivable so that they can call Dispute Case Processing functions in Accounts Receivable.</p> <p>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.</p>

Role	Description
SAP_BC_CM_ADMINISTRATOR <ul style="list-style-type: none"> <li>One-system and multiple-system scenario</li> </ul>	<i>Administrator in Case Management</i> Since the component <i>Case Management</i> represents the basis of <i>SAP Dispute Management</i> , you also require special <i>Case Management</i> authorizations when setting up <i>SAP Dispute Management</i> . These are included in this role.

### 15.3.2.1.2.5 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 <a href="#">Authorizations [page 317]</a> , 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 <a href="#">Authorizations [page 317]</a> , 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 <a href="#">Authorizations [page 317]</a> , 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 <a href="#">Authorizations [page 317]</a> , 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.

## 15.3.2.1.2.6 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 \[page 317\]](#).

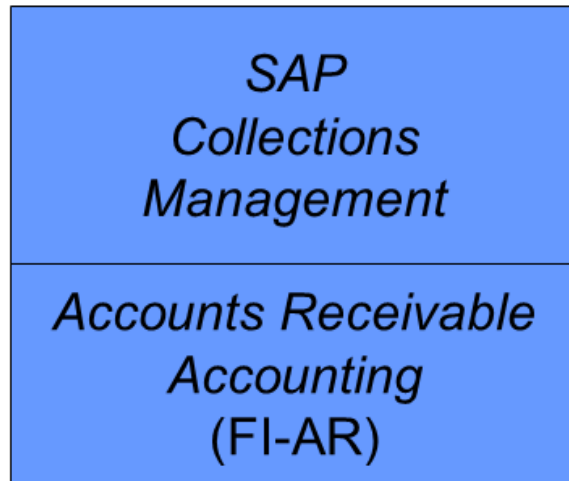
## 15.3.2.1.3 SAP Collections Management

### 15.3.2.1.3.1 Technical System Landscape

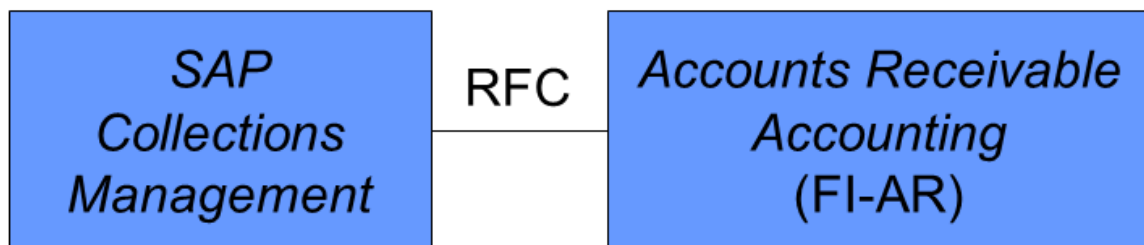
#### Use

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**:

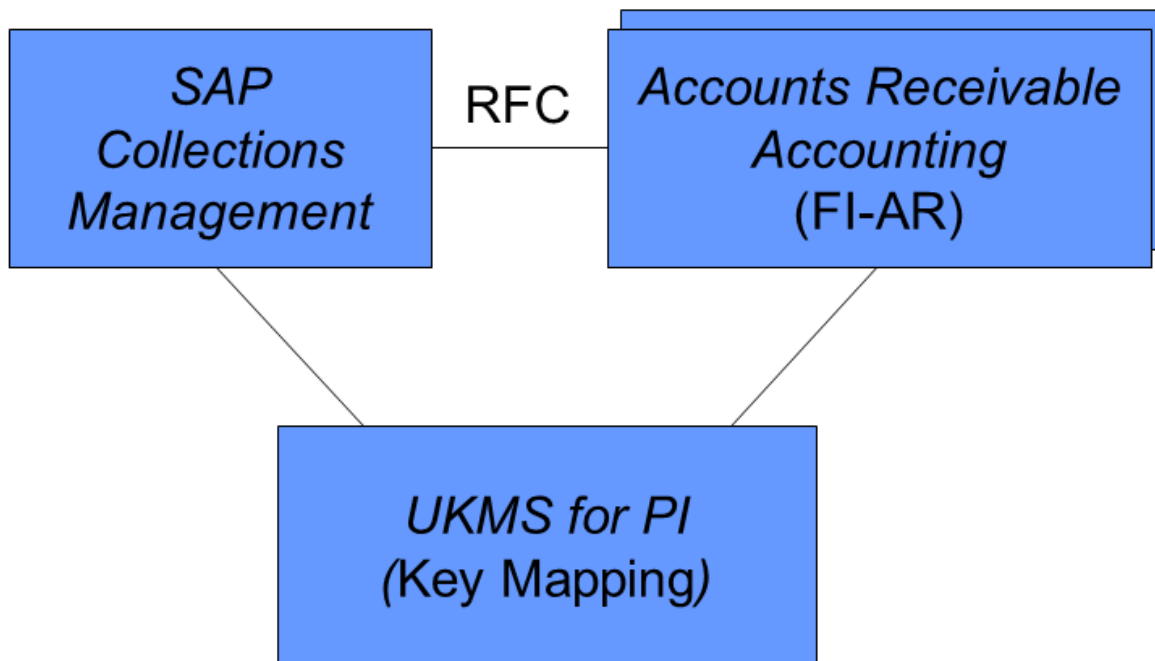


The following figure shows the technical system landscape in a **multiple-system scenario** :



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 the SAP NetWeaver 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.

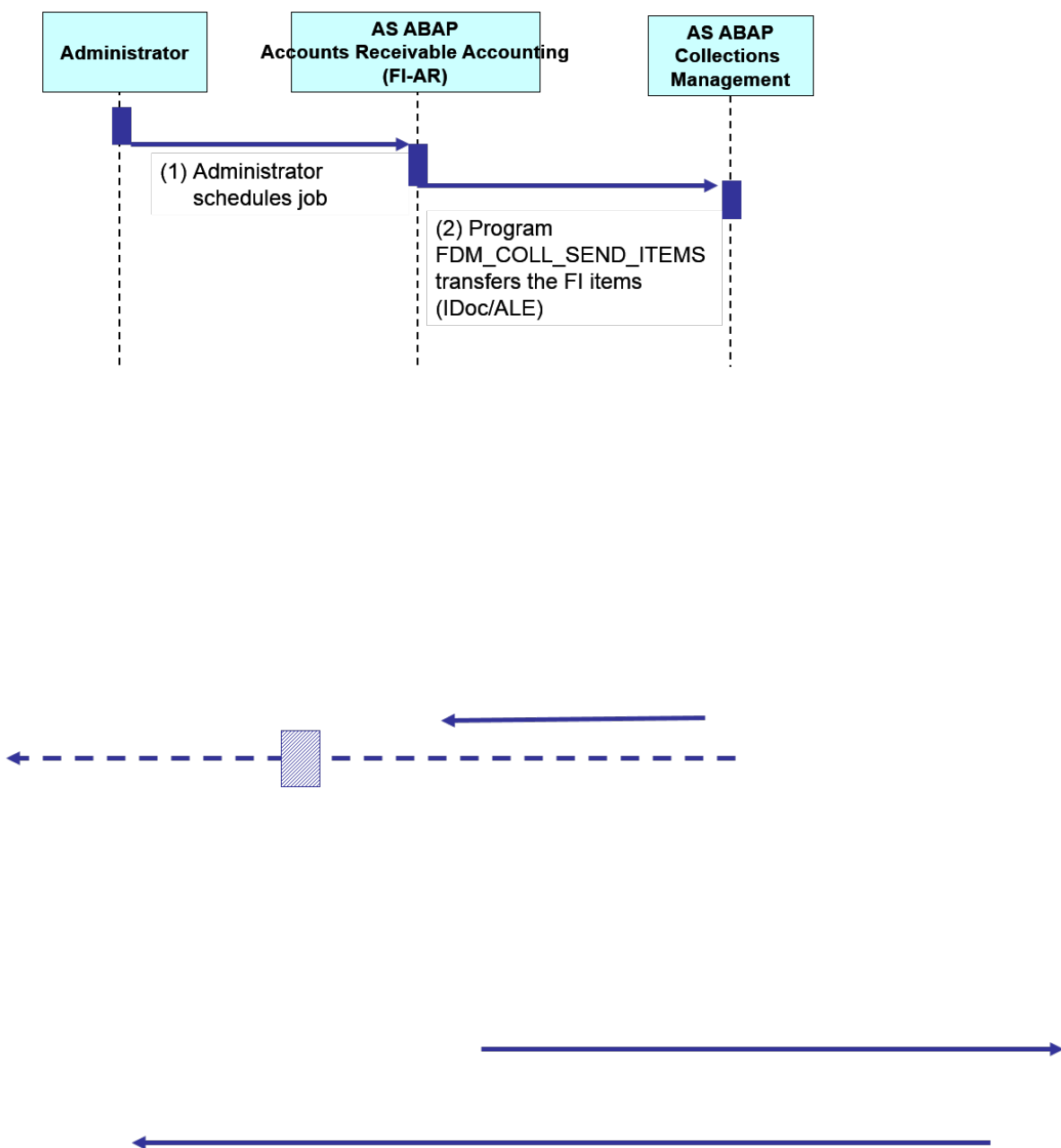
Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for <i>SAP Collections Management</i> and the underlying components such as <i>SAP NetWeaver</i>	<a href="#">Master Guide</a>	<a href="http://service.sap.com/instguides">http://service.sap.com/instguides</a>
High Availability	<a href="#">High Availability for SAP Solutions</a>	<a href="http://sdn.sap.com/irj/sdn/ha">http://sdn.sap.com/irj/sdn/ha</a>
Design of the technical landscape	See applicable documents	<a href="http://sdn.sap.com/irj/sdn/landscape-design">http://sdn.sap.com/irj/sdn/landscape-design</a>
Security	See applicable documents	<a href="http://sdn.sap.com/irj/sdn/security">http://sdn.sap.com/irj/sdn/security</a>

### 15.3.2.1.3.2 Security Aspects of Data, Data Flow and Processes

The following sections show an overview of the data flow in a multiple-system scenario.

#### 15.3.2.1.3.2.1 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.

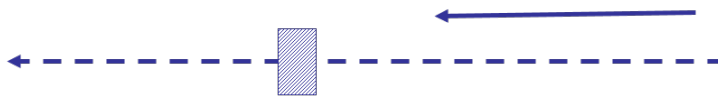
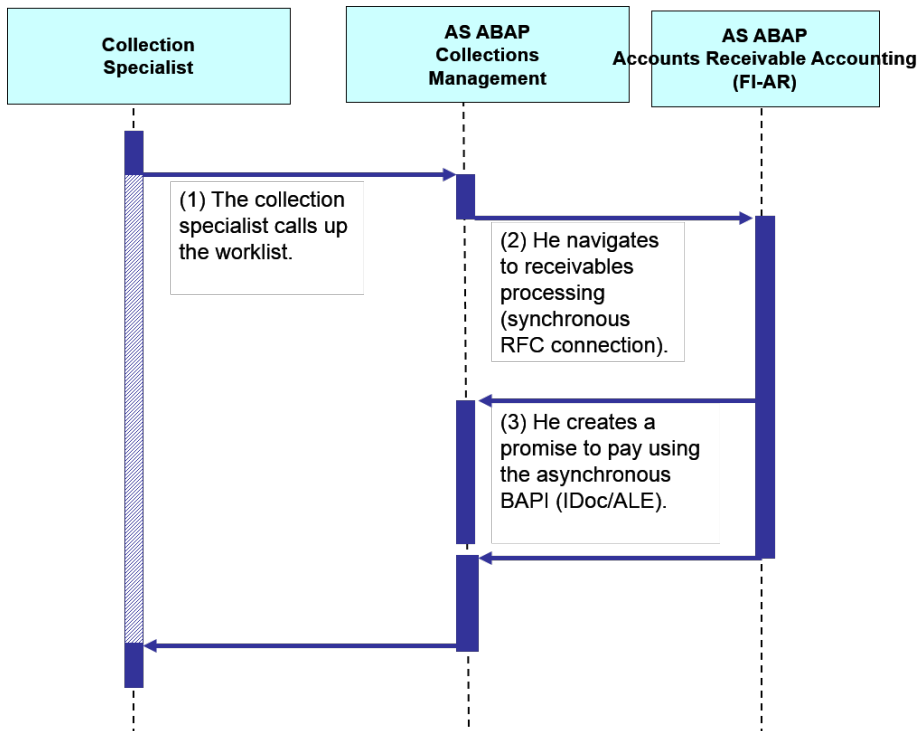


The table below shows the security aspect to be considered for the process step and what mechanism applies.

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 )

### 15.3.2.1.3.2.2 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_SPECIALIST)	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

### 15.3.2.1.3.3 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.

### 15.3.2.1.3.4 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
<p>SAP_FIN_FSCM_COL_SPECIALIST</p> <ul style="list-style-type: none"><li>One-system and multiple-system scenario</li></ul>	<p><i>Collection Specialist</i></p> <p>Contains the authorizations that the collection specialist needs to perform the activities in his task area.</p> <p>For example:</p> <ul style="list-style-type: none"><li>Calling the worklist</li><li>Displaying the business partner in <i>SAP Collections Management</i></li><li>Navigating to <i>Process Receivables</i></li><li>Creating contact persons in Collections Management</li><li>Creating promises to pay and dispute cases</li><li>Creating and changing customer contacts</li><li>Creating and changing resubmissions</li></ul>
<p>SAP_FIN_FSCM_COL_MANAGER</p> <ul style="list-style-type: none"><li>One-system and multiple-system scenario</li></ul>	<p><i>Collection Manager</i></p> <p>Contains the authorizations that the collection manager needs to perform the activities in his task area.</p> <p>In addition to all authorizations of the <i>collection specialist</i> (role SAP_FIN_FSCM_COLL_SPECIALIST), this covers the following actions, for example:</p> <ul style="list-style-type: none"><li>Definition of collection strategies</li><li>Definition of collection groups</li><li>Assignment of a strategy to a group</li><li>Change the role of the business partner specific to <i>SAP Collections Management</i></li><li>Overview of several worklists</li><li>Distribution of worklist items to the collection specialists</li></ul>

Role	Description
SAP_FIN_FSCM_COL_ADMIN <ul style="list-style-type: none"> <li>• One-system and multiple-system scenario</li> </ul>	<p><i>Collections Management Administrator</i></p> <p>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.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Worklist generation</li> <li>• Distribution of worklist items to the collection specialists</li> <li>• Mass change of the role of the business partner specific to <i>SAP Collections Management</i></li> <li>• Monitoring of parallel runs</li> <li>• Deleting Completed Resubmissions</li> </ul>
SAP_FIN_FSCM_COL_DIALOG <ul style="list-style-type: none"> <li>• One-system scenario</li> </ul>	<p><i>Role for promise to pay functions</i></p> <p>Contains authorizations required by end users in Accounts Receivable so that they can call promise to pay functions in Accounts Receivable.</p> <p>Examples are:</p> <ul style="list-style-type: none"> <li>• Creating, displaying, and changing promises to pay from receivables processing in Accounts Receivable</li> <li>• Automatic change of promises to pay as a result of clearing transactions in Accounts Receivable</li> </ul>
SAP_FIN_FSCM_COL_RFC_DIALOG <ul style="list-style-type: none"> <li>• Multiple-system scenario</li> </ul>	<p><i>RFC user (dialog) for collections management functions</i></p> <p>Contains authorizations for a user with which dialog methods are called in the <i>SAP Collections Management</i> system from the Financial Accounting system by means of RFC.</p> <p>For example, navigation from receivables processing to the detail display of the promise to pay or dispute case.</p>
SAP_FIN_FSCM_COL_RFC_COMM <ul style="list-style-type: none"> <li>• Multiple-system scenario</li> </ul>	<p><i>RFC user (communication) for collections management</i></p> <p>Contains authorizations for a user with which synchronous and asynchronous methods are called in the <i>SAP Collections Management</i> system from the Financial Accounting system.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Posting of IDocs with data from Financial Accounting</li> <li>• Creation of dispute cases, promises to pay, customer contacts, and resubmissions</li> <li>• Reading of attributes of dispute cases, promises to pay, customer contacts, and resubmissions for display in receivables processing</li> </ul>

Role	Description
SAP_FIN_FSCM_COL_AR_USER <ul style="list-style-type: none"> <li>One-system and multiple-system scenario</li> </ul>	<p><i>End user in Receivables Processing</i></p> <p>Contains the authorizations required by an end user in receivables processing in Accounts Receivable.</p> <p>This role is in the Accounts Receivable system.</p>
SAP_FIN_FSCM_COL_AR_RFC_COMM <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (communication) in Accounts Receivable</i></p> <p>Contains authorizations for a user with which synchronous and asynchronous methods are called from the <i>SAP Collections Management</i> system in the Financial Accounting system.</p> <p>An example of such a method is the automatic notification to Accounts Receivable when promises to pay are confirmed and voided.</p>
SAP_FIN_FSCM_COL_AR_ADMIN <ul style="list-style-type: none"> <li>One-system and multiple-system scenario</li> </ul>	<p><i>Collections Management Administrator Financial Accounting</i></p> <p>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.</p> <p>For example, the transfer of data relevant for <i>SAP Collections Management</i> from Accounts Receivable:</p> <ul style="list-style-type: none"> <li>Valuating promises to pay</li> <li>Automatic confirmation of promises to pay</li> </ul>
SAP_FIN_FSCM_COL_AR_RFC_DIALOG <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (dialog) in Receivables Processing</i></p> <p>Contains the authorizations for a user with which the navigate to receivables processing from the worklist by means of RFC. The authorizations permit the following activities:</p> <ul style="list-style-type: none"> <li>Display of invoice data</li> <li>Display of payment data</li> <li>Display of invoice history</li> <li>Creation, change, or display of a contact person</li> </ul>

### 15.3.2.1.3.5 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 <a href="#">Authorizations [page 328]</a> , 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 <a href="#">Authorizations [page 328]</a> , 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 <a href="#">Authorizations [page 328]</a> , 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 <a href="#">Authorizations [page 328]</a> , 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.

## 15.3.3 Contract Accounting

### 15.3.3.1 Authorizations

#### Business Roles

The following business roles are provided:

- SAP\_BR\_APR\_MANAGER\_FICA (Accounts Payable and Receivable Manager (FI-CA))
- SAP\_BR\_APR\_ACCOUNTANT\_FICA (Accounts Payable and Receivable Accountant (FI-CA))
- SAP\_BR\_INVOICING\_SPEC\_CINV (Invoicing Specialist (Convergent Invoicing))
- SAP\_BR\_INVOICING\_MANAGER\_CINV (Description: Invoicing Manager (Convergent Invoicing))

#### 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).

## 15.3.3.2 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.

### 15.3.3.3 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.

### 15.3.3.4 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.

## 15.4 Manufacturing

### 15.4.1 Maintenance Operations

#### 15.4.1.1 Authorizations in Plant Maintenance

Plant Maintenance 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 `PF03`) 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
<code>SAP_COCKPIT_EAMS_MAINT_WORKER2</code>	<i>Maintenance Worker 2</i>  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	<p data-bbox="804 371 1046 394"><i>Generic EAM Functions 2</i></p> <p data-bbox="804 423 1396 589">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.</p>

# 16 SAP S/4HANA Compatibility Packs

## 16.1 Finance

### 16.1.1 Travel Management

#### 16.1.1.1 Travel Management

##### Authorizations

Standard Roles in Travel Management (for Web Dynpro ABAP-Based Applications)

Role	Description
SAP_FI_TV_WEB_TRAVELER_2	<p><i>Traveler</i></p> <p>The role contains the authorization profile needed to execute the applications of the <i>Travel and Expenses</i> Employee Self-Service (ESS) in <i>SAP NetWeaver Portal</i>.</p>
SAP_FI_TV_WEB_TRAVELER_EXT_TP	<p><i>Traveler</i></p> <p>Users with this role can execute the work center for travelers and the corresponding applications in NWBC. NWBC calls a third-party travel planning solution instead of SAP Travel Planning.</p> <p>The role contains the authorization profile needed to execute the applications of the <i>Travel and Expenses</i> ESS in <i>SAP NetWeaver Portal</i>.</p>
SAP_FI_TV_WEB_ESS_TRAVELER_2	<p><i>ESS Single Role for Travelers</i></p> <p>Users with this role can execute the work center for travelers and the corresponding applications in NWBC.</p> <p>This role is integrated into the ESS role for Web Dynpro ABAP-based applications (<i>SAP_EMPLOYEE_ESS_WDA_1</i>).</p>

Role	Description
SAP_FI_TV_WEB_ASSISTANT_2	<p><i>Travel Assistant</i></p> <p>Users with this role can execute the work center for travel assistants and the corresponding applications in NWBC.</p> <p>The role contains the authorization profile needed to execute the applications of the <i>Travel and Expenses</i> ESS in <i>SAP NetWeaver Portal</i>.</p>
SAP_FI_TV_WEB_ESS_ASSISTANT_2	<p><i>Travel Assistant</i></p> <p>Users with this role can execute the work center for travel assistants and the corresponding applications in NWBC.</p>
SAP_FI_TV_WEB_APPROVER_2	<p><i>Approving Manager</i></p> <p>Users with this role can execute the work center for approving managers and the corresponding applications in NWBC.</p> <p>This role is integrated into the MSS role for Web Dynpro ABAP-based applications (<i>SAP_MANAGER_MSS_NWBC</i>).</p>
SAP_FI_TV_WEB_POLICY_ADMIN_2	<p><i>Travel Policy Administrator</i></p> <p>Users with this role can execute frequently used Customizing applications for policy management in NWBC.</p>
SAP_FI_TV_TIC_AGENT	<p><i>Travel Interaction Center Agent</i></p> <p>This role authorizes service agents to run the required transactions and Web Dynpro ABAP-based applications in the Travel Management system from within the Travel Interaction Center.</p> <p>The Travel Interaction Center is a Shared Services Center in <i>SAP Customer Relationship Management (SAP CRM)</i>.</p>

### Authorization Profiles

The standard system contains the travel profile FI-TV (infotype 0470 of *Human Resources Management* (HCM)). Alternatively, you can create the authorization profile by means of organizational assignment using the HR feature *TRVCP*.

### Authorization Objects

For all general functions, *Travel Management* uses the authorization object P\_TRAVL.

The transfer of results from expense reports to *accounting* is protected by the authorization object F\_TRAVL.

The travel plan status is protected by the authorization object F\_TRAVL\_S.

## Network and Communication Security

In Travel Management, you can set up connections to the following *global distribution systems* (GDS):

- [Amadeus](#)  
The partner is responsible for the Gateway.
- [Galileo](#)  
The partner is responsible for the Gateway.

Alternatively or in addition, you can use [SAP 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](#) attached to SAP Note 1414645.
- 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.

## 16.1.2 Real Estate Management

### 16.1.2.1 Real Estate Management

#### Authorizations

##### Standard Roles of Real Estate Management

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

#### Network and Communication Security

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

#### Trace and Log Files

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

#### Data Storage Security

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

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

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

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

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

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

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

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

#### **Activating the Validation of Logical Path and File Names**

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

## **16.2 R&D / Engineering**

### **16.2.1 Product Safety and Stewardship**



## 16.2.1.1 Product Compliance for Discrete Industries

### 16.2.1.1.1 User Management

The table below shows the standard users that are necessary for operating *Product Compliance for Discrete Industries*. For more generic information, see [User Management \[page 10\]](#) in the *Introduction* section.

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

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

#### i Note

Several business processes within *Product Compliance for Discrete Industries* use SAP Business Workflow and e-mail inbound and outbound processing. It is not recommended that you grant the corresponding system users (such as WF\_BATCH for Workflow System or SAPCONNECT for e-mail inbound processing) all authorizations of the system (SAP\_ALL).

### 16.2.1.1.2 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 \[page 241\]](#)
- [Roles for Managing Product Compliance for Discrete Industries \[page 347\]](#)

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.

### 16.2.1.1.2.1 Roles for Foundation Processes

Role	Description
SAP_EHSM_MASTER	Master PFCG role for <i>Product Compliance for Discrete Industries</i> . 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.
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

## 16.2.1.1.2.2 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 <i>Decide and Prepare for Assessment</i> 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.

### 16.2.1.1.3 Standard Authorization Objects

The following security-relevant authorization objects are used in *Product Compliance for Discrete Industries*:

- [Authorization Objects for Foundation Processes \[page 243\]](#)
- [Authorization Objects for Managing Product Compliance \[page 349\]](#)

- [Authorization Objects for Integration \[page 255\]](#)

### 16.2.1.1.3.1 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
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)	Activity
		02 (Change)	
		03 (Display)	
		06 (Delete)	

### 16.2.1.1.3.2 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)
	EHPRC_OLGR	See the Customizing activity <a href="#">Specify Object List Groups</a> under <a href="#">Product Safety and Stewardship</a> > <a href="#">Product Compliance for Discrete Industries</a> > <a href="#">General Configuration</a> >	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*	Web Dynpro ABAP: CHIP ID
		X-SAP-WDY- CHIP:EHPRC_CW_BCV_CHIP 1	
		EHPRCWDCHIP_SPBN	
S_PB_PAGE (ABAP Page Builder: Page Configuration)	ACTVT	03 (Display)	Activity  Needed for displaying infor- mation 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 infor- mation on the side panel
	BCV_CTXKEY	EHPRC_COMPL_DATA	Context Key
BCV_USAGE (Business Con- text Viewer usage)	ACTVT	US (Use)	Activity  Needed for displaying infor- mation on the side panel
BCV_QRYVW (Query View)	ACTVT	03 (Display)	Activity  Needed for displaying infor- mation 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 infor- mation 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 infor- mation on the side panel
	BCV_CTXKEY	EHPRC_COMPL_DATA	Context Key

## 16.2.1.1.4 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 <i>SAP Product Safety and Stewardship</i> as part of <i>SAP ERP</i> 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](#) ►.

## 16.2.1.1.5 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.

### 16.2.1.1.6 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 \[page 10\]](#) in the *Introduction* section

## 16.2.1.1.7 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 \[page 18\]](#) in the *Introduction* section.

## 16.2.1.2 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

### 16.2.1.2.1 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.

### 16.2.1.2.2 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 \[page 10\]](#) in the *Introduction* section.

### 16.2.1.2.3 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: <ul style="list-style-type: none"> <li>• Change management (character string C_AENR_*)</li> <li>• Task lists (character string C_ROUT*)</li> <li>• BOMs (character string C_STUE_*)</li> </ul>
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.

## 16.2.1.2.4 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 for Process Industries* 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 for Process Industries* are described in the following sections:

- [Communication Channel Security \[page 358\]](#)  
This topic describes the communication paths and protocols.
- [Network Security \[page 359\]](#)  
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 \[page 359\]](#)  
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

## 16.2.1.2.4.1 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:	TCP/IP DB-specific protocol	Label data	Usually no sensitive data, depending on the usage of the label.
WWI server to SQL database server			

### Note

Protect RFC connections with *Secure Network Communications* (SNC).

Use secure protocols (SSL, SNC) whenever possible.

## 16.2.1.2.4.2 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 SAP Developer Network at <http://scn.sap.com/community/security> under [Infrastructure Security](#) > [Network and Communications Security](#).

## 16.2.1.2.4.3 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
<a href="#">Basic Data and Tools</a> > <a href="#">Basic Settings</a> > <a href="#">Specify Environment Parameters</a>	No	RFC		RFC destination for <i>Business Partner</i>
Environment parameter DEST_BU				

<p>▶▶ <a href="#">Basic Data and Tools</a> &gt; <a href="#">Basic</a></p> <p><a href="#">Settings</a> &gt; <a href="#">Specify Environment</a></p> <p><a href="#">Parameters</a> ▶</p>	No	RFC	RFC destination for <a href="#">HR</a>
<p>Environment parameter DEST_HR</p>			
<p>▶▶ <a href="#">Basic Data and Tools</a> &gt; <a href="#">Basic</a></p> <p><a href="#">Settings</a> &gt; <a href="#">Specify Environment</a></p> <p><a href="#">Parameters</a> ▶</p>	No	RFC	RFC destination for <a href="#">Plant Maintenance</a>
<p>Environment parameter DEST_PM</p>			
<p>▶▶ <a href="#">Basic Data and Tools</a> &gt; <a href="#">Basic</a></p> <p><a href="#">Settings</a> &gt; <a href="#">Specify Environment</a></p> <p><a href="#">Parameters</a> ▶</p>	No	RFC	RFC destination of <a href="#">Report Shipping</a>
<p>Environment parameter DEST_SRE_DS</p>			
<p>▶▶ <a href="#">Basic Data and Tools</a> &gt; <a href="#">Basic</a></p> <p><a href="#">Settings</a> &gt; <a href="#">Specify Environment</a></p> <p><a href="#">Parameters</a> ▶</p>	No	RFC	RFC destination for <a href="#">Substance Volume Tracking</a>
<p>Environment parameter SVT_EHS_RFCDEST</p>			



<p>▶▶ <a href="#">Basic Data and Tools</a> ▶ <a href="#">Basic Settings</a> ▶ <a href="#">Specify Environment Parameters</a> ▶</p> <p>Environment parameter WWI_GENSESERVER_SYN_DEST</p>	No	RFC	Calling user	Synchronous generation of reports
<p>▶▶ <a href="#">Basic Data and Tools</a> ▶ <a href="#">Report Definition</a> ▶ <a href="#">Window Wordprocessor Integration (WWI)</a> ▶ <a href="#">Configuration of Generation PCs</a> ▶ <a href="#">Configuration of Generation Servers</a> ▶ <a href="#">Manual Configuration of Generation Servers</a> ▶ <a href="#">Specify Generation Servers</a> ▶</p> <p>Maintain the destination</p>	No	RFC	Configured Background Job user See <a href="#">Customizing activity Start WWI Dispatcher in Background</a>	Background generation of reports
<p>▶▶ <a href="#">Global Label Management</a> ▶ <a href="#">Prerequisites for Global Label Management</a> ▶ <a href="#">Define WWI Settings</a> ▶ <a href="#">Configure WWI Server for Print Request Generation</a> ▶</p>	No	RFC	Calling User	Print and preview tables in <a href="#">Global Label Management</a>

<a href="#">▶ Global Label Management ▶ Prerequisites for Global Label Management ▶ Define WWI Settings ▶ Configure WWI Server for Print Request Generation ▶</a>	No	RFC	Calling User or Configured background job user	Process print requests in <a href="#">Global Label Management</a>  See Customizing activity <a href="#">Background Jobs for Processing Print Requests</a>
<a href="#">▶ Basic Data and Tools ▶ Basic Settings ▶ Manage User Exits ▶</a>	No	RFC	Calling User	Determine secondary data for specifications with Expert
<a href="#">▶ Basic Data and Tools ▶ Basic Settings ▶ Specify Environment Parameters ▶</a>	No	RFC	Calling User	Mass change of specification data with Easy Expert

### Note

The WWI servers and the Expert servers are registering RFC servers.

For more information about setting up RFC destinations, see the Customizing for [Product Safety and Stewardship](#) under [▶ Basic Data and Tools ▶ Tools ▶ Expert ▶ Set Up RFC Destination. ▶](#)

## 16.2.1.2.5 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

## 16.2.1.2.6 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 from a PC file system, the transfer file that is stored on the application server will be overwritten.

### i Note

The transfer file of imported specification data is stored in file substance.dat on the application server. The transfer file path is configured in logical path `EHS_IMP_SUBSTANCES_PATH_2`.

## Using Logical Path and File Names to Protect Access

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

The following lists show the logical file names and paths used when importing or exporting data, and for which programs these file names and paths apply:

## Logical File Names Used in Export and Import

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

Logical File Names	Programs Using these Logical File Names
<code>EHS_EXP_PHRASES_2</code>	Export of Phrase Libraries
<code>EHS_EXP_PROPERTY_TREE_2</code>	Export of Property Tree
<code>EHS_EXP_SOURCES_2</code>	Export of Sources

EHS_EXP_SUBSTANCES_2	Export of Specification Master Data
EHS_EXP_TEMPLATE_2	Export of Report Templates
EHS_IMP_PHRASES_2	Import of Phrase Libraries
EHS_IMP_PROPERTY_TREE_2	Import of Property Tree
EHS_IMP_SOURCES_2	Import of Sources
EHS_IMP_SUBSTANCES_2	Import of Specification Master Data
EHS_IMP_TEMPLATE_2	Import of Report Templates
EHS_IMP_REPORT_2	Import of Reports
EHS_FTAPPL_2	Upload File; Download File

## Logical Path Names Used During Export and Import

These logical file names use the following logical file path:

Logical File Names	Logical Path Names
EHS_EXP_PHRASES_2	EHS_EXP_PHRASES_PATH_2
EHS_EXP_PROPERTY_TREE_2	EHS_EXP_PROPERTY_TREE_PATH_2
EHS_EXP_SOURCES_2	EHS_EXP_SOURCES_PATH_2
EHS_EXP_SUBSTANCES_2	EHS_EXP_SUBSTANCES_PATH_2
EHS_EXP_TEMPLATE_2	EHS_EXP_TEMPLATE_PATH_2
EHS_FTAPPL_2	EHS_FTAPPL_PATH_2
EHS_IMP_PHRASES_2	EHS_IMP_PHRASES_PATH_2
EHS_IMP_PROPERTY_TREE_2	EHS_IMP_PROPERTY_TREE_PATH_2
EHS_IMP_REPORT_2	EHS_IMP_REPORT_PATH_2
EHS_IMP_SOURCES_2	EHS_IMP_SOURCES_PATH_2
EHS_IMP_SUBSTANCES_2	EHS_IMP_SUBSTANCES_PATH_2
EHS_IMP_TEMPLATE_2	EHS_IMP_TEMPLATE_PATH_2

## Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log (transaction `SM19`).

Relevant audit log numbers:

- DUA – EHS-SADM: Service &A on client &B created
- DUB – EHS-SADM: Service &A on client &B started
- DUC – EHS-SADM: Service &A on client &B stopped
- DUD – EHS-SADM: Service &A on client &B stopped
- DUE – EHS-SADM: Configuration of service &A on client &B was changed
- DUF – EHS-SADM: File &A from client &B transferred
- DUG – EHS-SADM: File &A transferred to client &B

### 16.2.1.2.6.1 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.

### 16.2.1.2.7 Dispensable Functions with Impacts on Security

You can compile and display system information for Windows Wordprocessor Integration (WWI) as follows:

- You can display system information in the *WWI Monitor* (transaction `CG5Z`): In the menu, choose ► *Utilities* ► *Test Server* ▾
- In WWI.INI, under `[Global]`, enter as *DisableWwiServerInfo* the value 1. This prevents external access to the WWI system information (through the *WWI Server Monitor*, for example). The default value is 0.

### 16.2.1.2.8 Security for Additional Applications

#### Windows Authorization for Windows Wordprocessor Integration

Windows Wordprocessor Integration (WWI) requires a Windows user account that is used to run the WWI generation server services. This is because many printer settings and settings for Microsoft Word are user-specific.

As an abbreviation, the user account is called *WWI user*.

- Create a new Windows user. This user is used to execute the WWI generation server (WWI server). The user can be a local user or a domain user. We recommend creating a local user, for example, `WWI-USER`. Assign this user to the *Main users* group or the *Users* group. Use a password that does not expire.
- In Microsoft Windows Vista, in Microsoft Windows Server 2008 and higher releases, assign the WWI user to the administrators group.
- If the user is a domain user, ensure that the profile of the user is `local`.
- Check the security settings for the user that is used to execute the WWI server:
  - The user must have the *Log on as a service* authorization. In Microsoft Windows XP, Microsoft Windows Server 2003 and higher releases, also set this authorization for users of the administrators group. You can find this authorization in the Control Panel under ► *Administrative Tools* ► *Local Security Policy* ▾. Navigate to ► *Local Policies* ► *User Rights Assignment* ▾. Here, you assign the user privileges to the guideline *Log on as a service*.
  - Check the `DCOM` start authorization and access authorization for Microsoft Word using the `DCOMCNFG.EXE` configuration program. For more information, see the SAP Note [580607](#) 📄.

- Ensure that the user has write (change) authorization for the WWI root directory. We recommend using a local directory. The WWI work directory is configured in the [Specify Generation Servers](#) Customizing activity.
- Make sure that the Microsoft Windows TEMP directory exists. The TEMP directory is configured in Microsoft Windows under **▶ Control Panel ▶ System ▶ Advanced ▶ Environment Variables ▶**. There, check the user variables and system variables TMP and TEMP.
- Ensure that the user has write (change) authorization for the Microsoft Windows TEMP directory.

For further information, see SAP Note [580586](#).

## Windows Authorization for Expert

The Expert server service is run as a local system account.

## Windows Authorization for Administration Management Server

The Administration Management Server service is run as a local system account.

### 16.2.1.2.9 Security-Relevant Logging and Tracing

Windows Wordprocessor Integration (WWI) and Expert log all processing information in the Windows Application Event Log. A separate Security Log for WWI and Expert does not exist. For security relevant information from Windows, check the Windows Security Event Log.

For more information on maintaining a secure environment in Windows servers, check the [Microsoft Windows Security Guide](#) and the [Microsoft Security Compliance Manager](#).

## Tracking Configuration Changes

To track configuration changes of WWI and Expert Server Administration that are executed by [WWI and Expert Server Administration](#) (transaction `CGSADM`), enable the security audit log in the [Security Audit](#) (transaction `SM19`).

Relevant audit log numbers:

- DUA – EHS-SADM: Service &A on client &B created
- DUB – EHS-SADM: Service &A on client &B started
- DUC – EHS-SADM: Service &A on client &B stopped
- DUD – EHS-SADM: Service &A on client &B stopped
- DUE – EHS-SADM: Configuration of service &A on client &B was changed
- DUF – EHS-SADM: File &A from client &B transferred



- DUG – EHS-SADM: File &A transferred to client &B

For more information on configuration changes, change documents are used. Creating change documents in *WWI and Expert Server Administration* is enabled by default. To switch off the creation of change documents, set the environment parameter `CGSADM_NO_CHANGE_DOCS` in the *Specify Environment Parameters* Customizing activity to **X**.

To display change documents, start the program `RSSCD110` (Display change documents (cross-client)) and choose object class `ESSADM`.

## Tracking Configuration with Windows Features

To track WWI and Expert configuration changes, enable auditing in the Windows file system. For more information on Access Control and Security Auditing, see the Windows Help.

Before setting up auditing for files and folders, enable object access auditing by defining auditing policy settings for the object access event category.

To define or modify auditing policy settings for an event category for your local computer, proceed as follows:

1. Choose ► *Control Panel* ► *Administrative Tools* ► *Local Security Policy*. ►
2. In the console tree, go to ► *Local Policies* ► *Audit Policy*. ►
3. In the results pane, choose *Audit object access* to enable the auditing policy settings.

To configure auditing settings for a local file or folder, proceed as follows:

1. Open *Windows Explorer*.
2. In the context menu of the file or folder that you want to audit, choose *Properties* and go to the *Security* tab page.
3. Choose *Edit*, and then choose *Advanced*.
4. In the *Advanced Security Settings* go to the *Auditing* tab page.

To configure auditing settings for a registry key:

1. Open *Registry Editor*.
2. Go to the registry key.
3. In the context menu of the registry key that you want to audit, choose *Permissions*.
4. On the *Security* tab page, choose *Advanced*.
5. In the *Advanced Security Settings*, choose the *Auditing* tab page.

## Windows Wordprocessor Integration (WWI)

For WWI, the following files and folders must be covered by change auditing:

- `WWI.INI`
- `SAPRFC.INI`
- `GRAPHICS`
- Registry key: `HKEY_CLASSES_ROOT\WWIDOCUMENT`

## Expert

For Expert, the following files and folders must be covered by change auditing:

- SAPRFC.INI
- RULES
- Registry key: HKEY\_LOCAL\_MACHINE\SOFTWARE Wow6432Node\TechniData\EHS-AddOns  
  \Instances

For 32bit systems, omit Wow6432Node

- Registry key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\TechniData\EHS-AddOns\System



For 32bit systems, omit Wow6432Node

# 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.

© 2018 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.