



Master Guide | #UACP security level English Customer
SAP Application Interface Framework 4.0
2021-02-25

Master and Upgrade Guide for SAP Application Interface Framework

Content

1	Getting Started.	5
1.1	About this Document.	5
1.2	Useful Links.	6
1.3	Related Operations Information.	7
1.4	Important SAP Notes.	7
2	Implementation of SAP Application Interface Framework	10
2.1	SAP Application Interface Framework Licensing.	10
2.2	Software Units of SAP Application Interface Framework.	11
2.3	System Landscape.	11
2.4	Overall Implementation Sequence.	14
2.5	Media List.	15
3	Security for SAP Application Interface Framework.	16
3.1	Authorization Objects.	16
	Authorization Object for Interface Processing.	16
	Authorization Object for Customizing Steps.	17
	Authorization Object for Error Handling.	20
	Authorization Object for Technical Error Handling.	21
	Authorization Object for Emergency Corrections.	22
	Authorization Object for Custom Functions.	23
	Authorization Object for Custom Hints.	24
	Authorization Object for Interface Determination.	25
	Authorization Object for Value Mapping Maintenance.	26
	Authorization Object for File Adapter.	27
	Authorization Object for Serialization.	28
	Authorization Object for Change Log.	29
	Authorization Object for Custom Message Texts.	29
	Authorization Object for Custom Data Links.	30
	Authorization Object for AIF Persistence Messages Deletion.	32
	Authorization Object for Processor Assignment.	32
	Authorization Object for Read Access Log.	33
	Authorization Object for Read Access Log Customizing.	34
	Authorization Object for External Contacts.	35
3.2	Role Templates.	35
	AIF Administrator.	37
	AIF All Authorizations.	41

	AIF Architect.	41
	AIF Auditor.	46
	AIF Data Protection Officer.	46
	AIF Developer.	47
	AIF Power User.	51
	AIF Processing.	55
	AIF Test Template (Non-Productive).	56
	AIF Business User.	56
3.3	Set Up Interface-Specific and Key Field-Specific Authorizations.	58
3.4	Data Protection and Privacy.	59
	Glossary.	60
	Personal Data in the SAP Application Interface Framework.	61
	Limiting Access to Personal Data.	62
	Ensuring the User Consent.	63
	Providing an Information Report.	63
	Providing a Read Access Log.	64
	Providing a Change Log.	65
	Ensuring the Blocking and Deletion of Personal Data.	66
4	Upgrade of SAP Application Interface Framework.	69
5	Uninstallation of SAP Application Interface Framework.	71

Document History

Caution

Before you start the implementation, make sure that you have the latest version of this document that is available on SAP Help Portal at <http://help.sap.com/aif>.

Document Version	Date	Change
1.0	2018-04-20	First release of this Master Guide.

1 Getting Started

This section describes how to get started with SAP Application Interface Framework.

1.1 About this Document

Purpose

This Master Guide provides a central starting point for the technical implementation or upgrade of the SAP Application Interface Framework. You can find cross-scenario implementation and upgrade information as well as scenario-specific information in this guide.

In addition, this Master Guide contains security information about SAP Application Interface Framework.

Use the Master Guide to get an overview of the SAP Application Interface Framework, its software units, and its scenarios from a technical perspective. The Master Guide is a planning tool that helps you to design your system landscape. It refers you to the required detailed documentation, mainly:

- Installation instructions for single software units
- Important SAP Notes
- Configuration documentation
- Operations documentation
- Application help

The Master Guide consists of the following main sections:

- [Getting Started \[page 5\]](#)
Explains how to use this document and related information (documentation and SAP Notes) that is crucial to the installation, upgrade, configuration, operations, and security of SAP Application Interface Framework.
- [Implementation of SAP Application Interface Framework \[page 10\]](#)
Provides essential information about the supported scenarios, the installable software units, as well as how to plan your system landscape. This section provides an overall implementation sequence with related information (documentation and SAP Notes) and provides the information about how to install the SAP Application Interface Framework by referring to the relevant SAP Notes.
- [Security for SAP Application Interface Framework \[page 16\]](#)
Provides the security information that is specific to the SAP Application Interface Framework (authorization objects, roles, and so on). This section also provides a collection of links to SAP's various security topics.
- [Upgrade of SAP Application Interface Framework \[page 69\]](#)
Describes the manual efforts required to upgrade SAP Application Interface Framework from version 3.0 to version 4.0.

Constraints

- The business scenarios that are presented here serve as examples of how you can use SAP software in your company. The business scenarios are only intended as models and do not necessarily run the way they are described here in your customer-specific system landscape.
Ensure to check your requirements and systems to determine whether these scenarios can be used productively at your site. Furthermore, we recommend that you test these scenarios thoroughly in your test systems to ensure they are complete and free of errors before going live.
- This Master Guide primarily discusses the overall technical implementation, upgrade, and security of the SAP Application Interface Framework, rather than its subordinate components. This means, that additional software dependencies may exist without being mentioned explicitly in this document.

1.2 Useful Links

The following table contains links to other useful resources.

Resource	Where to Find It
User assistance for SAP Application Interface Framework	http://help.sap.com/aif
Information about creating customer incidents	http://support.sap.com/incident
SAP Notes search	http://support.sap.com/notes
SAP Software Download Center	http://support.sap.com/swdc
Product Availability Matrix	http://support.sap.com/pam
Early Knowledge Transfer and role-specific learning maps	http://support.sap.com/ekt
Sizing	https://www.sap.com/about/benchmark/sizing.html
Performance	https://www.sap.com/about/benchmark/sizing/performance.html
Information about support package stacks, latest software versions and patch level requirements	http://support.sap.com/sp-stacks
Information about Unicode technology	http://www.sdn.sap.com/irj/sdn/i18n

1.3 Related Operations Information

The SAP Application Interface Framework is based on an SAP NetWeaver 7.3 EHP1 (or higher) system. Therefore, the general operations information for the following areas is covered in the Operations Guide of SAP NetWeaver:

- Technical system landscape
- Overview of technical runtime scenarios, which result from setting up the corresponding business scenarios
- Backup and recovery
- High availability concept
- Starting and stopping (by which means and in which sequence)
- Scenario administration concept (possible dependencies between scenario components)
- Concept for data archiving and management of outdated technical data
- Software change management
- Scenario maintenance concept
- Concept for handling customer development
- Support desk management
- Troubleshooting


You can find more information about the corresponding Operations Guides for SAP NetWeaver in <http://help.sap.com/nw731> under *Operations*.

The operations information that is specific to SAP Application Interface Framework is included in the Application Help of the SAP Application Interface Framework. There, the following topics are covered:



- Data Archiving
- Data Destruction
- Performance Analysis
- Index Table Overview
- Interface Objects Summary
- Application Log Content
- Read Log and Change Log Viewers
- Data Correction
- Generation and Display of Snapshots

1.4 Important SAP Notes







You must read the following SAP Notes before you start the installation or the upgrade. These SAP Notes contain the most recent information about the installation and upgrade.







Make sure that you have the up-to-date version of each SAP Note, which you can find on SAP Support Portal at <http://support.sap.com/notes> .

Installation Notes of SAP Application Interface Framework

SAP Note Number	Title	Description
2608789 	ABAP Add-On AIF 703: Installation, upgrade, CSPs	See this note for the detailed information about installing and upgrading the component AIF 703 of SAP Application Interface Framework 4.0.
2288871 	ABAP Add-on AIFGEN 700: Installation, CSPs	See this note for the detailed information about installing the optional component AIFGEN 700 of SAP Application Interface Framework 4.0.

Relevant Notes of SAP NetWeaver

SAP Note Number	Title	Description
1930702 	CD: Generation - optional parameters	Needed to enable Change Documents for the change log functionality of SAP Application Interface Framework.
1844763 	ALE: Integration of SAP Application Interface Framework	Needed to enable IDoc monitoring with the SAP Application Interface Framework.
1828776 	AIF support in proxy inbound processing	Implement this note to enable inbound proxy monitoring with the SAP Application Interface Framework.
1989168 	Missing DB Indexes causing Performance Issues	Only needed if you configure interfaces for the Process Observer.
1994183 	Performance Improvements for metrics engine and event processing	Only needed if you configure interfaces for the Process Observer.
2009539 	Performance Improvements for Event Processing	Only needed if you configure interfaces for the Process Observer.

SAP Note Number	Title	Description
2035226 	Changing the sequence of logging entries into DB	Only needed if you configure interfaces for the Process Observer.
1684718 	WDA: Transaction WDYID – Configuration ID is lost	Only needed if you use Monitoring and Error Handling (Web) from the SAP Easy Access menu.
1726101 	Tables with more than five key elements are not supported	This note is only needed if you use the Service Implementation Workbench (SIW) template.
1705786 	SIW: Language conflict with LO-CAL packages	This note is only needed if you use the SIW template.
1698269 	SIW: Misleading error message	This note is only needed if you use the SIW template.
1718473 	SIW: Dump after leaving ungenerated project	This note is only needed if you use the SIW template.

2 Implementation of SAP Application Interface Framework

The SAP Application Interface Framework enables you to develop and monitor interfaces as well as execute error handling in a single framework residing in your SAP backend system.

Possible sources of demand for SAP Application Interface Framework are:

- You have a complex, heterogeneous system landscape
- You want to decouple technical and business aspects of your interfaces, thus enabling business users to perform error handling
- You use different technologies to implement interfaces, so you have duplicate efforts for implementing the same logic in multiple technologies
- You have to use multiple monitoring tools for different basis technologies and would like to use one tool to simplify the monitoring and error handling
- You experience difficulties in enforcing interface implementation guidelines
- You need to restrict access to interface data to fulfill your regulatory or company compliance rules

SAP Application Interface Framework enables you to:

- Implement interfaces in an easy and structured way mainly based on Customizing
- Re-use interface building blocks (checks, structure mappings, value mappings, actions, functions) inside of multiple interfaces and for different basis technologies
- Do functional instead of technical monitoring
- Restrict interface data and error monitor access by flexible authorization rules
- Enforce interface implementation guidelines

SAP Application Interface Framework provides you with the following functions:

- A powerful framework for the implementation of interfaces
- A user-friendly transaction for interface monitoring and error handling
- Tools for configuration and operations

The following chapters give an overview of the software components that are required within the SAP Application Interface Framework and its business scenarios, as well as an overview of the implementation process.

2.1 SAP Application Interface Framework Licensing

The licensing distinguishes the following basic usages of SAP Application Interface Framework:

- As stand-alone product for developing, processing and monitoring your own custom interfaces. For this usage, you need to purchase the full SAP Application Interface Framework license and have the AIFGEN software component installed in addition to the AIF component.

- As a supporting component for only processing and monitoring the AIF interfaces shipped with other SAP products, for example, SAP Advanced Track and Trace for Pharmaceuticals. For this usage, a limited runtime license of SAP Application Interface Framework is included in the licenses of the other products and AIFGEN is not required.

For more information about the SAP Application Interface Framework license check using AIFGEN, see SAP Note [2293938](#).

For more information about SAP Application Interface Framework system measurement, see [System Measurement Engine](#), measurement ID 3250.

2.2 Software Units of SAP Application Interface Framework

The following table contains the basic software units that you require to set up your SAP Application Interface Framework system landscape:

Software Unit	Component
SAP Application Interface Framework 4.0	AIF 703
SAP NetWeaver 7.3 EHP1 SPS06 or above	various

If you have purchased the full SAP Application Interface Framework license and want to develop SAP Application Interface Framework interfaces in your own custom namespaces, you require the following software unit in addition:

Software Unit	Component
Aifgen 700	AIFGEN 700

⚠ Caution

Make sure all the relevant and available support packages (SPs) and enhancement packages (EHPs) are also applied when any of the above software units are installed. For the latest component version and patch level requirements, see <http://support.sap.com/sp-stacks>.

2.3 System Landscape

The SAP Application Interface Framework offers various system landscape options depending on the customers' business requirements and possible system deployments. In the following section, exemplary system deployments are presented with the characteristics and restrictions of each case.

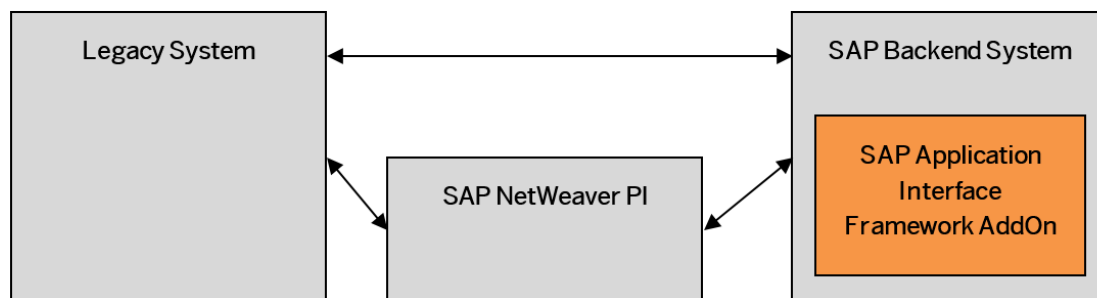
⚠ Caution

We strongly recommend that you use a minimal system landscape for test and demo purposes only. For performance, scalability, high availability, and security reasons, do not use a minimal system landscape as your production landscape.

General

The integration scenarios involve at least two systems, that is, a legacy system and an SAP backend system that contains the SAP Application Interface Framework. The integration scenarios can optionally involve an SAP NetWeaver PI. The legacy system can be any system that is able to exchange information directly with the SAP backend system or with the SAP NetWeaver PI system.

For any integration scenario you are using, you need to make sure that the systems you want to connect are capable of handling the chosen interface technology.



In your business processes, the legacy system can act as sender or receiver of information.

As a sender, the legacy system is the data source and sends data directly to the SAP backend system or to the SAP NetWeaver PI system.

If you choose to use direct integration between the legacy system and the SAP backend system, data is sent directly from the legacy system to the SAP backend system.

If you choose to use SAP NetWeaver PI for integration, SAP NetWeaver PI can act as the information broker, provide security features, and offer many other technical integration capabilities. Here, the technical mapping of the data structures or technical format conversions (for example, using existing adapters) can be executed. If the communication channel in your SAP NetWeaver PI is correctly configured, the message is sent to your SAP backend system. The SAP Application Interface Framework resides within the SAP backend system and provides different additional features depending on the chosen integration scenario.

If data is sent through the SAP NetWeaver PI system, you have the option to use different interface technologies for communication between the legacy system and SAP NetWeaver PI and between SAP NetWeaver PI and the SAP backend system. In this case, a technical format conversion needs to be done in SAP NetWeaver PI to translate from one interface technology to the other.

In both scenarios, the SAP Application Interface Framework in the SAP backend system provides the monitoring and error handling functionality.

Note

Note that the interface setting, mapping, interface variants, and error handling settings in the SAP Application Interface Framework are client-dependent. You have to make sure that message processing and error handling is executed in the correct client.

As a receiver, the legacy system is the consumer of information sent by the SAP backend system using the SAP Application Interface Framework. When triggered manually or by an application, the SAP Application Interface Framework executes the mapping from the internal to the external structure and sends the information in the external format directly to the legacy system or to SAP NetWeaver PI.

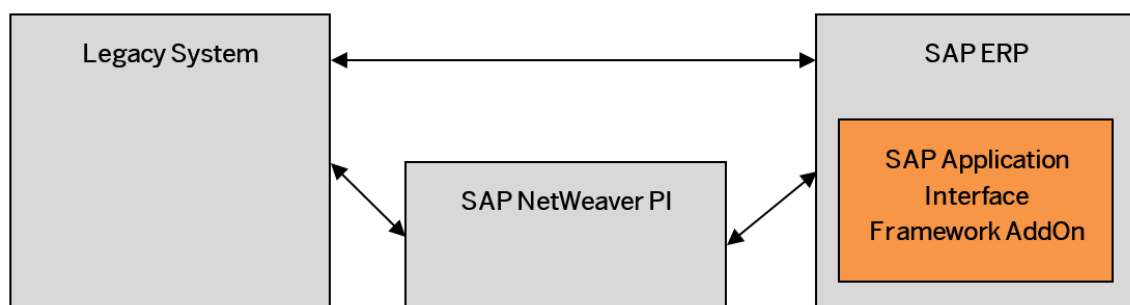
If you choose to use direct integration between the SAP backend system and the legacy system, data is sent directly from the SAP backend system to the legacy system.

If you choose to use SAP NetWeaver PI for integration, SAP NetWeaver PI can act as the information broker, provide security features, and offer many other technical integration capabilities. Here, the technical mapping of the data structures or technical format conversions (for example, using existing adapters) can be executed. If the communication channel in your SAP NetWeaver PI is correctly configured, the message is sent to the legacy system.

If data is sent through the SAP NetWeaver PI system, you have the option to use different interface technologies for communication between the SAP backend system and SAP NetWeaver PI and between SAP NetWeaver PI and the legacy system. In this case, a technical format conversion needs to be done in SAP NetWeaver PI to translate from one interface technology to the other.

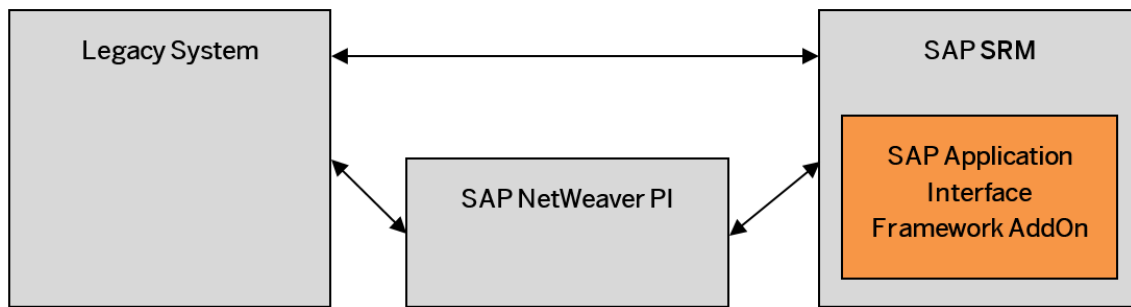
Example 1: SAP Application Interface Framework installed on SAP ERP

In this example, an SAP ERP system acts as the SAP backend system as described in the general scenario above.



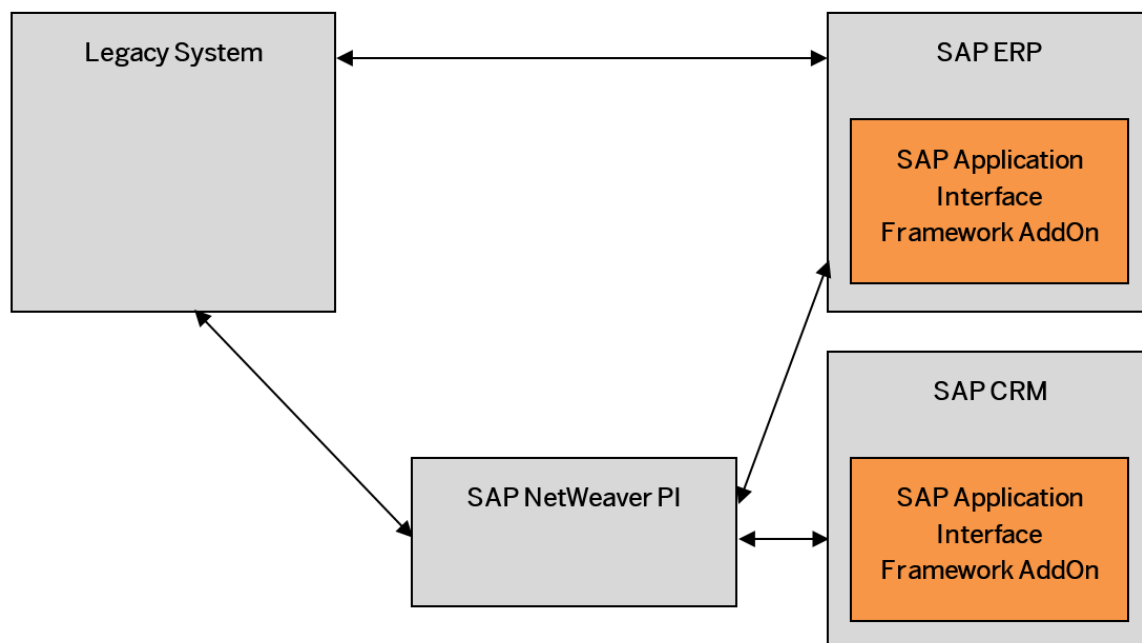
Example 2: SAP Application Interface Framework installed on SAP SRM

In this example, an SAP SRM system acts as the SAP backend system as described in the general scenario above.





Example 3: SAP Application Interface Framework installed on SAP ERP and SAP CRM

In this example, there is more than one SAP backend system. Every SAP backend system requires its own installation of the SAP Application Interface Framework.



2.4 Overall Implementation Sequence

The following table describes the overall implementation sequence for SAP Application Interface Framework. This table contains all available software units.

Step	Action	Required Documentation
1	Perform the installation of component AIF 703 with the latest available support package.	SAP Note 2608789 
2	Perform the (optional) installation of component AIFGEN 700 with the latest available support package.	SAP Note 2288871 
3	Customize settings for the SAP Application Interface Framework.	Application Help on SAP Help Portal at http://help.sap.com/aif , chapters Initial System Configuration and following.

2.5 Media List

All deliverables for the SAP Application Interface Framework are shipped electronically and no shipment is made via DVDs (or similar kind of data carrier media).

3 Security for SAP Application Interface Framework

Use

The SAP Application Interface Framework is built on an SAP NetWeaver system. Therefore, the corresponding security settings also apply to the SAP Application Interface Framework.

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

3.1 Authorization Objects

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

3.1.1 Authorization Object for Interface Processing

Definition

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

Authorization Fields

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

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

3.1.2 Authorization Object for Customizing Steps

Definition

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

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	You can enter the following activities: Change (02) Display (03)
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/MC	Customizing view	For the available values, see the table below

Use

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

Example

An interface developer is authorized to create, edit, and delete interfaces in namespace **x** but not **y**.

Allowed Values for the Namespace Field

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

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

Value	Description
/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
/AIF/V_IFKEY	Define Interface Key Fields for Variants
/AIF/V_NS	Define Namespace
/AIF/V_PERS_RTCG	Define Runtime Configuration Group
/AIF/V_RFC_FCOL	Define RFC Function Module Collection
/AIF/V_RFC_FUNCS	Assign Functions to RFC Function Module Collection
/AIF/V_SYSNAMES	Define Business Systems

Value	Description
/AIF/V_VALID_PER	Define Validity Period

3.1.3 Authorization Object 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>

Field Name	Heading	Authorization Object Setting
/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.

3.1.4 Authorization Object for Technical Error Handling

Definition

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

Authorization Fields

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

Use

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

3.1.5 Authorization Object for Emergency Corrections

Definition

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

Authorization Fields

Field Name	Heading	Authorization Object Setting
ACTVT	Activity	<p>You can enter the following activities (see description for authorization object <code>/AIF/ERR</code> 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	<p>This field refers to a namespace in the SAP Application Interface Framework</p>

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 key. The system then checks the authorization for emergency corrections and displays the [Emergency Correction Mode](#) checkbox, if applicable.

3.1.6 Authorization Object 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 Monitoring and Error Handling transaction)
/AIF/NS	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/IF	Interface Name	This field refers to an interface name in the SAP Application Interface Framework
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
/AIF/NSREC	Namespace of Recipient	Not used at the moment; enter *
/AIF/VISI	Visibility	Specifies for which users the custom function is visible. You can enter the following values: A means "Just for current user" B means "For a list of users" (maintained in transaction <code>/AIF/CUST_FUNC</code> Define Custom Functions Assign Users) C means "For all users"
/AIF/OTHUS	Authorization for other users	Not used at the moment; enter *

Use

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

3.1.7 Authorization Object for Custom Hints

Definition

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

Authorization Fields

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

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

Use

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

3.1.8 Authorization Object for Interface Determination

Definition

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

Authorization Fields

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

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

Use

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

3.1.9 Authorization Object for Value Mapping Maintenance

Definition

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

Authorization Fields

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

3.1.10 Authorization Object for File Adapter

Definition

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

Authorization Fields

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

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).

3.1.11 Authorization Object for Serialization

Definition

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

Authorization Fields

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

Use

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

3.1.12 Authorization Object for Change Log

Definition

The authorization object /AIF/CDLOG is used by the system to check the user's authorization to display the user name in the [Change Log Viewer](#) (transaction code /AIF/CHANGE_LOG).

Authorization Fields

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

Use

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

3.1.13 Authorization Object for Custom Message Texts

Definition

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

Authorization Fields

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

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

3.1.14 Authorization Object 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	<p>You can enter the following activities:</p> <p>Create or generate (01)</p> <p>Change (02)</p> <p>Display (03)</p> <p>Delete (06)</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
/AIF/VISI	Visibility	<p>Specifies for which users the custom data link is visible. You can enter the following values:</p> <p>A means "Just for current user"</p> <p>B means "For a list of users" (not used at the moment)</p> <p>C means "For all users" (not used at the moment)</p>
/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.

3.1.15 Authorization Object for AIF Persistence Messages Deletion

Definition

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

Authorization Fields

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

Use

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

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

3.1.16 Authorization Object for Processor Assignment

Definition

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

Authorization Fields

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

Field Name	Heading	Authorization Object Setting
/AIF/IF	Interface Name	This field refers to an interface name in the SAP Application Interface Framework
/AIF/IFVER	Interface Version	This field refers to an interface version in the SAP Application Interface Framework
/AIF/NSREC	Namespace	This field refers to a namespace in the SAP Application Interface Framework
/AIF/RECIP	Alert Management Recipient	This field refers to a recipient in the SAP Application Interface Framework.
/AIF/OTHUS	Authorization for Other Users	This field allows the user to change assignments, statuses, and comments also for other processors. An empty value means no authorization, while X means that the user has the authorization.
ACTVT	Activity	<p>You can enter the following activities:</p> <ul style="list-style-type: none"> • Change (02) • Display (03)

Use

Using the activity field, you specify the actions the user can execute in [Details and Processor Assignment](#) in the [Interface Monitor](#).

3.1.17 Authorization Object for Read Access Log

Definition

The authorization object `/AIF/RAL` is used by the system to check the user's authorization to display all read accesses to the content of data messages or uploaded files, using transaction [Read Log Viewer](#) (`/AIF/READ_LOG`).

Authorization Fields

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

3.1.18 Authorization Object for Read Access Log Customizing

Definition

The authorization object `/AIF/RAL_C` is used by the system to check the user's authorization to specify the fields for which the system logs read accesses, using transaction [Define Fields for Read Log](#) (`/AIF/READ_LOG_CUST`).

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/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

3.1.19 Authorization Object for External Contacts

Definition

The authorization object `/AIF/EXT_C` is used by the system to check the user's authorization to display, create, edit, and delete external contacts using transaction [Define External Contacts](#) (`/AIF/EXT_CON_LIST`).

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)

3.2 Role Templates

Definition

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

Features

Role Templates

The following role templates are delivered with the SAP Application Interface Framework 4.0:

- `SAP_AIF_ADMIN`: [AIF Administrator](#) [page 37]
- `SAP_AIF_ALL`: [AIF All Authorizations](#) [page 41]
- `SAP_AIF_ARCHITECT`: [AIF Architect](#) [page 41]
- `SAP_AIF_AUDITOR`: [AIF Auditor](#) [page 46]
- `SAP_AIF_DATA_PROT_O`: [AIF Data Protection Officer](#) [page 46]
- `SAP_AIF_DEVELOPER`: [AIF Developer](#) [page 47]
- `SAP_AIF_POWER_USER`: [AIF Power User](#) [page 51]
- `SAP_AIF_PROCESSING`: [AIF Processing](#) [page 55]
- `SAP_AIF_TEST_TEMPL`: [AIF Test Template \(Non-Productive\)](#) [page 56]

- SAP_AIF_USER: [AIF Business User \[page 56\]](#)

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.

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 versions 3.0 and 4.0, 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

3.2.1 AIF Administrator

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

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

Authorization Object	Activity	Activity Description
/AIF/CFUNC	1	Create or generate
/AIF/CFUNC	2	Change
/AIF/CFUNC	3	Display

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

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

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

Transaction Code	Description
/AIF/CORRECTIONS	Correction Report
/AIF/CUST	Customizing
/AIF/CUST_FUNC	Define Custom Functions
/AIF/CUST_HINTS	Define Custom Hints
/AIF/CUST_LINK	Define Custom Data Link
/AIF/CUST_TEXT	Define Custom Message Texts
/AIF/DEL_STRUC_CACHE	Delete Structure Cache
/AIF/DISPMMSGSNAP	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_IMPORT	AIF IDOC Import
/AIF/IDXTBL	Index Table Overview
/AIF/IF_TRACE	AIF Interface Trace Level
/AIF/IFMON	Interface Monitor
/AIF/LFA_CHECK_SEND	Read Files from folder; Send to AIF
/AIF/LFA_UPLOAD_FILE	Upload File to AIF
/AIF/LOG	Interface Logs
/AIF/MYRECIPIENTS	Recipients of Current User
/AIF/PERFORMANCE	Performance Tracking
/AIF/PERS_CGR	Runtime Configuration Group
/AIF/PERS_TEST	Test Persistence with Flight Booking
/AIF/RECIPIENTS	Recipients of a User
/AIF/REP_AC_ASGN	AIF Reprocessing Action Assignment
/AIF/REP_AC_DEF	AIF Reprocessing Action Definition
/AIF/SERIAL_INDEX	Manual Change of External Index
/AIF/TEXT_HINTS	Transport Text of Hints
/AIF/TJ_CONFIG	Configure Data Transfer
/AIF/TOPICDEF	AIF Topic Definition
/AIF/TOPICSTATUS	Maintain Topic ID Status
/AIF/TRANSFER	Transfer into AIF Persistence
/AIF/VMAP	Value Mapping
/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_CONS	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_FINE_TL	Define Trace Level
/AIF/V_HINTS	Define Custom Hints
/AIF/V_PERS_RTGC	Define Runtime Configuration Group

3.2.2 AIF All Authorizations

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

3.2.3 AIF Architect

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

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

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

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

In addition, an [AIF Architect](#) is provided with the authorization to the following transaction codes:

Transaction Code	Description
/AIF/BDC_GEN	Batch Input Structure Generator
/AIF/CORRECTIONS	Correction Report
/AIF/CUST	Customizing
/AIF/CUST_COPY	AIF Customizing Copy

Transaction Code	Description
/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
/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

Transaction Code	Description
/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_ALERT_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

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

3.2.4 AIF Auditor

The *AIF Auditor* is the only one who can display AIF data that is archived and blocked for data protection reasons.

The SAP Application Interface Framework archiving can use the SAP Information Lifecycle Management (SAP ILM) to manage the blocking and deletion of personal data. Once data is blocked by SAP ILM, special authorizations are required to display it anyway, for example, in an auditing scenario. For more information about blocking and deletion, see [Ensuring the Blocking and Deletion of Personal Data \[page 66\]](#).

For this tasks, an *AIF Auditor* is provided with the following authorization:

Authorization Object	Activity	Activity Description	Application Area
S_ARCHIVE	3	Display	CA

Along with this archiving authorization object, an *AIF Auditor* is provided with the authorization for the following AIF-specific archiving objects::

Archiving Object	Description
/AIF/FILE	Archiving object for AIF files
/AIF/MES	Archiving object for AIF messages
/AIF/PERSX	Archiving object for the AIF persistence

3.2.5 AIF Data Protection Officer

An *AIF Data Protection Officer* is responsible for checking the change log and the read access log of AIF to track user activities and fulfill data protection and privacy requirements. The AIF change log uses the change documents service of SAP NetWeaver.

For these tasks, an *AIF Data Protection Officer* is provided with the following authorizations:

Authorization Object	Activity	Activity Description
/AIF/CDLOG	70	Administer
/AIF/RAL	03	Display

Authorization Object	Activity	Activity Description
S_SCDO	*	All activities

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

Transaction Code	Description
/AIF/CHANGE_LOG	Change Log Viewer

For more information, see the following:

- [Providing a Read Access Log \[page 64\]](#)
- [Providing a Change Log \[page 65\]](#)

3.2.6 AIF Developer

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

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

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

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 Developer* is provided with the authorization to the following transaction codes:

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

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

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

View/View Cluster	Description
/AIF/ACTIONS	Define Actions
/AIF/BDC_V_CONF	Define Pre-Interface Determination for Batch Input

View/View Cluster	Description
/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

3.2.7 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/DISPMGSNAP	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_FINE_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

3.2.8 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

3.2.9 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.

3.2.10 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

Authorization Object	Activity	Activity Description
/AIF/ERR	34	Write
/AIF/ERR	71	Analyze
/AIF/ERR	75	Remove
/AIF/ERR	A4	Resubmit
/AIF/HINTS	1	Create or generate
/AIF/HINTS	2	Change
/AIF/HINTS	3	Display
/AIF/HINTS	6	Delete
/AIF/LFA	6	Delete
/AIF/LFA	33	Read
/AIF/LFA	34	Write
/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 display authorization to the following view:

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

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

Use

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

❖ Example

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

Process

1. You specify the fields that are relevant for authorizations as key fields and include them in a custom single index table. You do this in Customizing for the *SAP Application Interface Framework* under ► *Error Handling* ► *Interface-Specific Features* ►.
2. You create a custom authorization object in *Maintain the Authorization Objects* (transaction code SU21). The authorization object needs to fulfill the following requirements:
 - It requires a field called ACTVT.
 - The available activities in the ACTVT field must be the same as for the /AIF/ERR authorization object.
 - 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.

3.4 Data Protection and Privacy

The SAP Application Interface Framework supports data protection compliance by providing some security features and specific data protection-relevant functions.

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy regulations, it is necessary to consider compliance with industry-specific legislation in different locations. SAP provides specific features and functions to support compliance with regard to relevant legal requirements, including data protection. SAP does not give any advice on whether these features and functions are the best method to support company, industry, or regional requirements. Furthermore, this information should not be taken as advice or a recommendation regarding additional features that would be required in specific IT environments. Decisions related to data protection must be made on a case-by-case basis, taking into consideration the given system landscape and the applicable legal requirements.

i Note

SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and specific data protection-relevant functions, such as simplified blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. Definitions and other terms used in this document are not taken from a particular legal source.

3.4.1 Glossary

In the area of data protection and privacy, there are some central terms that are important to have a common understanding.

Term	Definition
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Business purpose	A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.
Deletion	Deletion of personal data so that the data is no longer available.
End of business	Date where the business with a data subject ends, for example the order is completed, the subscription is canceled, or the last bill is settled.
End of purpose (EoP)	End of purpose and start of blocking period. The point in time, when the primary processing purpose ends (for example contract is fulfilled).
End of purpose (EoP) check	A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose . After the EoP has been reached, the data is blocked and can only be accessed by users with special authorization (for example, tax auditors).
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person
Purpose	The information that specifies the reason and the goal for the processing of a specific set of personal data. As a rule, the purpose references the relevant legal basis for the processing of personal data.

Term	Definition
Residence period	The period of time between the end of business and the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Retention period	The period of time between the end of the last business activity involving a specific object (for example, a business partner) and the deletion of the corresponding data, subject to applicable laws. The retention period is a combination of the residence period and the blocking period.
Sensitive personal data	<p>A category of personal data that usually includes the following type of information:</p> <ul style="list-style-type: none"> • Special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or sex life or sexual orientation. • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses • Personal data concerning insurances and bank or credit card accounts
Where-used check (WUC)	A process designed to ensure data integrity in the case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.

3.4.2 Personal Data in the SAP Application Interface Framework

In the SAP Application Interface Framework, there are different entities that contain or might contain personal data.

The following entities contain or might contain personal data that are required for a business purpose. For these entities, SAP Application Interface Framework provides some security features and specific data protection-relevant functions that are described in this part of the security documentation.

- **Data Messages**

A data message is a message that is transferred between systems and that carries the actual business content. The SAP Application Interface Framework is monitoring and, in some scenarios, also persisting these data messages. The content of the data messages does not originate in the SAP Application Interface Framework but in the sending systems or applications. In the SAP Application Interface Framework, data messages can be displayed and, in some cases, also changed.

- **Value Mappings**

Value mapping is the process of mapping at field value level between source values and a particular destination value. Creating, changing, and deleting value mappings is part of the SAP Application Interface Framework configuration.

- **External Contacts**

An external contact is a name and an e-mail address or phone number to which you want to send SAP Application Interface Framework alerts, but which is not tied to an SAP user in the system. Creating, changing, and deleting external contacts is part of the SAP Application Interface Framework configuration.

- **Uploaded Files**

The file adapter of the SAP Application Interface Framework enables you to upload files whose content is then processed in the AIF runtime and can be monitored in the [Monitoring and Error Handling](#) transaction. The file content originates outside the SAP system. However, before uploading the content, authorized users can preview it in the file adapter.

For the following entities in SAP Application Interface Framework, there is no business purpose to contain personal data. Make sure that you do not add personal data to their content.

- **Test File**

In [Monitoring and Error Handling](#), from a set of data messages, you can create a file with test data for the AIF test tool. The system does not write the content of fields to the file that are marked as relevant for the read access logging (see [Providing a Read Access Log \[page 64\]](#)). Make sure that you marked all personal data as read log relevant.

i Note

You can remove read log relevant contents from existing test files using the program [Clear Sensitive Data in Test Files](#) (/AIF/CLEAR_SENSITIVE_TESTFILE).

- **Custom Texts**

In [Monitoring and Error Handling](#), in the [Log Messages](#) view, you can write custom hints and custom message texts. In the [Interface Documentation Tool](#) you can write documentation for an interface or for a Customizing object. Make sure that the users do not enter personal data.

- **Custom Modules**

In the SAP Application Interface Framework, you can integrate custom programming modules, for example, as action or value mapping step. Make sure that these modules do not display or log personal data.

3.4.3 Limiting Access to Personal Data

The SAP Application Interface Framework provides you with authorizations you can use to limit access to personal data that is collected or transferred by the SAP Application Interface Framework.

You can limit the access to the content of **data messages**, to the **value mapping**, to **external contacts**, and to **uploaded files** using the various dedicated authorization objects of SAP Application Interface Framework.

There are also authorization objects available to limit access to the read access and change logs for these entities. For more information, see [Authorization Objects \[page 16\]](#).

For your convenience, these authorizations are combined in predefined role templates, including the data protection-specific templates *AIF Data Protection Officer* and *AIF Auditor*. For more information, see [Role Templates \[page 35\]](#).

By default, the content of **data messages** and the related **log messages** can be accessed by all users who have the authorization to display or change messages of the corresponding interface in the [Monitoring and Error Handling](#). If you want to further protect certain parts of the data messages, you can define the corresponding structures as *Hide Structures*. You do this in Customizing for *SAP Application Interface Framework* under [► Error Handling ► Define Namespace-Specific Features ►](#).

In addition, you can set up even more specific authorizations to limit access to data contained in the data messages by creating custom authorization objects. For more information, see [Set Up Interface-Specific and Key Field-Specific Authorizations \[page 58\]](#).

3.4.4 Ensuring the User Consent

Data subjects need to be able to confirm that the usage of their personal data is allowed for a given purpose.

The SAP Application Interface Framework is used exclusively by corporate users and not by consumers. SAP assumes that the consent for collecting data of these corporate users, for example, when creating external contacts, is covered by their employment contract.

The SAP Application Interface Framework itself does not collect the personal data of consumers. But AIF might transfer personal data of consumers in data messages. SAP assumes that you have gained and documented the consent of the data subjects before the data was created in the sending system or application.

3.4.5 Providing an Information Report

Each person has the right to obtain confirmation as to whether or not personal data concerning him or her is being processed.

The SAP Application Interface Framework transfers personal data in **data messages**. The personal data being transferred is owned by the sending or receiving system or application and we assume that it can be displayed there.

The SAP Application Interface Framework can collect and store personal data in the following objects and you can display all the data they store about a certain data subject as follows:

- **External contacts**

You can display a list of external contacts in Customizing for *SAP Application Interface Framework* under

[► System Configuration ► Recipients ► Define External Contacts ►](#) (transaction code `/AIF/EXT_CON_LIST`).

External contacts are identified by name and contact method.

→ Recommendation

We strongly recommend that you choose unique names so that you can clearly relate one external contact in the system to one person (or one group of persons).

- **Value mappings**

You can display a list of value mappings from the SAP Easy Access menu by choosing ► [Cross-Application Components](#) ► [SAP Application Interface Framework](#) ► [Value Mapping](#) (transaction code `/AIF/VMAP`).

3.4.6 Providing a Read Access Log

The SAP Application Interface Framework provides read access logging for the content of data messages and uploaded files.

Read access logging is used to monitor and log read access to sensitive data. Data may be categorized as sensitive by law, by external company policy, or by internal company policy. Read access logging enables you to answer questions about who accessed particular data within a specified time frame.

The SAP Application Interface Framework provides a framework to develop interfaces. Interface developers define the fields and know which of the fields might hold personal data. Thus, interface developers need to ensure that the affected fields of an interface are marked as relevant for the read access logging of the SAP Application Interface Framework.

You mark fields as read log relevant in Customizing for [SAP Application Interface Framework](#) under ► [Interface Development](#) ► [Additional Interface Properties](#) ► [Define Fields for Read Log](#) (transaction code `/AIF/READ_LOG_CUST`). For each interface, you can decide which fields of the SAP structure, RAW structure, or index table are relevant for the log. In addition, you can define a log level for these fields in Customizing for [SAP Application Interface Framework](#) under ► [System Configuration](#) ► [Define General Settings](#).

For fields that are marked as read log relevant, the SAP Application Interface Framework writes a read log entry as soon as one of the following happens:

- The content of the structure is displayed in the [Monitoring and Error Handling](#) transaction (SAP GUI or Web).

i Note

In the [Monitoring and Error Handling](#), you can add a custom selection screen. If you do so make sure, that you do not allow your users to select personal data.

- A read log relevant field is changed, the change is written to the change log of the SAP Application Interface Framework, and the corresponding change log entry is displayed.
- The file adapter is used, a file is uploaded for an interface with read log relevant fields, and the file content is displayed.

i Note

The file content is also displayed if the file adapter cannot find an interface. Make sure that your file adapter configuration prevents this.

The system logs the following information per read access:

- Interface key
- Keys of the data record such as field path and field name
- Date and time of the read access
- The place (application) of the read access
- The user who read the data

You can display the read access logs of the SAP Application Interface Framework from the SAP Easy Access menu by choosing ► [Cross-Application Components](#) ► [SAP Application Interface Framework](#) ► [Administration](#) ► [Log](#) ► [Read Log Viewer](#) ► (transaction code /AIF/READ_LOG).

3.4.7 Providing a Change Log

The SAP Application Interface Framework provides change logging for the content of data messages, value mappings, and external contacts.

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary for you to track the changes made to this data. When these changes are logged, you should be able to check when a change was made, which employee made which change, the previous value, and the current value. You can also analyze errors in this way.

In the SAP Application Interface Framework, the change logging is always enabled for changes to the following:

- The content of data messages
- Value mappings
- External contacts

The system automatically logs the following information per change request and activity:

- Date and time of the change
- Identifying keys of the affected data records
- Name and path of the field that has been changed
- New and old value of the changed field
- ID of the user who made the change

i Note

The user ID is only available for users that have the authorization object /AIF/CDLOG assigned.

You can display the change logs of the SAP Application Interface Framework from the SAP Easy Access menu by choosing ► [Cross-Application Components](#) ► [SAP Application Interface Framework](#) ► [Administration](#) ► [Log](#) ► [Change Log Viewer](#) ► (transaction code /AIF/CHANGE_LOG).

3.4.8 Ensuring the Blocking and Deletion of Personal Data

The SAP Application Interface Framework supports you in blocking and deleting personal data according to various data protection regulations.

i Note

If you are not familiar with the typical lifecycle of personal data and with terms like end of purpose, retention period, residence period, or blocking, please read the following first: [General Considerations about the Lifecycle of Personal Data \[page 67\]](#)

Data Messages, Uploaded Files, and Related Log Messages

The end of the business activity for data messages and file adapter logs (and their related application log, read log, and change log entries) is reached once the SAP Application Interface Framework processing is finished. This is, for data messages, they have one of the following final statuses:

- *Successful*
- *Successful with warnings*
- *Canceled*

After the end of business activity, you can archive and delete these data messages, file logs, and related log messages using the data archiving feature of SAP Application Interface Framework.

i Note

SAP Application Interface Framework archives and deletes only data messages that reside in its own persistence (XML or structured). For data messages that are stored in another application, for example, the IDoc framework, AIF only archives and deletes the related AIF data, for example, index tables and logs.

After the archiving, the data is only available in archive files and, thus, blocked for everyone without the authorization to display archives. To finally destroy the data, you can delete the archives.

To support a more sophisticated and automated information lifecycle, the SAP Application Interface Framework provides an integration with SAP Information Lifecycle Management (SAP ILM) for the archiving and destruction of personal data. If SAP ILM is available in the system, you can use SAP ILM transactions to set up residence and retention rules that the SAP Application Interface Framework archiving and destruction programs will apply.

Archives that are blocked using SAP ILM can only be displayed if a user has a special auditing authorization. For more information, see [AIF Auditor \[page 46\]](#).

→ Recommendation

We recommend that you automate the archiving and destruction of the data by scheduling the corresponding programs in short periods.

For more information about archiving and destruction with and without SAP ILM, see the Application Help for SAP Application Interface Framework, chapters *Data Archiving* and *Data Destruction*.

External Contacts

The end of business activity for an external contact is reached once one of the following happens:

- The *End of Business Date* for the external contact has passed.
You can set this date for individual external contacts in Customizing for the *SAP Application Interface Framework* under ► *System Configuration* ► *Recipients* ► *Define External Contacts* ►.
- The external contact has not been used for the *Lifetime of the External Contacts* period. Not used means that the contact has not been assigned to a recipient nor has it been changed.
You can set this lifetime period globally in Customizing for the *SAP Application Interface Framework* under ► *System Configuration* ► *Define General Settings* ►.

After the end of business activity, the external contact is blocked. You can delete external contacts in the Customizing at any time. To mass-delete external contacts that passed their end of business date and lifetime period, you can use *Remove External Contacts* (transaction code /AIF/EXT_CONTACT_REMOVE). You can also use SAP ILM to manage the destruction of external contacts data.

For more information, see the Application Help for SAP Application Interface Framework, chapter *Data Destruction*.

Value Mappings

The end of business activity for a value mapping is reached once its *Validity Period* has passed.

You can define if and what type of validity period can be set for a value mapping in Customizing for the *SAP Application Interface Framework* under ► *Interface Development* ► *Define Value Mappings* ►. You set the actual validity period in the SAP Easy Access menu by choosing ► *Cross-Application Components* ► *SAP Application Interface Framework* ► *Value Mapping* ►.

After the end of business activity, the value mapping is blocked. You can delete value mappings in the Customizing at any time. You can also use SAP ILM to manage the destruction of value mapping data.

For more information, see the Application Help for SAP Application Interface Framework, chapters *Value Mapping Maintenance* and *Data Destruction*.

3.4.8.1 General Considerations about the Lifecycle of Personal Data

When considering compliance with data protection regulations, it is also necessary to consider compliance with industry-specific legislation in different locations. A typical potential scenario in certain locations is that personal data shall be deleted after the specified, explicit, and legitimate purpose for the processing of personal data has ended, but only as long as no other retention periods are defined in legislation, for example, retention periods for financial documents. Legal requirements in certain scenarios or locations also often require blocking of data in cases where the specified, explicit, and legitimate purposes for the processing of this data have ended, however, the data still has to be retained in the database due to other legally mandated retention periods.

The processing of personal data is subject to applicable laws related to the deletion of this data when the specified, explicit, and legitimate purpose for processing this personal data has expired. If there is no longer a legitimate purpose that requires the retention and use of personal data, it must be deleted. When deleting data in a data set, all referenced objects related to that data set must be deleted as well. Industry-specific legislation in different locations also needs to be taken into consideration in addition to general data protection laws. After the expiration of the longest retention period, the data must be deleted.

An end of purpose (EoP) check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period is part of the overall lifecycle of personal data which consists of the following phases:

- **Business activity:** The relevant data is used in ongoing business, for example contract creation, delivery or payment.
- **Residence period:** The relevant data remains in the database and can be used in case of subsequent processes related to the original purpose, for example reporting obligations.
- **Blocking period:** The relevant data needs to be retained for legal reasons. During the blocking period, business users of SAP applications are prevented from displaying and using this data; it can only be processed in case of mandatory legal provisions.
- **Deletion:** The data is deleted and no longer exists in the database.

Blocking of data can impact system behavior in the following ways:


- The system does not display blocked data.
- It is not possible to change a business object that contains blocked data.
- It is not possible to create a business object that contains blocked data.
- It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

4 Upgrade of SAP Application Interface Framework

This section describes the manual efforts required after the upgrade of SAP Application Interface Framework from version 3.0 to version 4.0.



Note

To perform the actual release upgrade of the SAP Application Interface Framework add-on (component AIF) to version 4.0 (component release 703), follow the instructions in SAP Note [2608789](#) .

To support data protection compliance, SAP Application Interface Framework 4.0 has been enhanced by some specific data protection-relevant functions. These enhancements require the following manual post-upgrade activities.

Convert External Addresses to External Contacts

SAP Application Interface Framework 4.0 introduces the **external contact** as a separate object. An external contact is an e-mail address or number you want to send SAP Application Interface Framework alerts to, but which is not tied to an SAP user in the system.

In version 4.0, you can manage external contacts in Customizing for the *SAP Application Interface Framework* under  [Error Handling](#)  [System Configuration](#)  [Recipients](#)  [Define External Contacts](#) .

In version 3.0, you could define **external addresses** as additions to the recipient objects. If you have defined external addresses, convert those to external contacts using the program [Convert External Addresses to External Contacts](#) (/AIF/EXT_CONTACT_MIGRATION).

Caution

To avoid data loss, carefully read the system documentation on the selection screen of the program before executing it.

Set up the Enhanced Data Archiving

SAP Application Interface Framework 4.0 introduces new archiving objects and archiving programs. The archiving object /AIF/PERSX was divided and is now obsolete. The following new archiving objects are available in version 4.0:

- /AIF/MES: Archives data messages and all related data
- /AIF/FILE: Archives everything that is related to the file adapter process

Using the new objects, SAP Application Interface Framework 4.0 allows for a more sophisticated and automated information lifecycle. The SAP Application Interface Framework provides an integration with SAP Information Lifecycle Management (SAP ILM) for the archiving and destruction of personal data.

Set up your archiving process from scratch using the new archiving objects and programs, and consider using SAP ILM to handle the blocking and deletion of the data.

i Note

The data archived before upgrading to version 4.0 does not hold lifecycle information like residence times or retention times. Hence, this data is considered as blocked. To enable the old archives for SAP ILM, you need to move them to the SAP ILM store. To ensure data protection, you can also delete the old archives.

Related Information

[Ensuring the Blocking and Deletion of Personal Data \[page 66\]](#)

5 Uninstallation of SAP Application Interface Framework

If you do not want to use SAP Application Interface Framework any more, you can remove the software components AIF and AIFGEN from your system using the add-on Installation tool (transaction SAINT).

Caution

Before performing the uninstallation procedure, consider the following:

- You need to perform several preparation actions to enable a safe uninstallation. Otherwise, the uninstallation of the add-ons may lead to loss of data.
- We strongly recommend that you do not uninstall SAP Application Interface Framework if there are compliance or auditing obligations to retain the messages data.



For more information about the preparation steps and the uninstallation procedure, see [2497991](#) 

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.

Videos Hosted on External Platforms

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

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

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

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.

© 2021 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.