



Connectivity

Alliance Access 7.1.10

On Alliance Web Platform

Configuration Guide

This guide describes how to use the Alliance Access Configuration package through the Alliance Web Platform to configure and manage Alliance Access. This document is for operators, Alliance security officers, and administrators who manage Alliance Access.

17 July 2015

Table of Contents

Preface	5
1 Training for SWIFT Users	6
2 Accessing Alliance Access Configuration	7
2.1 Logging In	7
2.2 Changing Your Password	8
2.3 Logging Out	8
3 The Alliance Access Configuration Workspace	10
3.1 Workspace Overview	10
3.2 Home Page	12
3.3 Task Pages in Alliance Access Configuration	13
3.4 Common Actions in Task Pages	20
3.5 Online Help	37
3.6 User Assistance	38
3.7 Preferences	43
4 Initial Configuration for SWIFTNet	45
4.1 Introduction	45
4.2 Check Connectivity	45
4.3 Define Alliance Access in Alliance Gateway	46
4.4 Configuring Alliance Access for FIN Messaging	52
4.5 Configuring Alliance Access for InterAct and FileAct Messaging	55
4.6 Configuration for Sanctions Screening	58
5 System	60
5.1 System Check	60
5.2 Software Integrity Check	63
5.3 Database Integrity Check	64
5.4 Restart/Stop	67
5.5 Components	71
5.6 Gateway Connectivity	76
5.7 Database Backups	84
5.8 Recovery Backups	88
5.9 User Space	95
5.10 Printers	98
5.11 Calendars	102
5.12 Reporting - BIC Selection	110
5.13 Parameters	111
5.14 Security Parameters	129
5.15 SNMP Heartbeat	146

6	Event Log	148
6.1	Distribution Lists	148
6.2	Event Distribution	154
6.3	Event Log Archives	160
6.4	Event Archive Backups	164
6.5	Event Log	170
7	Messages	181
7.1	Syntax Versions	181
7.2	Message Standards	184
7.3	Message Templates	193
7.4	Message File Archives	206
7.5	Message Archive Backups	210
8	User Management	217
8.1	Authentication Server Groups	218
8.2	LDAP Server Groups	226
8.3	Units	236
8.4	Operator Profiles	241
8.5	Operators	246
9	Reference Data	263
9.1	BIC Directory	263
9.2	BICs and Other Codes	269
9.3	Aliases	281
9.4	Countries	286
9.5	Currencies	290
10	Application Interface	294
10.1	Application Interface	294
10.2	Message Partners	294
11	SWIFTNet Interface	333
11.1	FIN Delivery Subsets	333
11.2	FIN Logical Terminals	343
11.3	Application Service Profiles	364
11.4	FIN Copy Profiles	370
11.5	Emission Profiles	377
11.6	Input Channels	394
11.7	Reception Profiles	398
11.8	Output Channels	413
11.9	Advanced Real-Time File Handler	417
11.10	Correspondent/Real-Time Service on Hold	420
12	CRnet Interface	425
12.1	Dashboard	425
12.2	Configuration	428

13 Routing	441
13.1 Overview of Routing in Alliance Access	441
13.2 How message routing works	443
13.3 Configuration of Routing in Alliance Access	445
13.4 Queues	446
13.5 Routing Keywords	516
13.6 Routing Schemas	536
Appendix A Integrating Back-office Applications with Alliance Access	541
A.1 Connection Methods	541
A.2 Message Formats	622
A.3 Message Validation and Disposition	758
Appendix B Cold Start	768
B.1 General Information	768
B.2 Cold Start Events	770
B.3 Cold Start Configuration Parameters	772
B.4 Input and Output Channel Management	772
B.5 FIN Message Processing	773
B.6 Store-and-forward Message Processing	776
B.7 Searching for Cold Start Messages	777
B.8 Message Details and Reports	778
B.9 FINCopy Services Setup	778
B.10 What To Do Before the First Login>Select	778
B.11 Performing the First Login>Select	780
B.12 Re-approving Messages to be Re-sent	780
B.13 Resuming Normal Operations	780
B.14 Cold Start Simulation	780
Appendix C Handling Double-Authenticated Messages with FINCopy	784
C.1 Message Flow	784
C.2 Implementation	787
C.3 Examples of MT 096 and MT 097 with PKI Signatures	790
Legal Notices	794

Preface

Purpose

This guide describes how to use the Alliance Access Configuration interface to perform Alliance Access configuration tasks. The Alliance Access Configuration interface is available through the Alliance Web Platform.

Audience

This guide is for Alliance Access operators and security officers who use the Alliance Access Configuration interface.

About Alliance Web Platform

Alliance Web Platform is the framework that hosts browser-based graphical user interfaces (GUI) of the Alliance portfolio. It offers a consistent end-user interface to the functionality managed by the Alliance servers. Alliance Web Platform runs in an application server environment, enabling centralised deployment of the software.

1 Training for SWIFT Users

Overview

SWIFT Training is your first point of contact for learning how to use SWIFT standards, products, and services accurately and effectively. Training is available to all SWIFT users.

Related courses

SWIFT recommends the following Alliance Access Configuration courses. For full descriptions, consult the Training pages on swift.com:

- [Operating Alliance Access and Entry](#)
- [Managing Alliance Access and Entry](#)
- [Deploying Alliance Access](#)
- [Optimising Your Alliance Resilience](#)
- [Alliance - Disaster Recovery](#)
- [SWIFT Audit Guidelines](#)

To view the full training portfolio that SWIFT offers, see www.swift.com > Training > [Training topics](#).

How to register for training

To register for SWIFT Training, visit www.swift.com/training. You must have a swift.com user name and password to register for SWIFT Training. If you do not have a swift.com user name and password, [register at swift.com](#). Instructions will be sent to you by e-mail.

2 Accessing Alliance Access Configuration

2.1 Logging In

Prerequisites

To log in to Alliance Access Configuration on Alliance Web Platform, you need the following:

- *URL*

You must have a valid URL for Alliance Access Configuration. The administrator of Alliance Web Platform provides this information.

This is the default URL:

`https://<host>[:<port>]/swp/group/accessconfig`

Where:

- `<host>` is the Alliance Web Platform host name
- `<port>` indicates the port number (optional)
It is not necessary to specify a value for `<port>` if the default port for HTTPS is used.
- `swp` refers to Alliance Web Platform
- `group/accessconfig` refers to the Alliance Access Configuration GUI application

- *User name and password*

You must have a user name and a password that correspond to your operator definition. The administrator of your Alliance Access server provides this information.

Screen resolution settings

For a proper display of the information in Alliance Access Configuration pages, set your screen resolution to 1280 by 1024 pixels or higher.

Do not use the zoom functionality of the browser. The layout of Alliance Access Configuration labels can be incorrect when the display value of the browser is not set at 100 percent.

Procedure

To log in to Alliance Access Configuration:

1. Start your browser.
2. Perform one of these actions to provide the URL for Alliance Access Configuration, as applicable:
 - Type the URL in the address bar of your browser and press **ENTER**.
 - Select the URL from your list of saved links, for example, from **Favourites** or **Bookmarks**.
 - Select the URL from the list of previously visited addresses.

The browser displays the Alliance Access Configuration login page.

3. Enter your **User Name** and **Password**. Both are case sensitive.

If you are using your password for the first time, then you must enter a four-character password received from the security officers of your Alliance server. When you click **Login**, you are prompted to change it. See "Changing Your Password" on page 8 for details.

This is not applicable if the authentication method used for your operator definition is either One-time Password or LDAP.

4. If multiple Alliance Access instances have been configured for the Alliance Web Platform host, then select the applicable Alliance Access server instance from the **Alliance Server Instance** drop-down list.
5. Click **Login**.

After you have successfully logged in, the Alliance Access Configuration Workspace appears. See "The Alliance Access Configuration Workspace" on page 10.

Tip

If you experience problems logging in, then try deleting the Browsing history files.

You can delete these files from the **Tools** menu or **Options** window. The exact location depends on your browser type and release.

2.2 Changing Your Password

Applicability

Operators with the authentication type **Password** are requested to change their password when logging in in the following situations:

- at the first login with a new operator password
- when the password has expired
- if the password was reset on the Alliance server

The frequency with which you have to change your password depends on the security configuration parameters set on the Alliance server. You can also change your password on demand. For password requirements, check with the security officers of your Alliance server.

Procedure

1. If you want to change your password on demand, then click **Change Password** in the upper right corner of the navigation area.
The **Change Password** dialog box appears.
2. Type your current password in the **Old Password** field. Then type your new password in the **New Password** and **Password Verification** fields.
3. Click **Change Password**.
The password is changed.

2.3 Logging Out

Applicability

You can log out from Alliance Access Configuration from any page except the login page.

Procedure

1. Click **Logout** in the top right corner of the browser window.

A confirmation window opens.

2. Click **OK** to log out or **Cancel** to cancel the request to log out.

If you click **OK**, then the browser displays the Alliance Access Configuration login page.

3 The Alliance Access Configuration Workspace

About this section

This section describes the layout, components, functionality, and behaviour of the Alliance Access Configuration workspace.

3.1 Workspace Overview

Description

The workspace is a browser-based GUI that communicates with an application server, which communicates with an Alliance Access server.

The Alliance Access Configuration workspace displays the home page by default when a user logs in.

The workspace has the following areas:

Area	Description
Navigation area	Displays a logo, the name and release of the GUI package, links for navigating, and menus for accessing the task pages of Alliance Access Configuration. See "Navigation area" on page 11.
Main area	Displays the home page or the task pages of Alliance Access Configuration.
Bottom banner	Displays copyright and status information. See "Bottom banner area" on page 12.

Example

The following example shows the workspace, with the home page selected:



1	"Navigation area" on page 11
2	Main area where the home page and the task pages appear. See "Home Page" on page 12 and "Task Pages in Alliance Access Configuration" on page 13.

3	"Bottom banner area" on page 12
---	---------------------------------

Navigation area

The navigation area is always visible and contains the following:

Logo

Click the logo to return to the home page of the workspace.

The "Example" on page 10 shows the SWIFT logo. The Alliance Access Configuration workspace can show a different logo, if the Alliance Web Platform administrator has changed the setting.

Menus

Select a menu in the navigation area to display the corresponding task page in the workspace.

Important While Alliance Access Configuration is processing a request, do not start another action. Always wait for the response before you click another link or button.

These are the menus which provide access to the home page and to the task pages:

Menu	Purpose
Home	Displays the home page of the workspace.

The menus available depend on .

Links in the navigation area

The top-right corner of the navigation area of the workspace provides links to the following:

Link	Function
Preferences	Sets the preferences that are available for the current page. See "Preferences" on page 43 Some pages do not have preferences, and in those cases, the Preferences link is unavailable.
Help	Opens the context-sensitive online help that is available for the page or entity that is currently selected. The page or window from which you click the Help link determines the information that the system shows. For example: <ul style="list-style-type: none"> If you click the Help link on the login page or the home page, then the system opens the Alliance Web Platform Server-Embedded online help. If you click the Help link on a page or window within Alliance Access Configuration, then the system opens the Alliance Access Configuration online help. See "Online Help" on page 37.
Change Password	Changes your password. See "Changing Your Password" on page 8 Online help for this task is available only from the Alliance Access Configuration Home page.
Logout	Logs out from Alliance Access Configuration See "Logging Out" on page 8.

Link	Function
About	<p>Displays the following:</p> <ul style="list-style-type: none"> • Information about the current session: <ul style="list-style-type: none"> – The user name that you are logged in as – The user type – The name of the instance that you are logged on to – The Alliance Access release – The Alliance Access host platform • Information about Alliance Web Platform: <ul style="list-style-type: none"> – The Alliance Web Platform release – The operating system on which Alliance Web Platform is installed – The Java Virtual Machine version

Bottom banner area

The bottom banner area is always visible. It displays the following:

Copyright details

The SWIFT copyright statement

Session details

Information about sessions:

- The user name that you are logged in as
- The name of the instance that you are logged on to

User

Displays the user name that you are logged in as

Status

A user can click **Status** to display the last 20 notification messages that Alliance Access Configuration provided to the user about the current task or about recently performed tasks.

3.2 Home Page

Description

The Alliance Access Configuration workspace displays the home page by default when a user logs in.

The home page shows a list of shortcuts to tasks that are also available through the menus in the navigation area.

Tip Click the logo at any time to return to the home page of the workspace.

Click the link to display the corresponding task page. For more information, see "Task Pages in Alliance Access Configuration" on page 13.

3.3 Task Pages in Alliance Access Configuration

Description

A task page opens when you select a shortcut from the **Welcome** application or from a menu. These pages enable you to perform tasks in Alliance Access Configuration.

For the Alliance Access Configuration pages, a task page displays a left pane and right pane area.

Example of a task page

Name	Description	Approval Status	Enable Status	Last Login	Authentication
Asma		Unapproved	Disabled		Token
CREST1	Crest operator 1	Approved	Enabled		Token
CREST2	Crest operator 2	Approved	Enabled		Password

Task page components

The task pages can contain these elements:

Left pane

The left pane provides a way to navigate amongst available entities. This is referred to as a tree view or structure.

A tree view in Alliance Access Configuration displays entities in a hierarchical view in the left pane of a task page in the workspace. Each level of information is called a *node*. A node in Alliance Access Configuration corresponds to the entities that are available, and to the information that is available for that node.

The tree view starts with a parent node, and each node is indented to show its relationship with the parent node.

If you click a node, then the right pane of the workspace shows the page that corresponds to that node. Some nodes are a container for other nodes and do not correspond to an entity.

If you click beside a node, then the tree view expands to show the nodes within that node.

If you click beside a node, then the tree view collapses to hide the nodes within that node.

Right pane

The right pane displays the information that is available for the entity that is selected in the left pane. The right pane display the information as a page view.

The page view enables you to modify the properties of the entity, if applicable.

A page can consist of the following components:

- "List View" on page 14
- "Form View" on page 16
- "List within a Form" on page 18

Splitter

A splitter is a line that divides the left pane and the right pane. You can drag the splitter left or right to resize the panes.

Button bar

On some pages, a button bar is present at the bottom of the main area of the workspace. The buttons enable you to perform an action for the entity that is currently selected. The buttons that are available depend on the selected entity and on the permissions assigned to your operator profile.

3.3.1 List View

Description

Some pages and windows in Alliance Access Configuration display a list to show the information that is relevant for the current selection.

You can find the following types of information in a list:

- Entities in Alliance Access
- MT, MX, and Application Control (APC) messages and message templates
- Message instances
- The results of a search

Some pages display a form above the list, to enable you to search for entities, or to filter the list. For more information about search or filter criteria, see "Perform a Search or Filter a List" on page 21.

Example

Event Log								
Search Criteria								
From Date	2015/02/04	?	Time	00:00:00	Severity	?	Package	
To Date	2015/02/06	?	Time	23:59:59	Class	?		
<input type="button" value="Clear"/>							<input type="button" value="Search"/>	
Events								
Change View								
Date & Time	Severity	Class	Package	Name	User	Description	Rows in list: 20	
2015/02/06 09:41:52	INFO	Security	Alliance Web Platform 7.0.60	login.success	swpadmin	User swpadmin logged in successfully to application group Alliance Web Platform Administration 7.0.60.	<input type="button" value="Previous"/>	<input type="button" value="Next"/>
2015/02/06 05:59:22	WARNING	Security	Alliance Web Platform 7.0.60	session.expired	fahmi	The session of user fahmi has expired.		
2015/02/06 04:25:41	INFO	Security	Alliance Web Platform 7.0.60	login.success	fahmi	User fahmi logged in successfully to application group Alliance Access/Entry Configuration 7.1 (to instance "benx0222")		
2015/02/05 13:58:11	INFO	Software	Alliance Web Platform 7.0.60	servers.Accessinstance.status.reachable		Alliance Access/Entry instance "benx0222" is reachable.		
2015/02/05 13:43:32	SEVERE	Software	Alliance Web Platform 7.0.60	servers.Accessinstance.status.unreachable		Alliance Access/Entry instance "benx0222" is unreachable. Failed to connect to Alliance Access/Entry due to connection timeout.		
2015/02/04 16:45:04	INFO	Software	Alliance Web Platform 7.0.60	servers.Accessinstance.status.reachable		Alliance Access/Entry instance "benx0222" is reachable.		
2015/02/04 16:03:34	SEVERE	Software	Alliance Web Platform 7.0.60	servers.Accessinstance.status.unreachable		Alliance Access/Entry instance "benx0222" is unreachable. Failed to connect to Alliance Access/Entry due to connection timeout.		
2015/02/04 14:40:03	INFO	Security	Alliance Web Platform 7.0.60	logout.success	swpadmin	User swpadmin logged out successfully from application group Alliance Web Platform Administration 7.0.		
2015/02/04 14:37:41	WARNING	Security	Alliance Web Platform 7.0.60	login.failure	Administrator	User Administrator failed to login to application group Alliance Gateway Administration 7.0.25 to instance "benx0222".		
2015/02/04 14:37:26	INFO	Security	Alliance Web Platform 7.0.60	logout.success	Administrator	User Administrator logged out successfully from application group Alliance Gateway Administration 7.0.3		
2015/02/04 14:34:24	INFO	Security	Alliance Web Platform 7.0.60	login.success	Administrator	User Administrator logged in successfully to application group Alliance Gateway Administration 7.0.35 (to instance "benx0222")		
2015/02/04 14:33:50	INFO	Software	Alliance Web Platform Admin 7.0.60	servers.Gatewayinstance.connectivity.reachable	swpadmin	Connectivity test for Alliance Gateway instance "benx0222" was successful.		
2015/02/04 14:33:35	INFO	Security	Alliance Web Platform 7.0.60	login.success	swpadmin	User swpadmin logged in successfully to application group Alliance Web Platform Administration 7.0.60.		
2015/02/04 14:31:27	INFO	Software	Alliance Web Platform 7.0.60	servers.Gatewayinstance.status.reachable		Alliance Gateway instance "benx0221_7035" is reachable.		
2015/02/04 14:31:27	INFO	Software	Alliance Web Platform 7.0.60	servers.Gatewayinstance.status.reachable		Alliance Gateway instance "benx013_7035" is reachable.		
2015/02/04 14:31:26	INFO	Software	Alliance Web Platform 7.0.60	servers.Gatewayinstance.status.reachable		Alliance Gateway instance "smx05_7025" is reachable.		
2015/02/04 14:31:26	INFO	Software	Alliance Web Platform 7.0.60	servers.Gatewayinstance.status.reachable		Alliance Gateway instance "benx022_7020" is reachable.		
2015/02/04 14:31:23	INFO	Software	Alliance Web Platform 7.0.60	servers.Accessinstance.status.reachable		Alliance Access/Entry instance "benx0222" is reachable.		
2015/02/04 14:31:16	INFO	Software	Alliance HTTP Proxy 7.0.60	proxy.enable		HTTP Proxy has been enabled successfully. Listener Address is "0.0.0.0:48600". Allowed Hosts are "benx0222".		
2015/02/04 14:29:38	INFO	Security	Alliance Web Platform 7.0.60	logout.success	swpadmin	User swpadmin logged out successfully from application group Alliance Web Platform Administration 7.0.		

Copyright © S.W.I.F.T. SCRL ("SWIFT"), Avenue Adèle 1, B-1310 La Hulpe, Belgium

User: swpadmin Status

Components

A list in Alliance Access Configuration usually contain these elements:

Title bar

At the top left, the title bar shows the title of the list.

At the top right, the title bar shows the number of rows in the current view of the list, and the number of rows that are selected.

Button bar

The button bar is below the title bar of the list.

The buttons enable you to perform an action for the entity that is currently selected. The buttons that are available depend on the selected entity and on the permissions assigned to your operator profile.

Check-box column

A check-box is associated with each row. The check-box enables you to select the row. You can select the check-box column to select a row, or to clear the selection.

Column heading

The names of the columns correspond to the properties and the elements of the entities in the list.

Row

Each row in the list corresponds to an entity.

How to use the list view

- Page size

You can use the **Change View** function to set the value for **Page Size**, which changes the maximum number of rows that the list shows at a time. You can use the **Change View** function to change the column width, and to show or hide columns, if it is applicable for the current list (see "Change View of a List" on page 23).

- Layout

To increase or decrease the width of a column, move the mouse pointer over the right-side edge of the column header, then click and drag. Alliance Access Configuration discards any changes to column widths at the end of the current session, unless you use the **Change View** function to save the changes.

You can use the **Change View** function to show specific columns in a specific order in the list.

You can use the reset option of the **Change View** function to restore the list to its original layout.

See "Change View of a List" on page 23.

- Navigation

If the total number of rows is greater than the value set for the page size, then you can navigate through the pages of the list:

- If the list does not currently show the last row, then the **Next** link is available at the far right of the list button bar. If you click **Next**, then the list shows the next page of rows.
- If the list does not currently show the first row, then the **Previous** link is available at the far right of the list button bar. If you click **Previous**, then the list shows the previous page of rows.

- Actions

The buttons that are present and that are available (not greyed-out) in the button bar depend on the entities currently selected. You can perform some actions on several entities at once. You can perform some actions only on one entity at a time.

Some lists allow you to click an entity and view its details, either in the page view or in a window.

- Selection

To select an entity from the list, select the corresponding check box. To select all the entities from the list, select the check box in the column header.

The system performs action on the entities that you selected only after you select an action that is valid for the selected entities. If you click a button in the list button bar that corresponds to an action that is valid, then the system performs the action only on the entities currently selected.

To sort a list

You can sort the rows in a list in ascending or descending order based on the content of a particular column.

If you click a column header, then Alliance Access Configuration sorts the list in ascending order according to the content of that column. Alliance Access Configuration places a symbol that points upwards next to the name of the column header to indicate that the sort order is ascending. If you click the same column header again, then Alliance Access Configuration sorts the list in descending order according to the content of that column and the symbol points downwards. If you click the same column header again, then Alliance Access Configuration removes the sorting.

Alliance Access Configuration sorts only the rows that are present on each of the pages of the list, therefore the sort order is not sequential across the pages of the list.

The sort order that you define is available throughout the user session. Logging out and in again restores the default order. You can also use the **Change View** function (open and click  Save) to restore the default order (see "Change View of a List" on page 23).

Sorting is also available in pickers that present content as rows in a table, as described in "User Assistance" on page 38.

3.3.2 Form View

Description

Some pages and windows display a form to search for information or to enter information in Alliance Access Configuration.

Some forms display related information in two or more tabs to make the form easier to navigate.

You can find the following types of information in a form:

- Details of an entity
- Search criteria
- Filtering criteria

You can find the following types of information in several tabs within a form:

- Details of an entity
- Details of a message

- Details of a routing rule
- Search criteria

Example

Components

Forms in Alliance Access Configuration usually contain these elements:

Title

The top left of the page view or the window shows the title of the form.

Fields

Different types of fields are available to show details of the entity, or configuration parameters:

- Text field
- Field with a drop-down list
- Selection list (see "Selection Lists" on page 19)
- Check box

The fields can have these additional features to assist with content input:

- Buttons
- Pickers to help you enter data in a field (see "Pickers" on page 39)

Button bar

- The button bar is usually at the bottom of the form.

The buttons enable you to perform an action for the entity that is currently selected. The buttons that are available depend on the selected entity and on the permissions assigned to your operator profile.

How to use the form view

- **Navigation**

If a form contains two or more tabs, then you can click a tab to show the corresponding view.

If the form shows the details of an entity in a list, then you can navigate to the details of the other entities in the list:

- If the page or the window does not currently show the details of the last entity, then **Next** is available at the far right of the button bar. If you click **Next**, then the page or window shows the details of the next entity.
- If the page or the window does not currently show the details of the first entity, then **Previous** is available at the right of the button bar. If you click **Previous**, then the page or window shows the details of the previous entity.
- If the page currently shows the details of an entity from a list of search results, then the **Search Results** link is available at the top right of the form. If you click **Search Results**, then the page shows the corresponding list of search results.

- **Data input or modification**

If you change existing information or add new information, then the button bar shows **Save** and **Cancel**:

- Click **Save**, to save the information or changes.
- Click **Cancel**, to discard the changes that you made.

- **Actions**

The buttons that are present and that are available (not greyed-out) in the button bar depend on the entity currently displayed.

3.3.3 List within a Form

Description

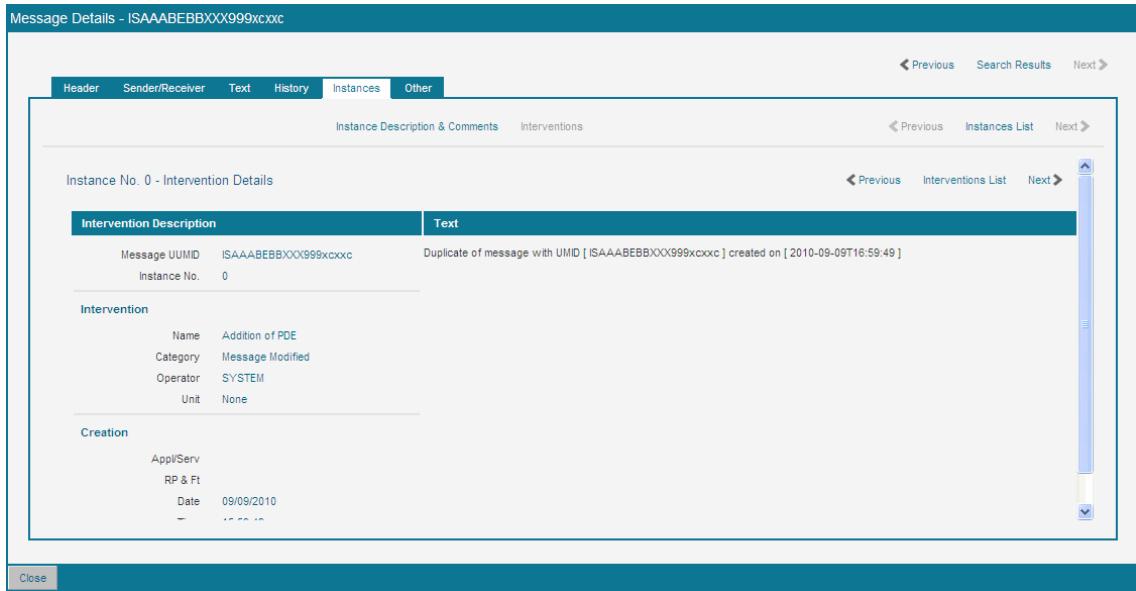
Some pages and windows in Alliance Access Configuration contain multiple levels of information.

Some forms contain lists that show a next level of entities. These lists enable you to navigate to additional information about the entities that they contain, which in turn can lead to other lists that contain further levels of entities.

You can find the following types of information in a list within a form:

- Interventions for an instance
- Scheduled actions
- Routing rules

Example



The screenshot shows the 'Message Details' window for message UMD [ISAAABEBBXXX999xcxxc]. The 'Instances' tab is selected. The main content area displays 'Instance No. 0 - Intervention Details'. The intervention list is titled 'Intervention Description' and includes a 'Text' column. The first item in the list is a duplicate message with UMD [ISAAABEBBXXX999xcxxc] created on [2010-09-09T16:59:49]. The intervention details show the following information:

Intervention	Text
Message UMD	ISAAABEBBXXX999xcxxc
Instance No.	0
Name	Addition of PDE
Category	Message Modified
Operator	SYSTEM
Unit	None

Below the intervention list, there is a 'Creation' section with the following details:

Creation	Text
App/Server	
RP & Ft	
Date	09/09/2010

How to use a list within a form

- General

The generic behaviour for lists and forms is applicable, as described in "List View" on page 14 and "Form View" on page 16.

- Multi-level navigation

Alliance Access Configuration provides navigational links where applicable to enable you to move between entity levels and between entity details within the same entity level.

3.3.4 Selection Lists

Description

Some pages and windows in Alliance Access Configuration display a list that enables you to select one or more values for a field.

The following elements are available:

- Available list**

This contains the list of available values for the current field.

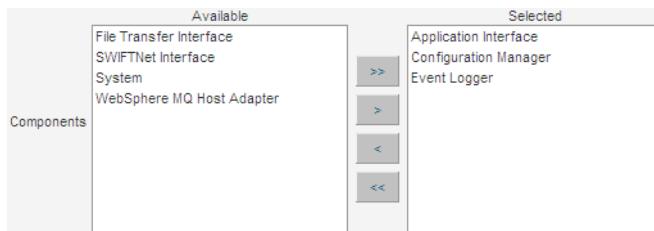
- Selected list**

This contains the list of selected values for the current field.

- Arrow buttons

The arrow buttons move the values from one list to the other.

Example



How to use the selection lists

- Selection

You can use these actions to select values from the **Available** list:

- To select a single value, click the value.
- To select a sequential group of values, either click and then drag the mouse pointer over the values, or click a value and then hold down the **SHIFT** key and click another value.
- To select a group of values that are not sequential, click a value and then hold down the **CTRL** key and click the other values.

- Reassignment

If you double-click a value in either list, then it moves to the other list.

[>] and **[<]** move the selected values from one list to the other.

[>>] and **[<<]** move all the values from one list to the other.

3.4 Common Actions in Task Pages

About this section

This section describes the actions that the administrator user performs frequently in the task pages of Alliance Access Configuration.

3.4.1 Common Buttons in Task Pages

Buttons

These buttons enable you to perform actions that are common to the task pages throughout the Alliance Access Configuration workspace:

Button	Description
Cancel	Cancels the current action.
Change View	Changes the layout of the list for the current page. Procedure: "Change View of a List" on page 23
Clear	Clears values in fields or resets the search criteria fields or the filtering criteria fields to the default values
Close	Closes the current window

Button	Description
 Next	Displays the next set of information, as applicable: <ul style="list-style-type: none"> On a page that contains a list, it displays the next page of entities. In a details window, it displays the details of the next entity.
 OK	Confirms the current action.
 Previous	Displays the previous set of information, as applicable: <ul style="list-style-type: none"> In a list, it displays the previous page of entities. In a details window, it displays the details of the previous entity.
 Refresh	Refreshes the information that the system currently displays.
 Report	Produces a report. Procedure: "Run a Report" on page 24
 Save	Saves the current information.
 Search	Searches using criteria provided on the current page. Procedure: "Perform a Search" on page 22
 Submit	Filters the list that the system currently displays. Procedure: "Filter a List" on page 23

3.4.2 Perform a Search or Filter a List

About this section

This section describes how to perform a search or to filter a list.

3.4.2.1 Criteria and Functions

Criteria

Where the functionality is available, you can use criteria to search or to filter the list for the current page for a specific set of information.

This is the behaviour for the search or filtering operation:

- If you do not specify a value for a criterion, then the system does not take that criterion into account.
- If you specify more than one value for a criterion, then the system uses an OR relationship to evaluate these values.
- If you specify values for more than one criterion, then the system uses an AND relationship to evaluate these criteria.

Wildcards

Some of the search criteria and the filtering criteria fields allow you to use these wildcards:

Wildcard	Purpose	Example
% (percent)	Replaces one or more contiguous unknown characters in a string	<p>a%a matches for example the following strings:</p> <ul style="list-style-type: none"> • aba • afedpa • azhg jdhsa
_ (underscore)	Replaces one unknown character in a string	<p>aa_a matches for example the following strings:</p> <ul style="list-style-type: none"> • aala • aaGa

Functions

The search criteria areas and the filtering criteria areas contain the following:

Button	Description
	Hides the content of the search criteria area or the filtering criteria area Present only when the content is visible
	Shows the content of the search criteria area or the filtering criteria area Present only when the content is hidden
	Resets the search criteria fields or the filtering criteria fields to the default values
	Populates the list of entities according to the current search criteria values Present only in search criteria areas
	Filters the list of entities according to the current filtering criteria values Present only in filtering criteria areas
	Enables you to produce reports of the entities returned by the search or filtering criteria as well as the search or filtering criteria

3.4.2.2 Perform a Search

Purpose

Where available, the **Search** function provides the list that is displayed in the current page.

Procedure

1. Use the input methods that are applicable to specify the search criteria that you require in the fields that are available:
 - Type the values.
 - Select values from a drop-down list.
 - Select values from a selection list.

2. Click **Search**.

The system provides a new list to include only the entities that match the search criteria.

3.4.2.3 Filter a List

Purpose

Where available, the filter function enables you to filter the list that is displayed currently.

Procedure

1. Use the input methods that are applicable to specify the filtering criteria that you require in the fields that are available:
 - Type the values.
 - Select values from a drop-down list.
 - Select values from a selection list.
2. Click **Submit**.

The system updates the list to include only the entities that match the filtering criteria.

3.4.3 Change View of a List

Purpose

The **Change View** function changes the layout of the list for the current page or window.

You can use the **Change View** function to the following:

- specify the maximum number of rows that the list shows at a time (page size)
- show or hide columns
- change the order of the columns
- save changes to column widths
- reset a list to the default layout, including column width
- reset a list to the default layout, except for column width changes

Change list layout

1. If you want to increase or decrease the width of a column in the list, then move the mouse pointer over the right-side edge of the column header, then click and drag.
 2. Repeat the previous step for the other columns in the list, as necessary.
 3. Click **Change View**.
- The **Change View** window opens.
4. Use these methods to change the list layout, as necessary:
 - Select or clear the check box for a column to show or hide it.
 - Click the name of a column and use the up or down arrow to change its position in the list.

5. If you made any changes to the column widths in the current list, then select or clear the **Save Column Widths** check box, as necessary.

If you select the **Save Column Widths** check box, then the system saves the changes to the column widths and retains them in subsequent sessions.

If you clear the **Save Column Widths** check box, then the system discards the changes to the column widths when the current session ends.

6. Type the number of rows for the list to show at a time into the **Page Size** field, if it is available.

The value must be between 10 and 999.

7. Click **OK**.

The **Change View** window closes and the list layout changes accordingly.

The system also saves any changes to the column widths, if the **Save Column Widths** check box is selected.

Reset list layout

1. Click **Change View**.

The **Change View** window opens.

2. If you made any changes to the column widths in the current list, then select or clear the **Save Column Widths** check box, as necessary.

If you select the **Save Column Widths** check box, then the system saves the changes to the column widths and retains them in subsequent sessions.

If you clear the **Save Column Widths** check box, then the system discards the changes to the column widths when the current session ends.

3. Click **Reset** and then click **OK**.

The **Change View** window closes and the system restores the original layout of the list:

- the default page size
- the original set of columns in the original sequence
- the original column widths (if the **Save Column Widths** check box is cleared)

3.4.4 Run a Report

Purpose

The **Report** function enables you to run a report about information in the database.

The **Report** function is available in several places:

- in the search or filtering criteria area of a page
- in the button bar of a list
- in the bottom button bar of a page or a window

Output

You can use the **Report** function to produce these types of reports:

- **Summary report**

Available only from pages that contain lists of entities, this report type enables you to include the information from at least one or more columns on the page for every entity included in the report.

- **Details report**

This report type includes all details for every entity included in the report. You can only choose the output format and formatting options.

If available in the search or filtering criteria area of a page, then the corresponding report includes all the entities that the current search or filtering criteria return as well as the current values for search or filtering criteria.

Generate a report

1. If applicable, select the entities in the list that you want to include in the report.
2. Click **Report**.

The **Report** window opens.

3. If applicable, select the report type.
4. Select the options that you require for the output format and formatting.
5. For summary reports, you can choose the columns for which details should be included in the report from the **Available** list.
6. Check the options **Display Expanded Text**, **Include Header/Footer**, and **Message Partner Print Layout** as required.
7. Click **OK**.

The system generates the report:

- If you set the **Output Format** to **HTML**, then the system opens the report in a new browser window.
 - If you set the **Output Format** to another value, then the **File Download** window opens and prompts you to open or save the report file.
8. If necessary, click **Open** to open the report or **Save** to save the report, as you require.

To open the report, you must have a tool installed that reads the corresponding file format: PDF, CSV (only for summary reports), or XLS.

The system opens or saves the report accordingly.

3.4.5 Choose Directory

Purpose

This function enables you to select a directory from the User Space (see "User Space" on page 95).

Procedure

1. Click  next to the corresponding field.
The **Choose Directory** window opens.
 2. Either navigate to the parent folder of directory that you require or add a new directory, as necessary.
 3. Select the directory that you require.
 4. Click .
- The **Choose Directory** window closes and the directory name populates the corresponding field.

3.4.6 Manage Entities

About this section

This section contains the procedures to manage the entities that are available in Alliance Access Configuration.

About entities

Alliance Access Configuration enables you to manage the available Alliance Access entities. The nodes present in Alliance Access Configuration provide access to the corresponding entities. The licence options of the Alliance Access instance and the operating profile of the current operator determine which entity types are available.

3.4.6.1 Add Entities

Add a new entity

When  is available in the button bar of the corresponding page, do the procedure that follows:

1. Click .
- The entity details window opens.
2. Enter the details for the new entity in the fields of the details window.
 3. Click , located at the bottom of the details window.
- The details window closes. The entity details are saved and the new entity appears in the list.

3.4.6.2 Edit Entities

Change the details of an entity

1. Click the entity.

- The entity details window opens.
2. Change the details of the entity using the input method that is available in the corresponding fields:
 - Select the value required from the drop-down list of the field.
 - Type the value required in the field.
 - Select or clear the check box.

Cancel and **Save** appear at the bottom of the details window.
 3. Click **Save** at the bottom of the details window.
- The details window closes and the changed entity details are saved.

3.4.6.3 Clone Entities

Clone an existing entity

When **Clone** is available in the button bar of the corresponding page, do the procedure that follows:

1. Select the entity to clone.
 2. Click **Clone**.
- The entity details window opens with the details of the selected entity copied into the fields.
3. Change the details as required, using the input method that is available in the corresponding fields:
 - Select the value required from the drop-down list of the field.
 - Type the value required in the field.
 - Select or clear the check box.
 4. Click **Save**, located at the bottom of the **Add** window.
- The **Add** window closes. The new entity details are saved.

3.4.7 Manage Scheduled Actions

About this section

This section describes scheduled actions that enable you to automate various Alliance Access processes.

3.4.7.1 How Scheduling Works

Overview

At the start of each day (midnight), Alliance Access checks the calendar and determines which day types apply to the current day. For example, today may be the First Working Day of Week and the First Working Day of Month. Alliance Access then checks to see whether any operations are scheduled for these day types. If an operation is scheduled, then Alliance Access carries it out at the specified time, unless the server is running in housekeeping mode.

The schedule is also rebuilt after each restart of the server. If the restart occurs between the earliest and latest start times of an event, then that event is started automatically.

You must add a calendar for the current year before you can schedule any processes to occur automatically. See "Calendars" on page 102.

3.4.7.2 Tabs with Scheduled Actions Lists

Content

Tabs with scheduled action lists contain these elements:

- Configuration parameters that allow you to configure the settings for the scheduled actions
See "Configuration parameters" on page 29
- Functions that enable you to manage the scheduled actions
See "Functions" on page 29
- Details of the scheduled actions

The details are described in the section "Scheduled Action Details Window" on page 29.

Display

Example

Scheduled Actions					Rows in list: 1 , in selection: 0
	Add	Delete			
<input type="checkbox"/>	1	Every Day	00:00	Select Input	

Configuration parameters

Configuration parameter	Definition
Category	<p>Determines the values that are available to use to specify when the scheduled actions occur</p> <p>If you change the value, then all the existing scheduled actions are deleted.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Business Day: when this option is selected, specific days from the business week may be selected (peak working day, normal working day, holiday). • Business Month: when this option is selected, you may select specific days from the business month (first working day, middle working day). • Business Week: when this option is selected, you may select specific days from the business week (first working day of the week, last working day of the week, other working day of the week, holiday). • Every Day: when this option is selected, no particular day is specified. The set action is carried out every day, at the same time. • Specific Day: when this option is selected, any day from Sunday to Saturday can be selected.
Calendar	<p>Specifies the calendar to use for the scheduled actions</p> <p>Valid only for these entities:</p> <ul style="list-style-type: none"> • FIN Logical Terminals • Emission Profiles • Reception Profiles

Functions

Function	Description
 Add	Enables you to add a scheduled action Procedure: "Add a Scheduled Action" on page 33
 Delete	Deletes the scheduled actions that are currently selected

3.4.7.3 Scheduled Action Details Window

Content

The **Scheduled Action Details** window contains these elements:

- Details of the scheduled actions

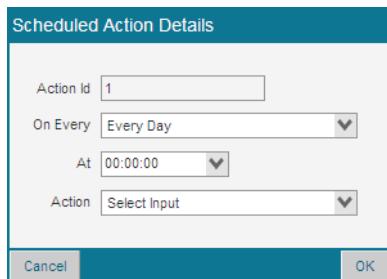
See "Details" on page 30

Display

Example

Scheduled Action Details

Action Id	<input type="text" value="1"/>
On Every	<input type="text" value="Every Day"/>
At	<input type="text" value="00:00:00"/>
Action	<input type="text" value="Select Input"/>



Details

Field	Description
Action Id ⁽¹⁾	The numerical identifier of the scheduled action Maximum nine digits
Category ⁽²⁾	The value that is set for the Category configuration parameter (see "Configuration parameters" on page 29)

Field	Description
On Every	<p>When the scheduled action occurs</p> <p>If Category is set to <code>Business Day</code>, then these are the possible values:</p> <ul style="list-style-type: none"> • Normal Working Day • Peak Working Day • Holiday <p>If Category is set to <code>Business Month</code>, then these are the possible values:</p> <ul style="list-style-type: none"> • First Working Day • Middle Working Day <p>If Category is set to <code>Business Week</code>, then these are the possible values:</p> <ul style="list-style-type: none"> • First Working Day • Last Working Day • Other Working Day • Holiday <p>If Category is set to <code>Every Day</code>, then these are the possible values:</p> <ul style="list-style-type: none"> • Every Day <p>If Category is set to <code>Specific Day</code>, then these are the possible values:</p> <ul style="list-style-type: none"> • Sunday • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday
At⁽¹⁾	<p>The time that the scheduled action starts</p> <p>Format: <code>HH:MM:SS</code></p>
Earliest Start⁽²⁾	<p>The earliest time that the scheduled action starts</p> <p>Format: <code>HH:MM:SS</code></p>
Latest Start⁽²⁾	<p>The latest time that the scheduled action starts</p> <p>Format: <code>HH:MM:SS</code></p>

Field	Description
Action⁽¹⁾	<p>For the FIN Logical Terminals entity, these are the possible values:</p> <ul style="list-style-type: none"> • Select Input: to perform a login to Application Control (APC), select FIN and send messages • Select Output: to perform a login to APC, select FIN and receive messages • Select Input & Output: to perform a login to APC, select FIN and send and receive messages • Logout: to quit FIN and logout from Application Control (APC) <p>When you select Select Output or Select Input & Output, a selection list appears where you can select the delivery subsets to be assigned to the logical terminal.</p> <p>For the Emission Profiles and Reception Profiles entities, these are the possible values:</p> <ul style="list-style-type: none"> • Activate: activates the emission or reception profile • Deactivate: deactivates the emission or reception profile
Delivery Subsets	<p>The type of messages that the logical terminal receives from the SWIFT network</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • NORMAL • SYSTEM • URGENT <p>Valid only for the FIN Logical Terminals entity and present only when Action is set to Select Output or Select Input & Output</p>
Mode	<p>The type of backup the system performs</p> <p>For the Event Archive Backups and Message Archive Backups entities, these are the possible values:</p> <ul style="list-style-type: none"> • Backup: to create a backup of the archive, without deleting the archive • Remove: to delete an archive that has the status DONE, without creating a backup for the archive • Backup and Remove: to create a backup of the archive, and then delete the original archive after the backup is complete <p>For the Recovery Backups entity, these are the possible values:</p> <ul style="list-style-type: none"> • Incremental Backup • Full Backup

(1) Valid only for the **FIN Logical Terminals**, **Emission Profiles**, and **Reception Profiles** entities

(2) Valid only for the **Restart/Stop**, **Database Backups**, **Recovery Backups**, **Event Log Archives**, **Event Archive Backups**, **Message File Archives**, **Message Archive Backups**, and **BIC Directory** entities

3.4.7.4 Add a Scheduled Action

Purpose

This procedure enables you to add a scheduled action for an applicable Alliance Access process.

Users and permissions

To add a scheduled action, your operator profile must have these actions:

- **System Management / Restart SWIFTAlliance** (for restart / stop)
The **Store schedule** permission must be set to Yes.
- **System Management / Backup** (for database backups)
The **Store schedule** permission must be set to Yes.
- **System Management / Manage Rec Backup** (for recovery backups)
- **Event Journal / Archive** (for event log archives)
- **System Management / Backup** (for event archive backups)
The **Store schedule** permission must be set to Yes.
- **Message File / Archive** (for message file archives)
The **Store schedule** permission must be set to Yes.
- **System Management / Backup** (for Message archive backups)
The **Store schedule** permission must be set to Yes.
- **Correspondent Info / Install Bankfile** (for BIC directory)
The **Store schedule** permission must be set to Yes.
- **SWIFT Interface / Add Action, Modify Action, Remove Action** (for logical terminals)
- **SWIFTNet Interface / Schedule EProf** (for emission profiles)
The **Add Action**, **Modify Action**, and **Remove Action** permissions must be set to Yes.
- **SWIFTNet Interface / Schedule RProf** (for reception profiles)
The **Add Action**, **Modify Action**, and **Remove Action** permissions must be set to Yes.

Prerequisites

Before scheduling the archiving of messages or events, you must have configured the number of days for which to keep messages or events available in the database from the **Configuration** tab.

For database backups, recovery backups, event archive backups, and message archive backups, you must have configured the backup in the **Configuration** tab.

To schedule the installation of a Bank Update File, a Bank Update File must be available in the UpdateBIC file directory.

The operation mode must be set to **Automatic** for scheduled actions to be taken into account.

If there are any untreated alarms for the events that you are archiving, then these alarms are also archived and can no longer be treated.

Procedure

1. Click **Add** on the **Scheduling** tab of the corresponding entity page or details window.
For the **Restart/Stop** entity, go to the **Restart** or **Stop** tab and click **Add**.
For the **Recovery Backups** entity, select **Time Schedule** in the **Recovery Backup Trigger** drop-down list and click **Add**.
The **Scheduled Action Details** window opens.
2. Select or enter the values that you require, as necessary in the fields that are available.
3. Click **OK**.
The **Scheduled Action Details** window closes.
The new scheduled action appears in the list of scheduled actions.
4. Click **Save**.

The system adds the scheduled action.

For backups, if a backup or restore process is running at the time the backup is scheduled, the scheduled backup is not performed and an event is logged in the event log. Also, a scheduled backup does not take into account archives that are either under construction (that is, the archive process is running), or being consulted.

3.4.8 Manage Alliance Gateway Connections

About this section

This section describes the functionality in Alliance Access Configuration for connections to Alliance Gateway.

3.4.8.1 About Alliance Gateway Connections

Overview

To connect to SWIFTNet, Alliance Gateway connections must be configured. You can define Alliance Gateway connections from the **Gateway Connectivity** page. See "Gateway Connectivity" on page 76 for more details.

Once Alliance Gateway connections have been defined, you can assign them to logical terminals, emission profiles, or reception profiles.

3.4.8.2 Connections to Alliance Gateway Lists

Content

Connections to Alliance Gateway lists contain these elements:

- Functions that enable you to manage the connections to Alliance Gateway
See "Functions" on page 35
- Details of the connections to Alliance Gateway
See "Details" on page 35

Display

Connections to Alliance Gateway					Rows in list: 2 , in selection: 1
	Add	Delete	Move down	Move up	
<input type="checkbox"/>	1	SAG			
<input type="checkbox"/>	2	test			

Functions

Function	Description
Add	Enables you to add an Alliance Gateway connection Procedure: "Add an Alliance Gateway Connection" on page 37
Delete	Deletes the Alliance Gateway connections that are currently selected
Move down	Moves the Alliance Gateway connection that is currently selected down in the list
Move up	Moves the Alliance Gateway connection that is currently selected up in the list

3.4.8.3 Gateway Connection Details Window

Content

The **Gateway Connection Details** window contains these elements:

- Details of the Alliance Gateway connections
See "Details" on page 35

Display

Gateway Connection Details

Sequence 1	
Connection Name <input type="text" value="SAG"/>	
Use Specific Authoriser DN <input checked="" type="checkbox"/>	
Authoriser DN <input type="text" value="o=saaabebb, o=swift"/>	
Use Specific CID Signing DN <input checked="" type="checkbox"/>	
CID Signing DN <input type="text" value="o=saaabebb, o=swift"/>	
<input type="button" value="Cancel"/>	<input type="button" value="OK"/>

Details

Field	Description
Sequence	The sequence number of the connection
Connection Name	The name of the connection
Use Specific Authoriser DN	<p>Determines whether the connection uses a specific authoriser DN For more information about the certificate that is used in this case, see the following sections:</p> <ul style="list-style-type: none"> • "Authoriser DN for logical terminals" on page 36 • "Certificates used if no Authoriser DN is specified" on page 36

Field	Description
Authoriser DN	<p>The specific authoriser DN that the connection uses to sign messages. Present only when the Use Specific Authoriser DN check box is selected. The value that you specify must comply with the DN format described in the SWIFTNet Naming and Addressing Guide.</p> <p>If an Authoriser DN is specified, then Alliance Gateway uses the certificate of that DN to sign messages and delivery notifications.</p> <p>For reception profiles that use the delivery mode store-and-forward, the authoriser DN must have been granted access from an external RBAC application to the queue indicated in the Queue Name field in the reception profile.</p>
Use Specific CID Signing DN⁽¹⁾	Determines whether the connection uses a specific CID signing DN. If you are using FINCopy, you have to indicate a Central Institution Destination (CID) signing DN, that is the DN which should sign the FINCopy authorisations.
CID Signing DN⁽¹⁾	The specific CID signing DN that the connection uses. Present only when the Use Specific CID Signing DN check box is selected

(1) Valid only for the **FIN Logical Terminals** entity

Authoriser DN for logical terminals

The following are requirements for the authoriser DN for logical terminals:

- If the logical terminal belongs to a live destination, then the certificate of the authoriser DN must be a business certificate and must be stored on a Hardware Security Module (HSM) with policy ID 1.3.21.6.2.
- If the logical terminal belongs to a Test and Training destination, then the certificate of the authoriser DN can be:
 - a business certificate
 - a Lite certificate

This certificate can be stored in an HSM or on disk.

Certificates used if no Authoriser DN is specified

If you do not select an Authoriser DN, then Alliance Gateway determines the certificate to use to sign incoming and outgoing traffic, and real-time delivery notifications.

Alliance Gateway selects the DN certificate in the list of the related gateway message partner that matches the level-2 DN (BIC8) for which a security context can be created (for example, the certificate is not revoked or expired):

- store-and-forward emission profile, if not Authoriser DN was specified
- store-and-forward reception profile, if not Authoriser DN was specified
- real-time emission profile, if not Authoriser DN was specified
- real-time reception profiles

It is not possible to specify the Authoriser DN for real-time reception profiles

- real-time delivery notifications

3.4.8.4 Add an Alliance Gateway Connection

Purpose

This procedure enables you to add an Alliance Gateway connection for an applicable Alliance Access entity.

Users and permissions

To add an Alliance Gateway connection, your operator profile must have this action:

- **SWIFT Interface / Modify LT** (for logical terminals)
- **SWIFTNet Interface / Modify EProf** (for emission profiles)
- **SWIFTNet Interface / Modify RProf** (for reception profiles)

Prerequisites

If the server is running in Operational mode, then you must first stop the SWIFT Interface Services (SIS) component before assigning an Alliance Gateway connection and an authoriser DN to a logical terminal.

You can assign an Alliance Gateway connection and an authoriser DN to an emission profile or a reception profile if the profile is **Disabled**.

Procedure

1. Click **Add** on the **Configuration** tab of the corresponding entity page.
The **Gateway Connection Details** window opens.
2. Select or enter the values that you require, as necessary in the fields that are available.
3. Click **OK**.

The **Gateway Connection Details** window closes.

A new item for the connection appears in the **Connections to Alliance Gateway** list.

4. Click **Save**.

The system adds the connection.

For logical terminals, when you have completed this procedure, restart the SWIFT Interface Services (SIS) component.

3.5 Online Help

Description

All pages within Alliance Access Configuration contain the **Help** link in the upper-right corner of the navigation area of the workspace. Most windows in Alliance Access Configuration also contain the **Help** link in the title bar because the link on the page is not available when a window is open.

Clicking the **Help** link displays the online help that corresponds to the page or entity that is currently selected. It also enables you to navigate to other topics within the online help.

Help for entering values in fields

Alliance Access Configuration provides tools to help you enter values with the correct syntax, for example, how to select and enter dates or times. For more information, see "User Assistance" on page 38.

Behaviour

If you click the **Help** link, then the corresponding help file opens in a new window. The system opens the help file at the content that corresponds to the page or entity that is currently selected.

You can use the navigational links that are available in the help window to show other topics from within the online help.

The page or window from which you click the **Help** link determines the topics that the system shows:

- If you click the **Help** link on the login page or the home page, then the system opens the Alliance Web Platform online help.
- If you click the **Help** link on a page or window within Alliance Access Configuration, then the system opens the Alliance Access Configuration online help.

3.6 User Assistance

About this section

This section describes the user assistance that is available to help you enter data in fields in Alliance Access Configuration using the correct format and syntax. For example, you can use a picker to select dates or times in the correct format.

For more information about the purpose of a field, or a description of the values that you can enter, see "Online Help" on page 37.

3.6.1 Relative Date and Time Values

Date and time values

Alliance Access Configuration enables you to enter values manually or to select values from a picker for fields that require date or time values. For more information about pickers, see "Pickers" on page 39.

You can enter relative values in date or time fields.

A relative value is automatically converted to an absolute date or time value when the cursor leaves the field. The conversion generates an absolute date or time value that corresponds to the syntax for the field. The absolute value is calculated relative to the current date or time of the host running the browser. For example, use a relative value to calculate quickly the date "five days ago".

The relative date calculation supports dates within the range of years 1970 to 2037.

Syntax

The following is the syntax used to enter relative date or time values:

`<symbol><number><unit>`

Where:

Variable	Values
<symbol>	+ or -
<number>	a numeric value
<unit>	d, m, or y for a date field, with d as default h, m, or s for a time field, with h as default Uppercase letters are accepted. The expected syntax for a field determines which values are relevant.

Examples

Typed value	Field type	Result
+6h or +6	Time	Alliance Access Configuration increases the current time by six hours.
-7d or -7	Date	Alliance Access Configuration sets the date to seven days before the current date.
+0 or -0	Time	Alliance Access Configuration sets the time to the current time.
+0 or -0	Date	Alliance Access Configuration sets the date to the current date.

3.6.2 Pickers

Description

A picker is a graphical element that is located beside a field in some pages and windows. It helps you to enter data according to the correct syntax and format that the field requires.

If Alliance Access Configuration shows  to the right of a field, then the picker lets you enter the following types of information:

- a path name using the **Choose Directory** function
For more information, see "Choose Directory" on page 25.
- data that is appropriate to the field, such as a date

Types of pickers

These are the different types of pickers available within Alliance Access Configuration:

- Date picker (see "Date Picker" on page 39)
- Time picker (see "Time Picker" on page 41)
- BIC picker (see "BIC Picker" on page 41)

3.6.3 Date Picker

Purpose

A date picker enables you to select and enter a date using the correct format in the date field.

Example of a date picker

The following is an example of the calendar that appears in a date picker:



Date formats

To view the format of the data that a field requires, move the mouse over the picker icon or the field.

The Alliance Web Platform administrator defines the date format that Alliance Access Configuration displays. For information about how to change the default date format, see "Alliance Web Platform Configuration Parameters" in the [Alliance Web Platform Administration and Operations Guide](#).

The date picker supports these date formats:

Date format	Example
YYYY/MM/DD	16 June 2012 is represented as: 2012/06/16
DD/MM/YYYY	16 June 2012 is represented as: 16/06/2012
MM/DD/YYYY	16 June 2012 is represented as: 06/16/2012

How to use a date picker

To open the date picker, click .

Select the values for the year, the month, and the day. If required, navigate to another year or month by clicking the arrow icons in the top left or right corners of the calendar.

The content of the field that is related to the picker determines the subsequent behaviour of the picker:

- If the field already contains a value that is syntactically correct, then the picker is set to that value.
- If the field is set to a date that is not valid (for example, 31 February 2009), then the colour of the date field changes. You must select a valid date in the correct format.

Type a date in a date field

You can type a date directly in the date field without using a date picker. The date that you type must use the correct format that the field requires.

Tip When you enter a date directly in the date field, you can omit the separator.

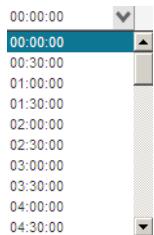
You can also enter a relative date, such as plus one month or minus five days. For information about relative dates, see "Relative Date and Time Values" on page 38.

3.6.4 Time Picker

Purpose

Alliance Access Configuration requires that a value entered in a time field be syntactically correct. The time picker enables you to select a time and then adds it to the field using the correct syntax. To open the time picker, click .

Example



Allowed values

The time picker enables you to select a time from a drop-down list, which is either on the hour or at a half past the hour. To enter a more specific time, for example 10:13:45, you can enter it directly in the time field.

When you enter a time, it is not necessary to include the colons, but you must include leading zeros where applicable. For example, you can enter either 082500 or 08:25:00.

If you enter a time that does not follow this syntax, then the time picker ignores it and sets the field to its default value.

Tip	You can also enter a relative time, such as plus 1 hour, or minus 5 minutes. For information about relative times, see "Relative Date and Time Values" on page 38.
------------	--

How to use a time picker

When the time picker is opened, the content of the related field determines the subsequent behaviour of the time picker:

- If the field does not contain a value, then the time picker drop-down list does not display any selected time.
- If the field already contains a value that is not syntactically correct, then the same behaviour occurs as if the field does not contain a value.
- If the field already contains a value that is syntactically correct and is a time on the hour or half hour, then the time picker is set to that value.

3.6.5 BIC Picker

Purpose

Alliance Access Configuration requires that a business identifier code (BIC) value entered in a relevant field be syntactically correct. The BIC picker enables you to search for BIC information based on values that you specify. Then, it adds the information about the selected BIC from the search results, to the field or fields, using the correct syntax.

The BIC picker is only available if your operator profile has the **Correspondent Info** entity selected.

Example

Search Criteria								
Type	SWHQ%	Institution Name	Branch	City	Country Code	Department	First Name	
Department		First Name		Last Name				
<input type="button" value="Clear"/> <input type="button" value="Search"/>								
Rows in list: 20 , in selection: 0								
◀ Previous Next ▶								
	Institution	Institution Name	City	Country Code	Branch	Department	Last Name	First Name
<input type="checkbox"/>	SWHQBEBBADS	SWIFT HEADQUAR	LA HULPE	BE	(ADMINISTRATION SERVICES)			
<input type="checkbox"/>	SWHQBEBBBCT	SWIFT HEADQUAR	LA HULPE	BE	(BROADCAST REQUESTS ON			
<input type="checkbox"/>	SWHQBEBBBIL	SWIFT HEADQUAR	LA HULPE	BE	(CUSTOMER BILLING SERVICI			
<input type="checkbox"/>	SWHQBEBBBRD	SWIFT HEADQUAR	LA HULPE	BE	(MEMBERSHIP MANAGEMENT			
<input type="checkbox"/>	SWHQBEBBE2E	SWIFT HEADQUAR	LA HULPE	BE	(END-TO-END ORDERING DEP			

Search criteria

The BIC picker enables you to enter a value in one or more search criteria and then click **Search** or press **ENTER** to submit the criteria.

Choose the type required from the **Type** drop-down list:

- Institution
- Department
- Individual

Depending on the type of BIC required, the BIC picker offers these fields as search criteria:

Field	Description
Institution	To search based on the BIC or part of it. If lower-case letters are typed, then they are converted to upper-case letters. If a value is already typed in the field in Alliance Access Configuration, then it is proposed in this field in the criteria. If the entered value is less than the expected value, then the wildcard % is added automatically. The wildcard _ can also be used.
Institution Name	To search based on the name of the institution or part of it. This is a case-sensitive field. Wildcards can be used.
Branch	To search based on the branch name of the institution or part of it. This is a case-sensitive field. Wildcards can be used.
City	To search based on the city name of the institution or part of it. This is a case-sensitive field. Wildcards can be used.
Country Code	To search based on the country code of the institution or part of it. If lower-case letters are typed, then they are converted to upper-case letters. Wildcards are not allowed.
Department	To search based on department-related information for an institution. This is a case-sensitive field.
First Name	To search based on a person's first name. This is a case-sensitive field.

Field	Description
Last Name	To search based on a person's last name. This is a case-sensitive field.

Note The wildcard % replaces one or more contiguous unknown characters in a string.
The wildcard _ replaces one unknown character.

How to use the BIC picker

To open the picker, click  .

Provide values for the search criteria and initiate the search.

The BIC picker sorts the search results in alphanumerical order by institution. The list shows no more than 20 search results at a time. If necessary, Alliance Access Configuration truncates the values to display them in the column width that is available.

Clicking a row in search results adds the information about the BIC in the relevant field or fields.

You can move the mouse over a row in the search results to display the complete institution name, city, and branch information.

You can sort the rows in the search results by clicking the name of a column.

Search results

The search results from the BIC picker contain some or all of the following columns based on the type of BIC required:

- Institution
- Institution Name
- Branch
- City
- Country Code
- Department
- Last Name
- First Name

3.7 Preferences

About this section

This section describes the preferences that you can set for some of the pages in Alliance Access Configuration.

3.7.1 Change the Preferences

Impact of changes

Some preferences will take effect after you log in the next time. The changes to preferences apply only to you, and not to other users.

Procedure

1. Click the **Preferences** link in the navigation area of the Alliance Access Configuration workspace.

The **Preferences** window opens.

The fields in the window vary depending on the task window that was open when you clicked the **Preferences** link.

2. To change the value of a setting, select the option you want from the drop-down list next to the setting:

Preference	Task window	Description
Date Format	Instances	Select either to use the default AWP server value, or a specific format (for example, American or European). You must restart the application for any changes to take effect.
Amount Format	Instances	Select either to use the default server value, or a specific format (for example, Decimal-Comma/Thousands-Nothing). You must restart the application for any changes to take effect.

3. Click **OK** to confirm the changes or **Cancel** to discard the changes.

4 Initial Configuration for SWIFTNet

4.1 Introduction

Purpose

This section describes the configuration that an Alliance Administrator must complete before you can send and receive FIN, InterAct, and FileAct messages.

Prerequisites

The following prerequisites apply:

- Connectivity setup. For details, see "Check Connectivity" on page 45.
- SWIFTNet Link 7.0 is installed and configured on the system that hosts Alliance Gateway 7.0.
- You have installed or upgraded to Alliance Gateway 7.0.
- You have set up valid certificates for an Authoriser DN.

Tasks related to the management of certificates are performed on Alliance Gateway. For more information, see the [Alliance Gateway Administration and Operations Guide](#).

- You have installed or upgraded to Alliance Access 7.1. For details, see the *Installation Guide* for [AIX](#), [Linux](#), [Oracle Solaris](#), or [Windows](#).

Configuration tasks

The main tasks are:

- Checking connectivity
- Defining Alliance Access in Alliance Gateway
- Configuring Alliance Access for FIN messaging
- Configuring Alliance Access for InterAct and FileAct messaging.

4.2 Check Connectivity

4.2.1 Configure SWIFT DNS Servers

Description

Before you can use your connection correctly, ensure that you have access to the SWIFT DNS servers. For details of configuring the SWIFT DNS servers, see the *SWIFTNet Link Installation Guide* for [AIX](#), [Linux](#), [Oracle Solaris](#), or [Windows](#).

Note To configure the DNS, you do not need the SNLOwner account. You can use a Windows Administrative account on Windows, or the root account on UNIX.

4.2.2 Confirm Connectivity

Description

You must ensure that the host computer can successfully reach the necessary ports on the SWIFT systems. The ports that must be accessible are defined in the [Connectivity to SWIFT - Network Configuration Tables Guide](#).

Before proceeding with the SWIFTNet Link installation, confirm your Network Connectivity by executing the **checkip** program, as explained in the [SWIFTNet Link Operations Guide](#). This program contacts all necessary ports and checks whether they are open and can be reached.

If this connectivity test is not successful, then the next step (SWIFTNet Link installation) will fail.

4.3 Define Alliance Access in Alliance Gateway

Overview

This section explains how to:

- set up Alliance Access as a message partner in Alliance Gateway, with **Relaxed SNL Format** selected
- define Alliance Access as an endpoint on Alliance Gateway.

These steps are similar whether you are configuring for FIN, InterAct, or FileAct messaging. Only the message partner and endpoint names differ.

4.3.1 Guidelines for Names

Message partner names

When Alliance Access connects to an Alliance Gateway system, it must provide a unique message partner name. The Alliance Access message partner name is derived from its instance name.

Alliance Access creates the message partner name with the characters `crs_` (for CREST messaging), `fin_` (for FIN messaging), or `sni_` (for InterAct and FileAct messaging) followed by a normalised Alliance Access instance name.

A normalised Alliance Access instance name is the Alliance Access instance name, reduced to lower case with underscores removed and truncated to 10 characters. The name can have a maximum of 14 characters.

For example, if the Alliance Access instance name is `SAA_Rel_70`, then the message partner name must be `crs_saarel70` (for CREST messaging), `fin_saarel70` (for FIN messaging), or `sni_saarel70` (for InterAct and FileAct messaging).

Note If you have multiple Alliance Access systems connecting to SWIFTNet through Alliance Gateway, then ensure that each system has a unique instance name.

On Alliance Web Platform, the instance name is displayed in the bottom banner area.

Endpoint names

When Alliance Access connects to SWIFTNet, it must provide an Endpoint name. Alliance Access always uses an Endpoint name that is identical to its message partner name.

4.3.2 FIN Messaging

4.3.2.1 Set Up a Message Partner in Alliance Gateway

Overview

You must configure your Alliance Access instance as a message partner in Alliance Gateway. This must be completed for each Alliance Access system that connects to this Alliance Gateway system.

- Note**
- If you have performed a fresh installation of Alliance Gateway 7.0 on your system, then a default message partner called **fin_relaxed** is provided. This message partner has the correct settings for connection between Alliance Access and Alliance Gateway. You can use the settings of this message partner as an example to create your **fin_<your_instance_name>** message partner.
 - You must select **Relaxed SNL Format** as default message format for emission and reception.

To set up a message partner for FIN messaging from the Alliance Gateway Administration interface on Alliance Web Platform

Add a new message partner as described in the section on managing message partners in the [Alliance Gateway Administration and Operations Guide](#), with the following details:

1. In the **General** tab, for the message partner and SWIFTNet Link Endpoint, enter a **Name**. Enter a unique message partner name based on the Alliance Access instance name. See "Guidelines for Names" on page 46.
2. In the **Type** drop-down list, select **ClientServer**.
3. In the list of **Supported Message Formats**, select the **Relaxed SNL Format** check box.
4. In the **Default Message Format for Emission** drop-down list, select **Relaxed SNL Format**.
5. Add the certificates for relaxed mode by clicking **Add**.
6. In the **Host Adapters** tab, select the **Local Authentication** and **Remote API Host Adapter** check boxes.
7. Select **Remote API Host Adapter** in the **Server Host Adapter** drop-down list.
8. Click **Save**.
9. Select the new message partner and click **Enable**.

4.3.2.2 Define Alliance Access as an Endpoint on Alliance Gateway

Overview

When data arrives from SWIFTNet into Alliance Gateway, it has the Endpoint name embedded in the data. Alliance Gateway must know how to route this data to the correct Alliance Access system.

This section explains how to configure Alliance Gateway with this routing information.

Note Before you define the Endpoint, you must have defined the message partner to be used by the Endpoint.

If you have performed a fresh installation of Alliance Gateway 7.0 on your system, then a default Endpoint called *fin_relaxed* is provided. You can use the settings of this endpoint as an example to create your *fin_<your_instance_name>* endpoint.

To define an Endpoint from the Alliance Gateway Administration interface on Alliance Web Platform

Add a new Endpoint as described in the section on managing Endpoints in the [Alliance Gateway Administration and Operations Guide](#), with the following details:

1. In the **General** tab, enter the message partner name that you defined in "Set Up a Message Partner in Alliance Gateway" on page 47 in the **Endpoint Name** field.
2. In the **Sequence** field, indicate a sequence number. It is the order in which Alliance Gateway evaluates the messages against the endpoints.
3. In the **Destination** area:
 - In the **To** drop-down list, select **Application Interface**.
 - In the **Application** drop-down list, select the message partner name that you defined in "Set Up a Message Partner in Alliance Gateway" on page 47.
 - In the **Mode** drop-down list, select **Relaxed**.
4. In the **Cryptographic Protocol** drop-down list, select **Advanced**.
5. Ensure that the **Namespace Declarations** check box is not selected.
6. In the **Error Code** drop-down list, select **Old**.
7. In the **Routing Criteria** tab, in the **SNL Endpoint** drop-down list, select **Equals** and enter the message partner name that you defined in "Set Up a Message Partner in Alliance Gateway" on page 47, in the second subfield.
8. In the **Traffic Type** drop-down list, select **All**.
9. Click **Save**.
10. Select the new endpoint and click **Enable**.

4.3.3 InterAct and FileAct Messaging

4.3.3.1 Set Up a Message Partner in Alliance Gateway

Overview

For InterAct and FileAct messaging, you must also configure Alliance Access as an additional message partner in Alliance Gateway. This must be completed for each Alliance Access system that connects to this Alliance Gateway system.

-
- | | |
|-------------|--|
| Note | <ul style="list-style-type: none"> • The message partner definition for the SWIFTNet Interface component (for InterAct and FileAct messaging) also follows a defined naming convention. The message partner name is also derived from the Alliance Access instance name, but with <code>sni_</code> as its prefix, that is, <code>sni_<your_instance_name></code>. • You must select Relaxed SNL Format as default message format for emission and reception. |
|-------------|--|
-

To set up a message partner for InterAct and FileAct messaging from the Alliance Gateway Administration interface on Alliance Web Platform

Add a new message partner as described in the section on managing message partners in the [Alliance Gateway Administration and Operations Guide](#), with the following details:

1. In the **General** tab, for the message partner and SWIFTNet Link Endpoint, enter a **Name**. Enter a unique message partner name based on the Alliance Access instance name. See "Guidelines for Names" on page 46.
2. In the **Type** drop-down list, select `ClientServer`.
3. In the list of **Supported Message Formats**, select the **Relaxed SNL Format** check box.
4. In the **Default Message Format for Emission** drop-down list, select `Relaxed SNL Format`.
5. Add the certificates for relaxed mode by clicking **Add**.
6. In the **Host Adapters** tab, select the **Local Authentication** and **Remote API Host Adapter** check boxes.
7. Select `Remote API Host Adapter` in the **Server Host Adapter** drop-down list.
8. Click **Save**.
9. Select the new message partner and click **Enable**.

4.3.3.2 Define Alliance Access as an Endpoint on Alliance Gateway

Overview

When data arrives from SWIFTNet into Alliance Gateway, it has the Endpoint name embedded in the data. Alliance Gateway must know how to route this data to the correct Alliance Access.

This section explains how to configure Alliance Gateway with this routing information.

-
- | | |
|-------------|---|
| Note | Before you define the Endpoint, you must have defined the message partner to be used by the Endpoint. |
|-------------|---|
-

To define an Endpoint from the Alliance Gateway Administration interface on Alliance Web Platform

Add a new Endpoint as described in the in the section on managing Endpoints in the [Alliance Gateway Administration and Operations Guide](#), with the following details:

1. In the **General** tab, enter the message partner name that you defined in "Set Up a Message Partner in Alliance Gateway" on page 48 in the **Endpoint Name** field.
2. In the **Sequence** field, indicate a sequence number. It is the order in which Alliance Gateway evaluates the messages against the endpoints.

3. In the **Destination** area:
 - In the **To** drop-down list, select Application Interface.
 - In the **Application** drop-down list, select the message partner name that you defined in "Set Up a Message Partner in Alliance Gateway" on page 48.
 - In the **Mode** drop-down list, select Relaxed.
4. In the **Cryptographic Protocol** drop-down list, select Advanced.
5. Ensure that the **Namespace Declarations** check box is not selected.
6. In the **Error Code** drop-down list, select Old.
7. In the **Routing Criteria** tab, in the **SNL Endpoint** drop-down list, select Equals and enter in the second subfield:
 - For the SnF traffic type, the SNL Endpoint should be the same as the message partner name that you defined in "Set Up a Message Partner in Alliance Gateway" on page 48, for example, sni_access.
 - For the RealTime traffic type, the SNL Endpoint will depend on the RealTime service definition. Such a service will have one or more Primary or Backup route endpoints; this must be specified in the SNL Endpoint in Alliance Gateway. This information is extracted from the final cn levels in the Primary or Backup Route, with the order reversed:

Primary Route: cn=ap1, cn=snl, cn=snl12345,ou=it1,o=swift,o=swift
Primary end point: snl_ap1

For example, in the case of Service: swift.generic.fa, the primary route for a BIC such as SWHQBEBB can be cn=sft, cn=snl, cn=snl12345,ou=it1,o=swift,o=swift, so the SNL endpoint will be snl_sft.

In either type of SNL Endpoint, you can further segregate the traffic based on information such as Requestor DN, Responder DN, service, Traffic Type, and so on.
8. In the **Traffic Type** drop-down list, select All.
9. Click **Save**.
10. Select the new endpoint and click **Enable**.

4.3.4 CREST Messaging

4.3.4.1 Setting Up the CREST Message Partner in Alliance Gateway

Overview

You must configure the CRNet component of Alliance Access as an additional message partner in Alliance Gateway. This must be completed for each Alliance Access system that connects to this Alliance Gateway system.

-
- | | |
|-------------|--|
| Note | <ul style="list-style-type: none"> • The message partner definition for the CRNet component also follows a defined naming convention. The message partner name is also derived from the Alliance Access instance name, but with <code>crs_</code> as its prefix, that is, <code>crs_<your_instance_name></code>. • You must select Relaxed SNL Format as default message format for emission and reception. |
|-------------|--|
-

To set up a message partner for the CRNet component

Add a new message partner as described in the creating a client/server message partner section of the [Alliance Gateway Operations Guide](#), with the following details:

1. For the message partner and SWIFTNet Link Endpoint, enter a **Name**. Enter a unique message partner name based on the Alliance Access instance name. See "Guidelines for Names" on page 46.
2. In the **Type** field, select **ClientServer**.
3. In the **Host Adapter** field, select **Remote API Host Adapter**.
4. For the **Default Message Format for Emission (from Message Partner)** field, select **Relaxed SNL Format**.
5. In the **Supported Message Formats** section, select **Relaxed SNL Format**. Move it from the **Available** to the **Selected** column by highlighting it and clicking the transfer icon.
6. In the **Additional Processing** section, select **Remote API Host Adapter** and **Local Authentication**, then define the Local Authentication keys.
7. Add the **Certificates for Relaxed Mode** to the message partner details by clicking **[Add]**.
8. Save the message partner details.
9. Finally, enable the message partner. See the [Alliance Gateway Operations Guide](#).

4.3.4.2 Defining the CRNet Component as an Endpoint on Alliance Gateway

Overview

When data arrives from SWIFTNet into Alliance Gateway, it has the Endpoint name embedded in the data. Alliance Gateway must know how to route this data to the correct Alliance Access.

This section explains how to configure Alliance Gateway with this routing information.

-
- | | |
|-------------|---|
| Note | Before you define the CRNet component Endpoint, you must have defined the message partner to be used by the Endpoint. |
|-------------|---|
-

To define an Endpoint for the CRNet component

Add a new Endpoint as described in the [Alliance Gateway Operations Guide](#), with the following details:

1. In the **Routing** tab:
 - in the **Name** field, enter the message partner name that you defined in "Set Up a Message Partner in Alliance Gateway" on page 48.

- in the **SNL Endpoint** field, select **Equals (=)** in the **Relation** subfield and enter **snl_crest** in the second subfield.
 - in the **Responder DN** field, specify a value for the Responder DN.
 - in the **Traffic Type** field, select **All**.
2. In the **Destination** tab:
- in the **Interface** field, select **Application Interface**.
 - in the **Application** field, select the message partner name that you defined in "Define Alliance Access as an Endpoint on Alliance Gateway" on page 47.
 - from the **Mode** option buttons, select **Relaxed**.
3. Save this configuration.
4. Finally, enable the Endpoint. See the [Alliance Gateway Operations Guide](#).

4.3.5 Data Encryption/Gateway Authentication between Alliance Access and Alliance Gateway

Description

If you have decided to use Data Encryption/Gateway Authentication between Alliance Access and Alliance Gateway, then perform these steps:

- On Alliance Gateway, create a Private Key and Certificate. See the [Alliance Gateway Administration and Operations Guide](#).
- On Alliance Access, configure the SSL settings on Remote API. See the [Alliance Gateway Remote API Operations Guide](#).

For information on the directory to be used in Alliance Access, see the section on the **SWIFTNet Connection Details** window in the [System Management Guide](#).

4.4 Configuring Alliance Access for FIN Messaging

Overview

To configure Alliance Access to send and receive FIN messages, you must:

- define an Alliance Gateway connection
- assign an Alliance Gateway connection to a Logical Terminal
- send and receive a Test MT message
- set up your access to the SWIFTNet FIN Test service (only if you are a vendor).

Requirements

When a FIN message is sent from Alliance Access over SWIFTNet, it is enveloped in an InterAct message. In addition, relationship management authorisations for the live RMA service are also exchanged as InterAct messages over SWIFTNet. An Authoriser DN signs the InterAct messages that are sent over SWIFTNet.

Therefore, the logical terminal that sends the message must be mapped to an Authoriser DN, as follows:

Role to assign to Authoriser DN	Associated Alliance Gateway message partner
<p>The fin role for the swift.fin service. In other words, such an Authoriser DN is a certified FIN User.</p>	<p><code>fin_<instance></code></p>

Connection Handling - SNL handling

By default, only the security officers, and the R7.1_Supervisor and R7.1_Superkey operator profiles can manage the Alliance Gateway connections. Assign these permissions to other operators, as needed.

If you use Local Authentication between Alliance Gateway and Alliance Access, then you can assign the two parts of the Local Authentication Key in the **SNL Handling** function (**SWIFTNet Support**) to a single operator, or separately to two operators. By default, the Security Officers (LSO and RSO) only have one part of the Local Authentication Key in the **SNL Handling** function assigned.

When assigning permissions, ensure that **Connection Handling** in the **SNL Handling** function is set to Yes.

For more information about assigning permissions, see "Operator Profiles" on page 241.

4.4.1 Define an Alliance Gateway Connection

Overview

You define an Alliance Gateway connection from **System > Gateway Connectivity**.

The default Alliance Gateway connection is created with the name **SAG** with pre-defined settings.

For detailed information about maintaining Alliance Gateway connections, see "Gateway Connectivity" on page 76.

4.4.2 Assign an Alliance Gateway Connection to a Logical Terminal

Overview

For information about assigning an Alliance Gateway connection to a Logical Terminal, see "FIN Logical Terminals" on page 343.

4.4.3 Install a Message Syntax Table

Overview

If a new message syntax table is available, then download and install it in Alliance Access. For more information, see "Install a New Message Syntax Table" on page 183.

You can download the message syntax table from www.swift.com > Support > Resources > [Download Centre](#).

4.4.4 Send and Receive a Test MT Message

Procedure

1. Ensure that the Alliance Access servers are running in operational mode.
2. Log on to Alliance Message Management as an operator with message processing entitlements and navigate to **Creation > FIN Message: New**.
3. Create an MT999 (free format message) to be sent from your Test and Training destination (which is assigned to SWIFTNet) addressed back to your Test and Training destination. The **Sender Logical Terminal (Sender part)** and **Institution (Receiver part)** fields in the message must be the same. Your Test and Training destination is the one that ends with 0.
4. Route the message to the **_SI_to_SWIFT** queue.
5. Log on to Alliance Access Configuration and navigate to **SWIFTNet Interface > FIN Logical Terminals**.
6. With the Test and Training logical terminal, log on to SWIFT and select FIN so that the queued message can be sent and received.
7. Check the status of the Test and Training logical terminal from the **Monitoring** tab of the **FIN Logical Terminal Details** window. The logical terminal must be selected and have one normal FIN pending message queued for transmission.
8. Navigate to **Routing > Queues**.
9. Open the **_SI_to_SWIFT** queue details and go to the **Monitoring** tab.
10. Click **Show Message Instances** and in the **Message Instances in Queue** window that opens, search for the MT999.

4.4.5 Access to the SWIFTNet FIN Test Service (Vendors only)

Important

To connect to the SWIFTNet FIN test-infrastructure (FIN Vendor Testbed (VTB) through the SWIFTNet Integration Testbed (ITB)), you must access the **swift.fin!x** service.

A system variable (**SERVICE_NAME**) must be set with the value **swift.fin!x**.

Important This section applies only to SWIFT, its partners, and vendors (your BIC must start with PT).

Procedure on Windows

1. Click **Start** and then select **Control Panel/System**.
2. Click the **Change settings** link.
3. In the windows that appears, click **Environment Variables** in the **Advanced** tab.
4. Click **New** to create a system variable and give it the name **SERVICE_NAME** and set the value to **swift.fin!x**.
5. Click **OK** to apply, then click **OK** again to save the changes.

Procedure on UNIX

1. Log on to UNIX as Alliance administrator.
2. Using vi or another text editor, open the file **\$HOME/.swa.\$ALLIANCE_INSTANCE.rc**.
3. Add the following line:

```
export SERVICE_NAME=swift.fin!x
```
4. Close and save the file.

The variable is only taken into account after closing and re-opening the **System Administration** window.

-
- Note** If the servers are running while setting the variable, then you must do the following:
- Stop the Alliance Access servers and the bootstrap.
 - Close the **System Administration** window, and open it again.
 - Start the Alliance Access bootstrap and the servers.
-

4.5 Configuring Alliance Access for InterAct and FileAct Messaging

Overview

To configure Alliance Access to send and receive InterAct and FileAct messages, you must:

- define a Gateway connection
- install Application Service Profiles
- configure SWIFTNet emission and reception profiles
- send and receive an InterAct or a FileAct message.

-
- Note** FileAct messages should not be sent to a stand-alone Alliance Access.
-

Requirements

When an InterAct or FileAct message is sent from Alliance Access over SWIFTNet, it is enveloped in an InterAct message. In addition, relationship management authorisations for the live RMA service are also exchanged as InterAct messages over SWIFTNet. An Authoriser DN signs the InterAct messages that are sent over SWIFTNet.

Therefore, the emission profile that sends the message must be mapped to an Authoriser DN, as follows:

Role to assign to Authoriser DN	Associated Alliance Gateway message partner
The appropriate role for the SWIFTNet Business service	sni_<instance>

4.5.1 Define a Gateway Connection

Overview

You must define a Gateway connection to assign to the SWIFTNet emission and reception profiles. For more information, see "Define an Alliance Gateway Connection" on page 53.

4.5.2 Install Application Service Profiles

Overview

You must install the latest Application Service Profiles on Alliance Access to send and receive traffic correctly for InterAct or FileAct services.

For more information, see "Application Service Profiles" on page 364, or the command "saa_manageasp" in the *Administration Guide* for [AIX](#), [Linux](#), [Oracle Solaris](#), or [Windows](#).

4.5.3 Configure SWIFTNet Emission and Reception Profiles

Purpose

To exchange messages through SWIFTNet, you must define, enable, and activate SWIFTNet emission and reception profiles for InterAct and FileAct messaging, and also for the RMA service.

You perform these tasks from **SWIFTNet Interface > Emission Profiles or Reception Profiles**.

During the installation or upgrade of Alliance Access, an emission profile and a reception profile is created automatically for each live licensed BIC8 for the live RMA service.

Permissions

By default, only the R7.1_Supervisor and R7.1_Superkey operator profiles have the permissions to manage emission and reception profiles. You can assign these permissions to other operators, if necessary.

To configure SWIFTNet profiles

1. Navigate to **SWIFTNet Interface > Emission Profiles or Reception Profiles**.

Add emission and reception profiles for each licensed BIC8, and assign the Gateway connection to the profiles. Open the details of the profiles and on the **Configuration** tab, click **Add** (see "Add an Alliance Gateway Connection" on page 37). Configure an emission and a reception profile for each licensed BIC8.

Note During the installation or upgrade of Alliance Access, an emission profile and a reception profile is created automatically for each live licensed BIC8 for the live RMA service.

Tip For emission profiles, there must be one emission profile per BIC8 and per SWIFTNet business service.

2. If required, add input and output channels.

Navigate to **SWIFTNet Interface > Input Channels or Output Channels** (see "Create an Input Channel on SWIFTNet" on page 395 and "Create an Output Channel on SWIFTNet" on page 414).

Then navigate to **SWIFTNet Interface > Emission Profiles** or **Reception Profiles** and assign the channels to the emission and reception profiles (see "Add an Emission Profile" on page 386 or "Add a Reception Profile" on page 407).

3. Enable and activate each emission and reception profile. See "Enable and Activate an Emission Profile" on page 389 and "Enable and Activate a Reception Profile" on page 409.

Enabling a profile makes it ready for use, and activating it starts message traffic.

4.5.4 Install MX Message Standards

Overview

If required, install MX message standards. See "Install a Message Standard" on page 186.

4.5.5 Send and Receive a Test InterAct Message

Procedure

This procedure applies to InterAct messages only:

1. Ensure that the Alliance Access servers are running in operational mode.
2. Log in to Alliance Message Management as an operator that has permissions to create and process messages.

Navigate to **Creation > MX Message: New**.

3. Create an MX message.
4. Route the message to the **_SI_to_SWIFTNet** queue.
5. Verify that an emission profile is available for the SWIFTNet business service to be used.

Verify that a reception profile is available to receive MX messages from the same SWIFTNet business service.

To verify this, log on to Alliance Access Configuration and navigate to **SWIFTNet Interface > Emission Profiles**, and **Reception Profiles**.

6. Enable and activate the emission profile and reception profile so that the queued MX message can be processed.
7. Check the status from the **Monitoring** tab of the **Emission Profile Details** and **Reception Profile Details** windows. The profiles must be **Enabled / Active** and have one normal pending message queued for transmission.
8. Navigate to **Routing > Queues**.
9. Open the **_SI_to_SWIFTNet** queue details and select the **Monitoring** tab.
10. Click **Show Message Instances**, and in the **Message Instances in Queue** window that opens, search for the MX message.

Note To create a test FileAct message, from the Message Management GUI, navigate to **Creation > File Message: Send**.

4.6 Configuration for Sanctions Screening

Overview

This section provides an overview of the configuration tasks that are required before Alliance Access can support the screening of messages as part of Sanctions Screening.

For more information about how Sanctions Screening works, see the [Sanctions Screening Service Description](#).

Possible results of sanctions screening

When the Sanctions Screening service processes a message, the following results are possible:

- The message does not generate an alert (field tag 433 : /AOK).
- A string in an MT message matches an element of your selected sanctions list. In this case, the result is one of the following:
 - **False positive** (field tag 433 : /FPO)
Sanctions Screening generates an alert that your compliance officer investigates, and then authorises message delivery.
 - **True hit** (field tag 433 : /NOK)
Sanctions Screening generates an alert that your compliance officer investigates, and then confirms as a true match with the element of the sanctions list.

Warning message for a true hit

If the message is a true hit, then the field tag 433 in block 3 of an MT message contains 433 : /NOK.

You can view the warning message through a message search and message print:

- **message search**

The **Message Details - Header** tab displays the following warning message: Sanctions screening - Message blocked.

Depending on the value of the configuration parameter **Display/Print FIN User Header**, the **Message Details - Text** tab displays block 3 of MT messages.

- **message print**

The first sentence of the warning header contains the following: **Sanctions screening - Message blocked**.

Depending on the value of the configuration parameter **Display/Print - FIN User Header**, the printed report of the **Message Details** displays block 3 of MT messages.

Configuration tasks

1. Change the value of the configuration parameter, **Display/Print - FIN User Header** to always display block 3 in the Message details, and to always print block 3.
For more information about the configuration parameters, see "Display/Print" on page 117.
2. You can define conditional routing rule using the keyword **FIN_user_header** to route any message that Sanctions Screening flags as a true hit.

For more information about message keywords, see "List of Message Keywords" on page 517.

5 System

5.1 System Check

Introduction

System checks enable you to quickly assess if your operating system configuration is compliant with the SWIFT configuration requirements for Alliance Access.

The system check page displays the actual configuration values found and the expected values. If the requirements are not met, then the information provided enables you to co-ordinate with your system administrator and take the actions required to make the alignments during scheduled maintenance.

5.1.1 System Check Page

Content

The **System Check** page contains these elements:

- Status of the system check
See "Status" on page 60
- Details of the system check
See "Details" on page 61

Display

System Check

System Check				Rows in list: 3
Name	Result	Actual	Expected	
OS version	passed	Windows 2008 Server R2	Windows 2008 Server R2	
Installed patches	reported	Not Available		
uptime	passed	70 day(s)	90 day(s)	

Execution Date and Time 2010/10/18 20:30:00

Result Succeeded

Attention: the expected values displayed may vary depending on the parameters and how the system is used.
Click the Help link above for more information and check the release letter to get the current values.

Status

Field	Description
Execution Date and Time	The date and time of the system check
Result	<p>This field specifies the overall result of the system check.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Succeeded • Failed

Details

Column	Description
Name	The name of the feature that was checked See "System Check names" on page 61
Result	<p>The result of the check</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • passed • failed (the actual value is not sufficient when compared to the expected value) • reported <p>Depending on your system configuration, the system check may show a passed result although the actual values do not meet the expected values.</p>
Actual	The content checked for a feature
Expected	The expected value of the feature according to SWIFT requirements

System Check names

Name	Applicable platforms	Description
dev_attributes - maxuproc	AIX	Maximum number of processes per user
dev_attributes - fullcore	AIX	Full core dump
dev_attributes - ncargs	AIX	Maximum size of the ARG/ENV list
Ulimit - processes	AIX or Linux	User limits
IPC Resources - kernel.semmsl	Linux Linux	Linux kernel settings
IPC Resources - kernel.semnn		
IPC Resources - kernel.semopm		
IPC Resources - kernel.semnni		
IPC Resources - kernel.shmall		
IPC Resources - kernel.shmmax		
IPC Resources - kernel.shmmni		
IPC Resources - fs.file-max		

IPC Resources - max-msg-qbytes	Oracle Solaris	Oracle Solaris or Linux kernel settings
IPC Resources - max-sem-ids		
IPC Resources - max-sem-nsems		
IPC Resources - max-shm-ids		
IPC Resources - max-shm-memory		
IPC Resources - max-sem-ops		
IPC Resources - max-msg-ids		
IPC Resources - max-msg-messages		
Kernel Parameters - noexec_user_stack		
Mount options	Oracle Solaris or Linux	File system nosuid mount option
Ulimit - nofiles	AIX, Oracle Solaris, Linux	User limits
Ulimit - coredump		
Ulimit - data		
Ulimit - file		
Ulimit - stack		
Ulimit - memory		
Ulimit - time		
Paging space	AIX, Oracle Solaris, Linux	System paging space
OS patch level	AIX, Oracle Solaris, Linux	OS level check
uptime	AIX, Oracle Solaris, Linux, or Windows	Number of days since the system was rebooted
OS version	AIX, Oracle Solaris, Linux, or Windows	OS version check
Installed patches	Windows	Reports the Service Pack on Windows

5.1.2 Run a System Check

Purpose

This procedure explains how to run a system check.

Users and permissions

To run a system check, your operator profile must have this action:

- **Access Control / Embedded Checks**

Procedure

- From the **System Check** page, click **Run**.

A status popup message appears.

The result of the system check is displayed.

5.2 Software Integrity Check

Introduction

The software integrity check verifies the integrity of the files for the installed Alliance Access software. The result of the check indicates whether any software files were added, removed, or updated.

5.2.1 Software Integrity Check Page

Content

The **Software Integrity Check** page contains these elements:

- Status of the software integrity check
See "Status" on page 63
- Details of the software integrity check
See "Details" on page 64

Display

Software Integrity Check

Execution Date and Time 05/10/2010 23:00:00

Result Added: 5 files, removed: 0 files, changed: 24 files

Software Integrity Check		Rows in list: 29 , in selection: 0
Change View	Run Software Integrity Check	
<input type="checkbox"/>	Name	Result
<input type="checkbox"/>	C:\Alliance\Access\WSS\lib\win32\libWS_calendar.dll	file owner, group ID, file contents changed
<input type="checkbox"/>	C:\Alliance\Access\WSS\lib\win32\libWS_connection.dll	file owner, group ID, file contents changed
<input type="checkbox"/>	C:\Alliance\Access\WSS\lib\win32\libWS_rma.dll	file owner, group ID, file contents changed
<input type="checkbox"/>	C:\Alliance\Access\lappsrv\loc4\j2ee\home\applications\calendar\META-INF\MANIFEST.MF	file owner, group ID changed

Status

Field	Description
Execution Date and Time	The date and time of the software integrity check
Result	<p>The summary information of the software integrity check</p> <p>The result includes the following values along with the corresponding number of files:</p> <ul style="list-style-type: none"> • added • removed • changed <p>If 0 files appears next to each value, then this means that the software integrity check is successful.</p>

Details

If the software integrity check is successful, then the following details are empty:

Column	Description
Name	The location and the name of the file
Result	<p>The result of the check</p> <p>These are the possible values:</p> <ul style="list-style-type: none">• Added• Removed• File content changed

5.2.2 Run a Software Integrity Check

Purpose

This procedure explains how to run a software integrity check.

Users and permissions

To run a software integrity check, your operator profile must have this action:

- **Access Control / Embedded Checks**

Procedure

- From the **Software Integrity Check** page, click **Run**.

A status popup message appears.

The result of the software integrity check is displayed.

If the check is successful, then the **Software Integrity Check** details are empty.

5.3 Database Integrity Check

Introduction

The database integrity check verifies the integrity of files in the database of the Alliance Access server. The result of the check indicates any problem detected. You can view entity-specific details for any check that failed.

5.3.1 Database Integrity Check Page

Content

The **Database Integrity Check** page contains these elements:

- Status of the database integrity check

See "Status" on page 65

- Details of the database integrity check

See "Details" on page 65

Display

Database Integrity Check

Execution Date and Time 2010/10/18 20:30:00

Result Succeeded

Database Integrity Check		Rows in list: 111
Change View	Run	
Name	Result	
inst_oper	Succeeded	
frmt	Succeeded	
appe_20101018	Succeeded	
appe_20101019	Succeeded	
intv_20101018	Succeeded	

Status

Field	Description
Execution Date and Time	The date and time of the database integrity check
Result	<p>The overall result of the database integrity check</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Succeeded • Failed

Details

Column	Description
Name	The name of the table that was checked
Result	<p>The result of the check for a specific table</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Succeeded • Failed

5.3.2 Database Integrity Check Details Window

Content

The **Database Integrity Check Details** window contains these elements:

- Status of the individual table integrity check
See "Status" on page 66
- Details of the individual entity check if the integrity check for the table failed
See "Details" on page 66

Display

Error Details		Rows in list: 1
Entity	Description	
a	mismatch	

Status

Field	Description
Name	The name of the database table that was checked
Result	<p>The result of the check</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Succeeded • Failed

Details

Column	Description
Entity	The name of the entity that was checked
Description	The explanation of the error for an entity

5.3.3 Run a Database Integrity Check

Purpose

This procedure explains how to run a database integrity check.

Users and permissions

To run a database integrity check, your operator profile must have this action:

- **Access Control / Embedded Checks**

Procedure

1. From the **Database Integrity Check** page, click **Run**.

A status popup message appears.

The result of the database integrity check is displayed.

If the check for a table succeeded, then no error details are displayed.

2. Click any row to see details about the check for a specific table.

The **Database Integrity Check Details** window opens. If the check for a table failed, then the window shows any relevant entity and the related explanation.

3. Click **Previous** or **Next** to navigate to the next table.

-
4. Click **Close**.

The **Database Integrity Check Details** window closes.

5.4 Restart/Stop

5.4.1 Housekeeping Mode and Operational Mode

Description

You can stop and restart Alliance Access manually or, if a calendar has been created, schedule and automate these actions.

When doing a restart, you can choose between these modes:

- **Operational:** This is the normal multi-user mode for operating Alliance Access, allowing all functions of Alliance Access to be used. It is the default mode.
- **Housekeeping:** This is a maintenance mode.

In this mode, messages are not sent or received, and queues are frozen. Alliance Access does not run scheduled processes. You cannot search for messages (live or archived) in the database.

By default, only one user can be signed on to Alliance Access at a time. However, it is possible to configure Alliance Access to allow several users to sign on in housekeeping mode.

Tasks that require housekeeping mode

The following tasks can *only* be performed in housekeeping mode:

- install a Message Syntax Table for FIN messages, and set a Message Syntax Table as default
- install, remove, activate or deactivate FIN Copy Profiles

In addition, the following information or functionality is not available in housekeeping mode:

- Gateway connections are not visible.
- You cannot activate or deactivate a correspondent.
- You cannot add or delete countries or currencies.

Start automatically at system boot time

It is possible to start Alliance Access automatically when the machine where Alliance Access is installed is booted. For more information, see the configuration parameter, **Startup Mode**, in the section "System" on page 124.

5.4.2 Restart/Stop Page: Restart Tab

Content

The **Restart** tab contains these elements:

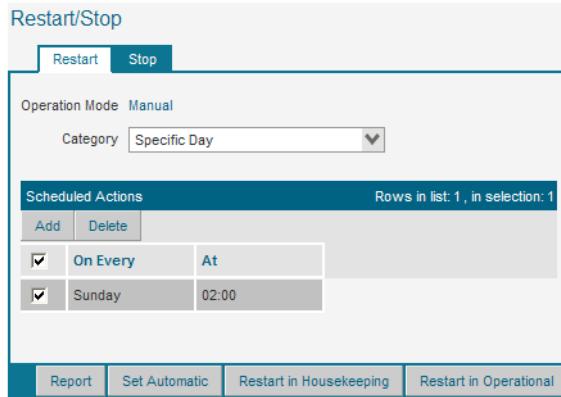
- Details of the available restart scheduled actions

See "Details" on page 68

- Functions that enable you to manage the restart actions

See "Functions" on page 68

Display



Details

Field	Description
Operation Mode	<p>These are the possible values:</p> <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
Category	<p>The functionality for scheduled actions is generic within Alliance Access Configuration:</p> <ul style="list-style-type: none"> • For details of the Restart tab, see "Tabs with Scheduled Actions Lists" on page 28. • For details of the Scheduled Action Details window, see "Tabs with Scheduled Actions Lists" on page 28.

Functions

Function	Description
Add	Enables you to add a scheduled action Procedure: "Add a Scheduled Action" on page 33
Delete	Enables you to delete a scheduled action
Set Automatic / Set Manual	Enables you to set the operation mode to Automatic or to Manual Procedure: "Change the Operation Mode" on page 71
Restart in Housekeeping	When the operation mode is set to Manual , enables you to restart manually Alliance Access in housekeeping mode
Restart in Operational	When the operation mode is set to Manual , enables you to restart manually Alliance Access in operational mode

5.4.3 Restart/Stop Page: Stop Tab

Content

The **Stop** tab contains these elements:

- Details of the available stop scheduled actions
See "Details" on page 69
- Functions that enable you to manage the stop actions
See "Functions" on page 69

Display

The screenshot shows the 'Restart/Stop' page with the 'Stop' tab selected. The 'Operation Mode' is set to 'Manual'. The 'Category' is set to 'Specific Day'. The 'Scheduled Actions' table shows one row: 'On Every' is checked, 'At' is set to '03:00', and 'Sunday' is checked. Buttons at the bottom include 'Report', 'Set Automatic', and 'Stop'.

Details

Field	Description
Operation Mode	These are the possible values: <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
Category	The functionality for scheduled actions is generic within Alliance Access Configuration: <ul style="list-style-type: none"> • For details of the Stop tab, see "Tabs with Scheduled Actions Lists" on page 28. • For details of the Scheduled Action Details window, see "Tabs with Scheduled Actions Lists" on page 28.

Functions

Function	Description
Add	Enables you to add a scheduled action Procedure: "Add a Scheduled Action" on page 33
Delete	Enables you to delete a scheduled action
Set Automatic / Set Manual	Enables you to set the operation mode to Automatic or to Manual Procedure: "Change the Operation Mode" on page 71
Stop	Enables you to stop Alliance Access manually

5.4.4 Stop Alliance Access

Purpose

This procedure enables you to stop Alliance Access manually.

You must shut down Alliance Access before loading a patch or performing any offline backup, file reorganisation, or system upgrade.

Users and permissions

To stop Alliance Access, your operator profile must have this action:

- **System Management / Stop SWIFTAlliance**

Security officers can stop Alliance Access.

Prerequisites

The operation mode must be set to **Manual**.

Procedure

1. From the **Stop** tab, click **Stop**.

The **Stop Confirmation** window opens.

2. Click **OK**.

The **Stop Confirmation** window closes.

A status popup message appears.

You must log off from Alliance Access Configuration.

When you click **Stop**, an alarm for information is logged in the event log. Once the system is shut down, no more message processing is allowed and offline utilities can be run to perform additional system management functions.

5.4.5 Restart Alliance Access in Housekeeping Mode or in Operational Mode

Purpose

This procedure enables you to restart Alliance Access manually.

Each restart involves a shutdown of the servers, followed by an automatic start in the selected operating mode.

Note If there is no active routing schema when stopping the servers, then a restart is only possible in housekeeping mode.

Following any maintenance work in housekeeping mode, you must restart Alliance Access in operational mode.

If a calendar has been created, then you can schedule the servers to restart automatically. See "Add a Scheduled Action" on page 33.

Users and permissions

To restart in housekeeping mode or in operational mode, your operator profile must have this action:

- **System Management / Restart SWIFTAlliance**

Security officers can restart Alliance Access in housekeeping mode or in operational mode.

Prerequisites

The operation mode must be set to **Manual**.

Procedure

1. From the **Restart** tab, click **Restart in Housekeeping** or **Restart in Operational**.

The **Restart Confirmation** window opens.

2. Click **OK**.

A status popup message appears.

3. Log off from Alliance Access Configuration and log on again.

Alliance Access restarts automatically in the selected operating mode.

When you click **Restart in Housekeeping** or **Restart in Operational**, the request for stopping the server generates an alarm for information in the event log.

5.4.6 Change the Operation Mode

Purpose

This procedure enables you to change the operation mode.

Users and permissions

To change the operation mode, your operator profile must have this action:

- **System Management / Restart SWIFTAlliance**

The **Modify operating mode** permission must be set to **Yes**.

Procedure

- From the **Restart** tab or the **Stop** tab, given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

5.5 Components

5.5.1 Description of a Component

Overview

The Alliance Access software is broken down into major functional entities called *components*. The **Components** page lists all registered components with their version number.

You can edit the details of the Alliance Access Developers Kit components only (for unit re-assignment, if required).

Types of components

The Alliance Access software is made of major functional entities called **components**. These components recognise the client-server architecture of Alliance Access (using remote procedure calls between server and client processes).

The following are the main types of components:

- a **Service component** provides services to applications (the server in the client-server architecture model)
- an **Application component** requests services from server components (the client in the client-server architecture model)

The last character of the component name identifies the type of component: 'S' for Service and 'A' for Application.

For a complete list of components in Alliance Access, see the description of the release tree in the *Installation Guide* for [AIX](#), [Linux](#), [Oracle Solaris](#), or [Windows](#).

5.5.2 Components Page

Content

The **Components** page contains these elements:

- Details of the components
See "Details" on page 72
- Functions that enable you to manage the components
See "Functions" on page 74

Display

Components						Rows in list: 20 , in selection: 1	
	Name	Description	Type	Version	Status	◀ Previous	Next ▶
<input type="checkbox"/>	ADK	Alliance Developer's Kit	Alliance Component	Version 7.0	---		
<input checked="" type="checkbox"/>	BSA	Base Support Application	Alliance Component	Version 7.0	---		
<input type="checkbox"/>	BSS	Base Support Services	Alliance Component	Version 7.0	---		
<input type="checkbox"/>	FSS	File Support Services	Alliance Component	Version 7.0	---		
<input type="checkbox"/>	INS	Installation Services	Alliance Component	Version 7.0	---		

Details

Column	Description
Name	The name of the component
Description	The description of the component
Type	<p>The component type</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Alliance Component • ADK Component

Column	Description
Version	The version number of the component
Status	<p>The current status of the component</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Running • Stopped • Disabled • In Transition: intermediate state between Running and Stopped • ---: for base components of Alliance Access which cannot be stopped or started manually

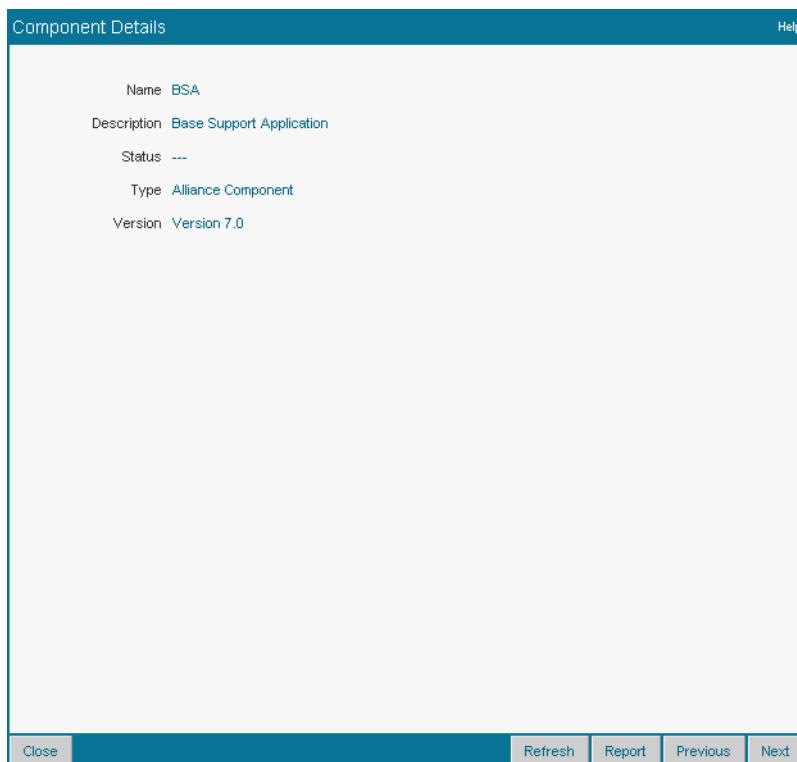
5.5.3 Component Details Window

Content

The **Component Details** window contains these elements:

- Details of the components
See "Details" on page 74
- Functions that enable you to manage the components
See "Functions" on page 74

Display



Details

Field	Description
Name	The name of the component
Description	The description of the component
Status	<p>The current status of the component</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Running • Stopped • Disabled • In Transition: intermediate state between Running and Stopped • ---: for base components of Alliance Access which cannot be stopped or started manually
Type	<p>The component type</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Alliance Component • ADK Component
Version	The version number of the component
Assigned Units	The units that are assigned to the component
Assigned Categories	The categories that are assigned to the component

5.5.4 Component Functions

Overview

These functions enable you to manage the components.

Functions

Function	Description	Components page	Component Details window
Start	<p>Enables you to start a component in operational mode</p> <p>Procedure: "Stop or Start a Component in Operational Mode / Stop a Component in Housekeeping Mode" on page 75</p>	✓	✓
Stop	<p>Enables you to stop a component in operational mode</p> <p>Procedure: "Stop or Start a Component in Operational Mode / Stop a Component in Housekeeping Mode" on page 75</p> <p>You can also stop a component in housekeeping mode</p>	✓	✓

5.5.5 Stop or Start a Component in Operational Mode / Stop a Component in Housekeeping Mode

Purpose

This procedure enables you to stop or start a component in operational mode or stop a component in housekeeping mode.

If the licence package **07:STANDALONE REC** is installed, then SIS (SWIFT Interface Services) and SNIS (SWIFTNet Interface Services) do not appear in the list of components.

If you stop components in housekeeping mode, then these components are not restarted when you restart the servers in operational mode. For example, you can prevent any Alliance Access Developers Kit component, or the SIS (SWIFT Interface Services), SNIS (SWIFTNet Interface Services), SNSS (SWIFTNet Support Services), or MXS (Application Interface Services) components from starting when you restart the servers in operational mode.

Users and permissions

To display the list or the details of components, your operator profile must have these actions:

- **Security Definition / Mod Component** or **System Management / Stop/Start Component** (to display the list)
- **Security Definition / Mod Component** (to display the details)

To stop or start components, your operator profile must have the following additional action:

- **System Management / Stop/Start Component**

Security officers can stop or start components.

Procedure

1. Verify whether you are in operational mode or in housekeeping mode.
2. From the list of components, select the check box of a component in the left column.
3. Click **Stop** or **Start**.

A status popup message appears.

5.5.6 Modify an Alliance Access Developers Kit Component

Purpose

This procedure enables you to modify the units assigned to the Alliance Access Developers Kit components.

Users and permissions

To display the list or the details of components, your operator profile must have these actions:

- **Security Definition / Mod Component** or **System Management / Stop/Start Component** (to display the list)
- **Security Definition / Mod Component** (to display the details)

To modify components, your operator profile must have this action:

- **Security Definition / Mod Component**

Security officers can modify components.

Procedure

1. From the list of components, click the check box of the Alliance Access Developers Kit component that you want to modify.
The **Component Details** window opens.
2. Select the units to assign to the component from the **Assigned Units/Available** list.
3. Select the categories to assign to the component from the **Assigned Categories/Available** list.
4. Click **Save**.
A status popup message appears.
5. Click **Close**.
The **Component Details** window closes.

5.6 Gateway Connectivity

5.6.1 Gateway Connections

Overview

In order to connect to SWIFTNet, Alliance Gateway connections must be configured.

With the change to relaxed certificates, it is no longer required to specify a certificate profile name, HSM name and password when defining Alliance Gateway connections. Only an authoriser DN is required. The mapping between the authoriser DN and the certificate profile name is done in the Alliance Gateway Message Partners configuration.

5.6.2 Gateway Connectivity Page

Content

The **Gateway Connectivity** page contains these elements:

- Details of the Alliance Gateway connections
See "Details" on page 77
- Functions that enable you to manage the Alliance Gateway connections
See "Functions" on page 81

Display

Gateway Connectivity			
Gateway Connections			
Rows in list: 1 , in selection: 1			
Change View	Add As	Delete	Mark As Reliable
<input checked="" type="checkbox"/>	Name	Host Name	Status
<input checked="" type="checkbox"/>	SAG	bewx206	Reliable

Details

Column	Description
Name	The name of the Alliance Gateway connection
Host Name	The IP address or host name of the Alliance Gateway instance
Status	<p>Indicates whether the connection between Alliance Access and the SWIFTNet Link host is Reliable or Not Reliable. The Alliance Gateway connection status can only be modified when the SIS and SNIS components are stopped.</p> <p>If the status is Not Reliable (because the local authentication failed), the message transfer over the Alliance Gateway connection is stopped immediately until the status becomes reliable again. An event is logged in the Event Log with detailed information on the failure.</p> <p>Alliance Gateway connections that do not use local authentication keys are always Reliable.</p>

5.6.3 Gateway Connection Details Window

Content

The **Gateway Connection Details** window contains these elements:

- Details of the Alliance Gateway connection selected
See "Details" on page 78
- Functions that enable you to manage the Alliance Gateway connection
See "Functions" on page 81

Display

Gateway Connection Details

Name: beax017

Host Name: 172.24.95.183

Port Number: 48002

Remote File Transfer Port Number: 48003

SSL: Data Encryption

FIN Message Partner: fin_

SNI Message Partner: sni_

Alliance Remote Gateway: No

Connection Status: Reliable

Local Authentication:

Left Part Key:

Right Part Key:

Show Clear Text:

LAU Key Automatic Renewal:

Cancel Save

Details

Field	Description
Name	The name of the Alliance Gateway connection
Host Name	The IP address or host name of the Alliance Gateway instance. The maximum length of the host name is 255 characters.
Port Number	The port number of the Alliance Gateway instance. The default value is 48002.
Remote File Transfer Port Number	The port number used to connect to the File Transfer component of the Alliance Gateway instance. The default value is 48003.
SSL	<p>The type of security required for the communication between Alliance Access and Alliance Gateway (SSL is used to secure transactions using PKI)</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • No additional security: no additional security to be used • Data Encryption: provides two-way encryption of data sent between Alliance Access and Alliance Gateway • Data Encryption/Host Authentication: provides two-way encryption of data sent between Alliance Access and Alliance Gateway. In addition, Alliance Access checks the SSL certificate of the Alliance Gateway to verify that it communicates with the Alliance Gateway that it expects. <p>If you select Data Encryption/Host Authentication, then the DN and CA Certificate fields are displayed.</p>
DN	The DN of the SSL certificate used by the Alliance Gateway Transport Agent

Field	Description
CA Certificate	<p>Enter the name of the file (without path) containing the CA certificate. A different CA certificate can be used for the authentication of each Alliance Gateway connection. The CA certificate must be available locally to Alliance Access:</p> <ul style="list-style-type: none"> Windows: %alliance%\data UNIX: \$ALLIANCE/data <p>This certificate is used when establishing the low-level connection between Alliance Access and Alliance Gateway.</p> <p>If the CA certificate is not self-signed but has been signed by another authority, then a single file should be generated containing the CA certificate and the one used for signing. This is the file that will now be used as the CA certificate for Gateway that needs to be accessible to the Alliance Access server.</p>
FIN Message Partner	<p>For all SWIFTNet connections (whether Alliance Remote Gateway connections or not), you can optionally enter a name to be used for the FIN Message Partner.</p> <p>Following are the naming rules:</p> <ul style="list-style-type: none"> Only alphanumeric characters are allowed. All alphabetic characters must be in lower case. The maximum length is 10 characters. <p>If left blank, the Alliance Access server builds this name based on the Alliance Access instance name as follows: fin_<FIN Message Partner>.</p>
SNI Message Partner	<p>For all SWIFTNet connections (whether Alliance Remote Gateway connections or not), you can optionally enter a name to be used for the SNI Message Partner.</p> <p>Following are the naming rules:</p> <ul style="list-style-type: none"> Only alphanumeric characters are allowed. All alphabetic characters must be in lower case. The maximum length is 10 characters. <p>If left blank, the Alliance Access server builds this name based on the Alliance Access instance name as follows: sni_<SNI Message Partner>.</p>
Alliance Remote Gateway	<p>If an Alliance Remote Gateway connection has been set up by the Alliance Access software owner using the <code>saa_configarg</code> tool, this read-only field is set to <code>Yes</code>. Otherwise, it is set to <code>No</code>.</p> <p>For an Alliance Remote Gateway connection, only the Local Authentication fields can be edited. All others are read-only.</p> <p>Operators cannot add or delete Alliance Remote Gateway connections.</p>
Connection Status	<p>Indicates whether the connection between Alliance Access and the SWIFTNet Link host is <code>Reliable</code> or <code>Not Reliable</code>. The Alliance Gateway connection status can only be modified when the SIS and SNIS components are stopped.</p> <p>If the status is <code>Not Reliable</code> (because the local authentication failed), the message transfer over the Alliance Gateway connection is stopped immediately until the status becomes reliable again. An event is logged in the Event Log with detailed information on the failure.</p> <p>Alliance Gateway connections that do not use local authentication keys are always <code>Reliable</code>.</p>
Use Specific Authoriser DN	<p>If this field is selected, you can specify a specific authoriser DN in the Authoriser DN field.</p>

Field	Description
	<p>When you are assigning an Alliance Gateway connection to a real-time reception profile for which the Service and Responder DN fields are populated, this field is available.</p> <p>For more information on the Service and Responder DN fields, see "Reception Profile Details Window: Configuration Tab" on page 402.</p>
Authoriser DN	<p>With this field, you can specify the specific authoriser DN that the connection uses to sign messages. If Authoriser DN is specified, then Alliance Gateway uses the certificate of that DN to sign messages and delivery notifications.</p> <p>When you are assigning an Alliance Gateway connection to a real-time reception profile for which the Service and Responder DN fields are populated, this free-text field is available. You can enter only levels 3 and above of the authoriser DN</p> <p>For more information on the Service and Responder DN fields, see "Reception Profile Details Window: Configuration Tab" on page 402.</p>
Local Authentication	<p>Local authentication secures the link between Alliance Access and the SWIFTNet Link host, where the PKI signatures for FIN message authentication are calculated (on an HSM).</p> <p>If you select the Local Authentication check box, then the Left Part Key and Right Part Key fields and the Show Clear Text check box are displayed.</p>
Left Part Key / Right Part Key	<p>The first / second 16 characters of the key to authenticate the link between Alliance Access and the SWIFTNet Link host. The two parts together form a 32-character hexadecimal string.</p> <p>The key must be the same as the one that is entered in Alliance Gateway and must be renewed at regular intervals.</p>
Show Clear Text	<p>Determines whether the system displays the authentication keys. By default, the system does not display the authentication keys. This is to help prevent unauthorised users reading the authentication key information "from over your shoulder".</p>
LAU Key Automatic Renewal	<p>For FIN and SNI message partners only, indicates whether LAU key automatic renewal is active on the SWIFTNet connection.</p> <p>For Alliance Remote Gateway connections, the field is read-only. For other SWIFTNet connections, the field can be selected, but is initially unselected. If selected, LAU keys that are within 90 days of their expiry date are automatically renewed.</p> <p>This feature is only available with Alliance Gateway 7.0.25 or higher.</p> <p>LAU key automatic renewal is not performed on non-reliable SAG connections.</p>

5.6.4 Gateway Connectivity Functions

Overview

These functions enable you to manage the Alliance Gateway connections.

Functions

Function	Description	Gateway Connectivity page	Gateway Connection Details window
Add / Add As	Enables you to add an Alliance Gateway connection You can also add an Alliance Gateway connection using the characteristics of an existing connection with the Add As button. Procedure: "Add an Alliance Gateway Connection" on page 81	✓	x
Delete	Deletes an Alliance Gateway connection Procedure: "Delete an Alliance Gateway Connection" on page 83	✓	x
Mark As Reliable	Enables you to mark a connection as reliable Procedure: "Mark an Alliance Gateway Connection as Reliable" on page 83	✓	✓

5.6.5 Add an Alliance Gateway Connection

Purpose

This procedure enables you to add Alliance Gateway connections.

Users and permissions

To display the list or the details of Alliance Gateway connections, your operator profile must have these actions:

- **SWIFTNet Support** (to display the list)
- **SWIFTNet Support / SNL Handling** (to display the details)

The **Connection Handling** permission must be set to **Yes**.

If the connections use local authentication, the following permissions must be set to **Yes**:

- **First Part Local Authentication Key** (to view the first part of the local authentication key)
- **Second Part Local Authentication Key** (to view the second part of the local authentication key)

Left security officers can only see the first part of the key; right security officers can only see the second part.

To add Alliance Gateway connections, your operator profile must have this action:

- **SWIFTNet Support / SNL Handling**

The **Connection Handling** permission must be set to **Yes**.

Security officers can add Alliance Gateway connections.

Prerequisites

You cannot add Alliance Gateway connections if the SWIFT Interface Services (SIS) and the SWIFTNet Interface Services (SNIS) components are running.

Procedure

1. From the list of Alliance Gateway connections, click **Add**.

You can also add a connection using the characteristics of an existing connection. Select the check box of a connection and click **Add As**.

The **Gateway Connection Details** window opens.

2. In the **Name** field, type the name of the Alliance Gateway connection.
3. In the **Host Name** field, type the IP address or the host name of the Alliance Gateway instance.
4. In the **Port Number** field, type the port number of the Alliance Gateway instance. The default value is 48002.
5. In the **Remote File Transfer Port Number** field, type the port number used to connect to the File Transfer component of the Alliance Gateway instance. The default value is 48003.
6. In the **SSL** drop-down list, select one of the following values:
 - No additional security
 - Data Encryption
 - Data Encryption/Host Authentication
7. If you selected Data Encryption/Host Authentication in the **SSL** drop-down list, then indicate the following:
 - In the **DN** field: the DN of the SSL certificate used by the Alliance Gateway Transport Agent
 - In the **CA Certificate** field: the name of the file (without path) containing the CA certificate.
8. If you are using local authentication, select the **Local Authentication** check box.

Depending on your rights, either the **Left Part Key** or **Right Part Key** field is displayed.

Note

If you select the **Show Clear Text** check box, then the first part or the second part of the key appears in clear.

9. Enter either the left part or the right part of the secret. Each part consists of 16 characters.
10. Click **Save**.
A status popup message appears.
11. Click **Close**.

The **Gateway Connection Details** window closes.

The connection is added to the list.

5.6.6 Mark an Alliance Gateway Connection as Reliable

Purpose

All processes that transfer FIN messages regularly verify the Alliance Gateway connection status. If the status is Not Reliable (the local authentication failed), the message transfer over the Alliance Gateway connection is stopped immediately until the status becomes reliable again.

This procedure enables you to mark an Alliance Gateway connection as reliable.

Users and permissions

To mark Alliance Gateway connections as reliable, your operator profile must have this action:

- **SWIFTNet Support / SNL Handling**

The **Reset Connection Status** permission must be set to Yes.

Security officers can mark Alliance Gateway connections as reliable.

Prerequisites

The Alliance Gateway connection status can only be modified when the SIS and SNIS components are stopped.

Alliance Gateway connections that do not use local authentication keys are always Reliable.

Procedure

1. From the list of Alliance Gateway connections, select the check box for the Alliance Gateway connections that you want to mark as reliable in the left column.
2. Click **Mark As Reliable**.

A status popup message appears.

5.6.7 Delete an Alliance Gateway Connection

Purpose

This procedure enables you to delete Alliance Gateway connections.

Users and permissions

To delete Alliance Gateway connections, your operator profile must have this action:

- **SWIFTNet Support / SNL Handling**

The **Connection Handling** permission must be set to Yes.

Security officers can delete Alliance Gateway connections.

Prerequisites

You cannot delete Alliance Gateway connections if the SWIFT Interface Services (SIS) and the SWIFTNet Interface Services (SNIS) components are running.

Procedure

1. From the list of Alliance Gateway connections, select the check boxes for the Alliance Gateway connections that you want to delete in the left column.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

5.7 Database Backups

5.7.1 Database Backups

Overview

Database backups can either be launched manually or scheduled on a regular basis. Backups can be done in both housekeeping and operational mode.

Note A database backup cannot be restored from the GUI. For more information about restoring the database, see the *Administration Guide* for [AIX](#), [Linux](#), [Oracle Solaris](#), or [Windows](#).

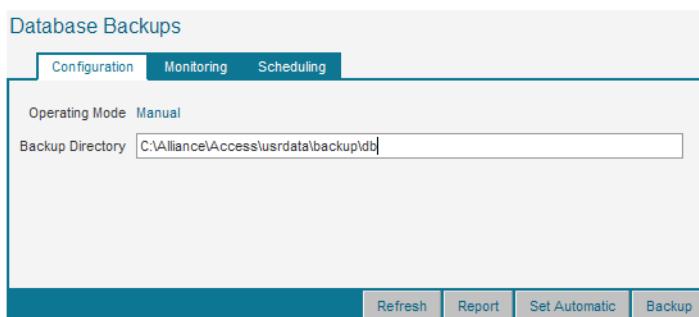
5.7.2 Database Backups Page: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details of the database backup configuration
See "Details" on page 84
- Functions that enable you to manage the database backups
See "Functions" on page 86

Display



Details

Field	Description
Operating Mode	<p>These are the possible values:</p> <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations

Field	Description
Backup Directory	<p>The location where Alliance Access stores database backup files. The default location is: <software dir>\usrdata\backup\db where <software dir> is the directory in which Alliance Access is installed.</p> <p>Note: On Windows only: If you have a hosted database configuration, you can access remote file directories by specifying UNC paths. Do not use a mapped drive</p>

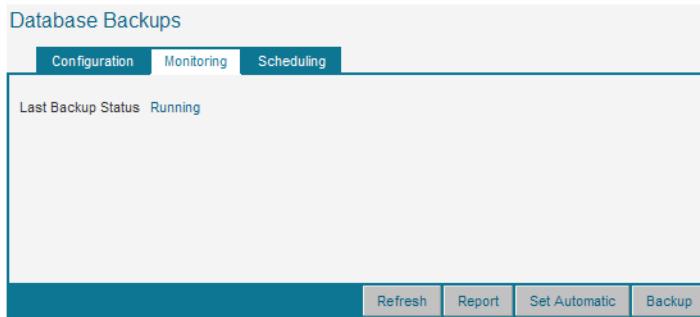
5.7.3 Database Backups Page: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details of the last database backup
See "Details" on page 85
- Functions that enable you to manage the database backups
See "Functions" on page 86

Display



Details

Column	Description
Last Backup Status	The status of the last database backup and date and time when it was carried out

5.7.4 Database Backups Page: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Tabs with Scheduled Actions Lists" on page 28.

5.7.5 Database Backup Functions

Overview

These functions enable you to manage the database backups.

Functions

Function	Description
<input type="button" value="Set Automatic"/> / <input type="button" value="Set Manual"/>	Enables you to set the operation mode to <code>Automatic</code> or to <code>Manual</code> Procedure: "Change the Operation Mode" on page 87
<input type="button" value="Backup"/>	Enables you to launch a database backup manually Procedure: "Configure and Launch a Manual Database Backup" on page 87

5.7.6 Change the Default Directory for Database Backups

Purpose

This procedure enables you to change the location where Alliance Access stores database backup files.

The default location is: `<software dir>\usrdata\backup\db` where `<software dir>` is the directory in which Alliance Access is installed.

When doing a manual backup, you can provide a different location in the **Backup Database** window. This location will not be recorded permanently.

If you are using a hosted database, the directory cannot be changed manually. The path is deduced from the value of a system parameter. After installation, the parameter is not initialised. You have to change its value before being able to perform a backup.

Names of database backup directories

Alliance Access creates a directory for every database backup.

The following naming convention is used: `YYYYMMDDTHHMMSS_SAA_DATA_BACKUP`

Where:

- `YYYYMMDDTHHMMSS` represents the local time on the server when the backup was created.

Example of directory names: `20100426T120000_SAA_DATA_BACKUP`

Users and permissions

To display the configuration details and the status of the last database backup, or change the default directory, your operator profile must have this action:

- **System Management / Backup**

Procedure

1. From the **Configuration** tab, modify the path in the **Backup Directory** field.
2. Click .

A status popup message appears.

5.7.7 Configure and Launch a Manual Database Backup

Purpose

This procedure enables you to back up the Alliance Access database manually.

You can also create backups using command line tools.

Users and permissions

To display the configuration details and the status of the last database backup, or launch manual backups, your operator profile must have this action:

- **System Management / Backup**

Procedure

1. From the **Configuration** tab, click **Backup**.

The **Backup Database** window opens.

2. In the **Backup Directory** field, change the location where Alliance Access stores the database backup files if needed.

If you change the location from the **Backup Database** window, then the new location is only used for the current backup. It is not recorded permanently.

3. Select the **Overwrite oldest Backup** check box if you want the oldest backup contained in the backup directory to be overwritten.

4. Click **Backup**.

The **Backup Database** window closes.

A status popup message appears.

The status popup message informs you about the status of the backup request. If the request is accepted, the backup is launched as a background task. You have to monitor the status of the backup from the **Monitoring** tab.

5.7.8 Change the Operation Mode

Purpose

This procedure enables you to change the operation mode.

Users and permissions

To display the configuration details and the status of the last database backup, or change the operation mode, your operator profile must have this action:

- **System Management / Backup**

The **Modify operating mode** permission must be set to **Yes**.

Prerequisites

You cannot change the operation mode if no default calendar has been defined.

Procedure

- From the **Configuration** tab, the **Monitoring** tab, or the **Scheduling** tab, given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.
A status popup message appears.

5.7.9 Monitor a Database Backup

Purpose

This procedure enables you to monitor the status of the last database backup process.

Users and permissions

To display the configuration details and the status of the last database backup, your operator profile must have this action:

- System Management / Backup**

Security officers can monitor backups.

Procedure

- Click the **Monitoring** tab.
- You can click **Refresh** to refresh the list.

5.8 Recovery Backups

5.8.1 Recovery Backups

Overview

The relational database of Alliance Access can be configured to enhance protection against media failures such as a disk crash or data file loss.

Alliance Access provides functionality that allows to recover the database content to its last committed state before an incident leading to a media failure occurred. This functionality is subject to the 14:DATABASE RECOVERY licence option.

Once activated, the database recovery feature maintains ready-to-use backups of database updates on separate disks. In case of a media failure resulting in the loss of the database content, database recovery provides a simple command to restore the database content from these backups, resulting in no data loss.

The main database recovery functions are:

- configure the database for enhanced resilience, by defining additional mirror and backup disks
- automatically schedule recovery backups. These backups can also be generated upon request, typically to be included in an external scheduler maintained by the customer.

A recovery backup of the database contains all the data present in the database.

5.8.2 Recovery Backups Page: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details of the recovery backup configuration

See "Details" on page 89
- Functions that enable you to manage the recovery backups

See "Functions" on page 92

Display



Details

Field	Description
Recovery Mode	Indicates whether the recovery mode is Activated or Deactivated .
Recovery Backup Directory	The location where Alliance Access stores recovery backup files. The path is only shown when DB Recovery is Activated.
Include Archive Backups	<p>Include the following archives (of messages and events) in the recovery backup:</p> <ul style="list-style-type: none"> • Archives that have been backed up already • Archives that have been restored <p>By default, these archives are excluded from the recovery backups, which reduces the time that Alliance Access needs to create the recovery backup.</p>
Compress Recovery Backups	Indicates that the recovery backups are compressed, which reduces the disk space required for their storage.

5.8.3 Recovery Backups Page: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details of the last full or incremental recovery backup

See "Details" on page 90

- Functions that enable you to manage the recovery backups

See "Functions" on page 92

Display



Details

Field	Description
Full Recovery Backup	<p>The status of the last full recovery backup and date and time of the backup</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Running • Completed • Failed
Incremental Recovery Backup	<p>The status of the last incremental recovery backup and date and time of the backup</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Running • Completed • Failed
Recovery Backup DiskSpace	The free amount of disk space available in MB on the recovery backup disk

5.8.4 Recovery Backups Page: Scheduling Tab

Content

The **Scheduling** tab contains these elements:

- Details of the available scheduled actions

You can specify the type of event which triggers a recovery backup in the **Recovery Backup Trigger** drop-down list:

- **Thresholds:** A recovery backup is created when the total size of the archived redo log files or the incremental backups reach the values that you specify.

See "Details" on page 91

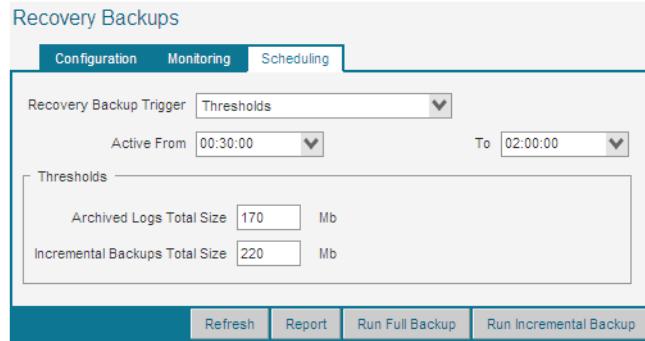
- **Time Schedule:** A recovery backup is created at the time defined with scheduled actions.

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Scheduled Action Details Window" on page 29.
- Functions that enable you to manage the recovery backups

See "Functions" on page 92

Display



Details

If in the **Recovery Backup Trigger** drop-down list **Thresholds** is selected:

Field	Description
Active From / To	Specify the period of the day (hour, minute, and second) during which recovery backups may be triggered. The default values are 02:00:00 and 06:00:00.
Archived Logs Total Size	Specify a threshold (in MB) for the total size of the archived redo log files. If the size of the archived redo logs is greater than this value, then the total size of the incremental backups is compared with the size of the latest full database backup. The default value is 1024. The value must be included in the range [64, 999999]. If the total size of the incremental backups is greater, then a full backup is taken. If not, the total size of the incremental backups is compared with the threshold.
Incremental Backups Total Size	Specify a threshold (in MB) for the total size of the existing incremental backups. If the size of the existing incremental backups is less than this value, then an incremental backup is taken. If it is greater, then a full backup is taken. The default value is 2048. The value must be included in the range [64, 999999]. As such, this threshold value must not be considered as the maximum size of the total of incremental backups: this total size can be greater than this threshold value.

5.8.5 Recovery Backup Functions

Overview

These functions enable you to manage the recovery backups.

Functions

Function	Description
Run Full Backup	Enables you to launch a full backup Procedure: "Configure and Launch a Manual Recovery Backup" on page 92
Run Incremental Backup	Enables you to launch an incremental backup Procedure: "Configure and Launch a Manual Recovery Backup" on page 92

5.8.6 Configure and Launch a Manual Recovery Backup

Purpose

This procedure enables you to create a recovery backup manually.

You can perform manual recovery backups from the Alliance Access Configuration or using the **saa_dbrecovery** tool.

There are two types of database recovery backups: full backup and incremental backup:

Backup type	Contents and results
Full	<p>The backup on the recovery-backup disk contains all data files including archive that have not been backed up or restored.</p> <p>To include archives that have been backed up or restored, select the Include Archive Backups option.</p> <p>Alliance Access deletes the existing backups of the type:</p> <ul style="list-style-type: none"> incremental backups and the archived redo logs full recovery backup⁽¹⁾
Incremental	<p>The backup on the recovery-backup disk contains all data files for which changes have occurred since the last backup was created (any backup type).</p> <p>To include archives that have been backed up or restored, select the Include Archive Backups option.</p> <p>The existing archived redo logs are deleted.</p>

(1) You can remove the existing full recovery backup before taking a new one, by using the option `-e` with the `saa_dbrecovery` command. You can also use this option to create disk space if there is insufficient disk space to launch a new full recovery backup.

Users and permissions

To display the configuration details and the status of the last recovery backups, or launch a backup, your operator profile must have this action:

- System Management / Manage Rec Backup**

Security officers can also launch recovery backups.

Prerequisites

The database recovery feature is only available if the licence package 14:DATABASE RECOVERY is installed.

You must use the **saa_dbrecovery** tool to activate the recovery mode.

When you perform a recovery backup, Alliance Access first verifies that the estimated size of the recovery backup is less than the available disk space on the recovery backup disk.

Procedure

1. From **System**, select the **Recovery Backups**.

2. Verify that **Recovery Mode** is Activated.

If the Recovery Mode is deactivated, then use **saa_dbrecovery** tool to activate the recovery mode. For more information, see **saa_dbrecovery** in the *Administration Guide for AIX, Linux, Oracle Solaris, or Windows*.

3. In the **Configuration** tab, select the configuration parameters required. For more information, see "Recovery Backups Page: Configuration Tab" on page 89.

4. Click **Save**.

5. Click **Run Full Backup** or **Run Incremental Backup**.

If you clicked **Run Full Backup**, a confirmation window opens about the removal of existing full backups.

Click **OK**.

Note

Alliance Access verifies that the estimated size of the recovery backup is less than the available disk space on the recovery backup disk. If insufficient space is available, then the backup operation will fail. This will not affect normal Alliance Access operations.

You can monitor the status of the recovery backup from the **Monitoring** tab.

5.8.7 Schedule a Recovery Backup

Purpose

This procedure enables you to schedule a recovery backup.

Users and permissions

To display the configuration details and the status of the last recovery backups, or schedule a backup, your operator profile must have this action:

- **System Management / Manage Rec Backup**

Security officers can schedule backups.

Prerequisites

The database recovery feature is only available if the licence package 14:DATABASE RECOVERY is installed.

You must use the **saa_dbrecovery** tool to activate the recovery mode.

If **Time Schedule** is selected in the **Recovery Backup Trigger** drop-down list, then a calendar for the current year must have been defined.

When you perform a recovery backup, Alliance Access first verifies that the estimated size of the recovery backup is less than the available disk space on the recovery backup disk.

Procedure

1. From the **Scheduling** tab, select one of the following values:

- **Thresholds**
- **Time Schedule**

- 2.

If	Then
You selected Thresholds	Define the following: <ul style="list-style-type: none">• Active From / To• Archived Logs Total Size• Incremental Backups Total Size
You selected Time Schedule	See "Add a Scheduled Action" on page 33

3. Click **Save**.

A status popup message appears.

If a backup process is running at the time the backup is scheduled, then the scheduled backup is not performed and an event is logged in the event log. Also, a scheduled backup does not take into account archives that are either under construction (that is, the archive process is running), or being consulted.

5.8.8 Monitor a Recovery Backup

Purpose

This procedure enables you to monitor the status of recovery backups.

Users and permissions

To display the configuration details and the status of the last recovery backups, your operator profile must have this action:

- **System Management / Manage Rec Backup**

Security officers can monitor backups.

Procedure

1. Click the **Monitoring** tab.
2. You can click **Refresh** to refresh the fields.

5.9 User Space

5.9.1 User Space

Purpose

The User Space is a file management system which enables you to upload or download files for further processing by Alliance Access.

Files are located on the Alliance Access server. The root path of the User Space is defined by the **Root Path for User Space** security parameter. Each operator has a User Space and cannot access folders or files which are located in the User Space of other operators.

In the User Space, the files are identified by User Space names which are not necessarily the same as the physical names of the files.

Users and permissions

In order to manage folders and upload or download files on the user space, the File on User Space (**Access Control** application) permission is required.

5.9.2 User Space Page

Content

The **User Space** page contains these elements:

- Details of the available folders or uploaded files
See "Details" on page 95
- Functions that enable you to manage the folders and files
See "Functions" on page 96

Display

User Space				
Current Folder ~ /				
Rows in list: 1 , in selection: 0				
Change View	Refresh	Go to Parent Folder	Add Folder	Upload
Rows in list: 1 , in selection: 0	Download	Rename	Delete	
<input type="checkbox"/>	Name	Type	Size in Bytes	Last Modification Time
<input type="checkbox"/>	Folder	Folder	0	2010/11/09 12:15:40

Details

Column	Description
Name	The User Space name of the file
Type	<p>The element type</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Folder • File

Column	Description
Size in Bytes	The size of the file
Last Modification Time	The date and time when the folder or the file was last updated

Functions

Function	Description
Go to Parent Folder	Navigates to the parent folder of the current folder
Add Folder	Enables you to add folders at the current folder level Procedure: "Add a Folder to the User Space" on page 96
Upload	Enables you to upload files to the User Space Procedure: "Upload a File to the User Space" on page 96
Download	Enables you to download files from the User Space Procedure: "Download a File from the User Space" on page 97
Rename	Enables you to rename a folder or a file Procedure: "Rename a User Space Folder or File" on page 97
Delete	Enables you to delete a folder or a file Procedure: "Delete a User Space Folder or File" on page 98

5.9.3 Add a Folder to the User Space

Purpose

This procedure enables you to create a folder at the current folder level within the User Space.

Procedure

1. From the **User Space** page, click **Add Folder**.
The **Add Folder to User Space** window opens.
2. Type a name in the **Folder Name** field.
3. Click **Add Folder**.
The **Add Folder to User Space** window closes.

A folder with the name that you specified appears in the list for the current User Space folder.

5.9.4 Upload a File to the User Space

Purpose

This procedure enables you to copy a file located on your desktop to the User Space. You must define a User Space name which will be used to identify the file in the User Space.

Procedure

1. From the **User Space** page, click a folder.
2. Click **Upload**.

- The **Upload** window opens.
3. Click **Browse**.
- The **Choose file** window opens.
4. Browse to the location of the file, select it and click **Open**.
- The **Choose file** window closes.
5. In the **User Space File Name** field, type a name for the file.
This name is used for the file in the User Space. The physical name does not change.
6. Click **Upload**.
- The **Upload** window closes.
- The file appears in the list.
- If a file with the same User Space name exists in the folder, then the **File Overwrite Confirmation** window opens.

5.9.5 Download a File from the User Space

Purpose

This procedure enables you to get a copy of a file located in the User Space and save it to a local drive.

Procedure

1. From the **User Space** page, navigate to the file that you want to download.
2. Click **Download**.
The **File Download** window opens.
3. Click **Save**.
The **File Download** window closes.
The **Save As** window opens.
4. Browse to a location for the file and click **Save**.
The **Save As** window closes.
The **Download complete** window opens.
5. Click **Close**.
The **Download complete** window closes.

The file is downloaded.

5.9.6 Rename a User Space Folder or File

Purpose

This procedure enables you to change the User Space name of a folder or a file. For files, the physical names remain unchanged.

Procedure

1. From the **User Space** page, select the check box of the element that you want to rename.
2. Click **Rename**.

The **Rename Item From User Space** window opens.

3. Type a name in the **New Name** field.
4. Click **Rename**.

The **Rename Item From User Space** window closes.

The element is renamed.

5.9.7 Delete a User Space Folder or File

Purpose

This procedure enables you to delete folders or files from the User Space.

Prerequisites

You cannot delete folders which contain files. You must delete all the files contained in the folder that you want to delete.

Procedure

1. From the **User Space** page, select the check boxes for one or several elements in the left column.
2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

The **Delete Confirmation** window closes.

The element or elements selected are deleted.

5.10 Printers

5.10.1 Printers

Overview

You can print messages from Alliance Access to a file or to a printer.

If you need to print messages, then one or several printers must be defined:

- On Windows, you must configure printers using the standard Windows printer management tool. Alliance Access reuses the settings defined at the operating system level.
- On UNIX or Linux, you can configure printers with Alliance Access Configuration.

Note To print reports generated from the GUI, you can directly use the printers defined on your computer.

5.10.2 Printers Page

Content

The **Printers** page contains these elements:

- Details of the available printers
See "Details" on page 99
- Functions that enable you to manage the printers (UNIX or Linux only)
See "Functions" on page 99

Display

Printers		Rows in list: 5 , in selection: 1
Printers		◀ Previous Next ▶
Name		
<input type="checkbox"/>	Microsoft XPS Document Writer (redirec...	
<input checked="" type="checkbox"/>	Microsoft XPS Document Writer	
<input type="checkbox"/>	Lexmark T640 (MS) (Copy 1)	
<input type="checkbox"/>	Lexmark T640 (MS)	
<input type="checkbox"/>	Epson AL-C1100	

Details

Column	Description
Name	The name of the printer

Functions

Function	Description
<input type="button" value="Add"/> (UNIX or Linux only)	Enables you to add a printer Procedure: "Add a Printer (UNIX or Linux Only)" on page 100
<input type="button" value="Delete"/> (UNIX or Linux only)	Enables you to delete a printer Procedure: "Delete a Printer (UNIX or Linux Only)" on page 101

5.10.3 Printer Details Window

Content

The **Printer Details** window contains these elements:

- Details of the available printers

See "Details" on page 100

Display

The screenshot shows a 'Printer Details' dialog box with the following fields:

- Name:** behw0650
- Description:** (empty)
- Bold Emulation:** Character Overstrike
- Lines / Page:** 60
- Columns:** 80

Details

Field	Description
Name	The name of the printer
Description	The description of the printer
Bold Emulation	<p>Specifies how bold characters are printed</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Character Overstrike • Line Overstrike • Disable Bold • HP PCL Compatible • DEC LN03 Compatible • IBM/EPSON Matrix
Lines / Page	The number of lines per page
Columns	The number of characters per line

5.10.4 Add a Printer (UNIX or Linux Only)

Purpose

This procedure enables you to add a printer.

Users and permissions

To display the list or the details of printers, your operator profile must have this entity:

- **System Management**

To add or modify a printer, your operator profile must have these actions:

- **System Management / Add Device**
- **System Management / Mod Device**

Security officers can add printers.

Procedure

1. From the list of printers, click **Add**.
The **Printer Details** window opens.
 2. In the **Name** field, type the name of the printer.
Once created, you cannot change the name.
 3. In the **Description** field, type a description.
 4. In the **Bold Emulation** drop-down list, select one of the following values:
 - Character Overstrike
 - Line Overstrike
 - Disable Bold
 - HP PCL Compatible
 - DEC LN03 Compatible
 - IBM/EPSON Matrix
 5. Indicate the number of lines per page in the **Lines / Page** field.
 6. Indicate the number of characters per line in the **Columns** field.
 7. Click **Save**.
A status popup message appears.
 8. Click **Close**.
The **Printer Details** window closes.
- The printer is added to the list.
Once you have defined a printer, it must be enabled under UNIX.

5.10.5 Delete a Printer (UNIX or Linux Only)

Purpose

This procedure enables you to delete a printer.

It is not possible to delete a printer which is currently assigned to a message partner.

Users and permissions

To display the list or the details of printers, your operator profile must have this entity:

- **System Management**

To delete a printer, your operator profile must have this action:

- **System Management / Rem Device**

Security officers can delete printers.

Procedure

1. From the list of printers, select the check box of one or several printers in the left column.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

The **Delete Confirmation** window closes.

A status popup message appears.

5.11 Calendars

5.11.1 Calendars and Scheduled Operations

Introduction

Operators can use calendars to schedule automatic operations (for example stopping and restarting the Alliance Access servers, backups, connection to the SWIFT network). You can set up multiple calendars for a given year. This enables logical terminals to have their own calendar, which can be useful if the logical terminals are located in different countries, with different working days or public holidays.

Operators must set up a calendar for the current year before being able to schedule processes to occur automatically.

Alliance Access users can only schedule processes if the operator profiles allow them to do so. After you create your calendar, you must modify the appropriate profiles. Once you have created a calendar and modified the profiles, any users with the appropriate profiles can schedule processes.

At the start of each day (midnight), Alliance Access checks the calendar and determines which day types apply to the current day. For example, today may be the "First working day of week" and the "First working day of month". Alliance Access then checks to see whether any operations are scheduled for these day types. If an operation is scheduled, then Alliance Access carries it out at the specified time, unless the server is running in housekeeping mode.

Some actions can be scheduled to start at a specific time. Other actions can be scheduled to start between an earliest time and a latest time.

The schedule is also rebuilt after each restart of the server. If the restart occurs between the earliest and latest start times of a scheduled action, then that action is started automatically.

During the startup of the Alliance Access servers, each calendar is checked to see whether the current year has been defined. For each calendar for which no current year is defined, an alarm event is generated.

5.11.2 How Alliance Access Defines System Attributes for Days

Overview

Depending on the profiles that you have defined for the days in a calendar, such as holidays and weekends, Alliance Access automatically assigns the following system attributes to the days:

- **First working day of month.** This is assigned to the first day of the month that is not a Holiday or a Weekend.
- **Middle working day of month.** This is assigned to the 16th of the month, or the next day that is not a Holiday or a Weekend.

If you assign the profile Weekend to a day, Alliance Access automatically calculates the following system attributes:

- **First working day of week.** This is assigned to the first day following a Weekend which is not a Holiday or a Weekend.
- **Last working day of week.** This is assigned to the first day before a Weekend that is not a Holiday or a Weekend.

At the end of the year, a week can fall partly in one year and partly in the following year. In this case, the **First working day of week** refers to the first day *in the current year* following a Weekend which is not a Holiday or a Weekend.

Similarly the **Last working day of week** refers to the last day *in the current year* before a Weekend that is not a Holiday or a Weekend.

The following examples explain the scenario.

Definitions:

- WD = Working day
- FWDW = First working day of week
- LWDW = Last working day of week

The last WD of December will be a LWDW and the first WD of January will be a FWDW. There are some configurations where a LWDW and FWDW fall on the same day. For example, if 31 December is a Monday or 2 January (assuming 1 January is a holiday) is a Friday, then in these cases, the day will be treated as FWDW.

Example 1

If 31 December is a Wednesday and 1 January is not a holiday and Saturday, Sunday are weekends, then the days are considered as follows:

- Mon = FWDW
- Tue = Normal
- Wed = LWDW
- Thu = FWDW
- Fri = LWDW

Example 2

If 31 December is a Monday, 1 and 2 January (Tuesday and Wednesday) are holidays, then the days are considered as follows:

- Mon = FWDW
- Tue = Hol
- Wed = Hol
- Thur = FWDW
- Fri = LWDW

Example 3

If 31 December is Wednesday and 1 January (Thursday) is a holiday, then the days are considered as follows:

- Mon = FWDW
- Tue = Normal
- Wed = LWDW
- Thu = Hol
- Fri = FWDW

Note If you make any changes to a calendar, then once the changes are saved, Alliance Access re-assigns the First and Last working day of the week and the First and Middle working day of the month accordingly.

5.11.3 Calendars Page

Content

The **Calendars** page displays information about the calendars defined in your system.

The **Calendars** page contains these elements:

- Details of the available calendars
See "Details" on page 105
- Functions that enable you to manage the calendars
See "Functions" on page 105

Display

Calendars					Rows in list: 1 , in selection: 1
	Change View	Add As	Delete	Set Default	Report
	Name		Year	Default	
<input checked="" type="checkbox"/>	BE		2010		Yes

Details

Column	Description
Name	The name of the calendar
Year	The year of the calendar
Default	Indicates whether the calendar is set as default

Functions

Function	Description
<input type="button" value="Add"/> / <input type="button" value="Add As"/>	Enables you to add a calendar You can also add a calendar using the characteristics of an existing calendar with the <input type="button" value="Add As"/> button. Procedure: "Add a Calendar" on page 107
<input type="button" value="Delete"/>	Enables you to delete a calendar Procedure: "Delete a Calendar" on page 109
<input type="button" value="Set Default"/>	Enables you to set the calendar as default Procedure: "Set a Calendar as Default" on page 108

5.11.4 Calendar Details Window

Content

The **Calendar Details** window displays the details of the calendar selected.

The **Calendar Details** window contains these elements:

- Details of the calendars defined
See "Details" on page 106
- Functions that enable you to manage the calendar
See "Functions" on page 107

Display

Calendar Details

Name: BE
Year: 2010

Available Selected

Weekend Definition: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Displayed Month: January

Month Details

Set Normal | Set Peak | Set Holiday

Rows in list: 31 , in selection: 1

<input type="checkbox"/>	Date	Day	Profile	Information
<input type="checkbox"/>	01	Fri	Normal	First working day of month/First working day of week
<input checked="" type="checkbox"/>	02	Sat	Normal	First working day of week
<input type="checkbox"/>	03	Sun	Normal	First working day of week
<input type="checkbox"/>	04	Mon	Normal	First working day of week
<input type="checkbox"/>	05	Tue	Normal	First working day of week
<input type="checkbox"/>	06	Wed	Normal	First working day of week
<input type="checkbox"/>	07	Thu	Normal	First working day of week
<input type="checkbox"/>	08	Fri	Normal	First working day of week
<input type="checkbox"/>	09	Sat	Normal	First working day of week

Close **Report** **Previous** **Next**

Details

Field	Description
Name	The name of the calendar
Year	The year of the calendar
Weekend Definition	The Weekend Definition list enables you to define a day as a weekend or as a normal working day. The days selected are considered as weekends. The changes apply throughout the year. For example, you can redefine every Friday as a weekend, or every Saturday as a normal working day.
Displayed Month	The month for which you can define peak days, holidays, or normal days

Field	Description
Month Details	<ul style="list-style-type: none"> • Date • Day • Profile: <ul style="list-style-type: none"> – Normal – Peak – Holiday • Information: <ul style="list-style-type: none"> – First working day of month – Middle working day of month – First working day of week – Last working day of week

Functions

Function	Description
Set Normal	<p>Enables you to set the day as a normal day Procedure: "Add a Calendar" on page 107</p> <p>Days defined as weekend days are considered to be holidays. For example, you can set all Saturdays to be weekend days, which automatically sets them as holidays as well. If you then set one specific Saturday to a normal day, this goes against the fact that all Saturdays are weekend days (and thus considered to be holidays). The Set Normal button can be used only to set days back to normal, so this function is relevant only to the days that are manually set to be peak days or holidays.</p>
Set Peak	<p>Enables you to set the day as a peak day Procedure: "Add a Calendar" on page 107</p>
Set Holiday	<p>Enables you to set the day as a holiday Procedure: "Add a Calendar" on page 107</p>

5.11.5 Add a Calendar

Purpose

This procedure enables you to add a calendar.

Users and permissions

To display the list or the details of calendars, your operator profile must have these actions:

- **Calendar** (to display the list)
- **Calendar / Open/Print Calendar** (to display the details)

To add or modify a calendar, your operator profile must have these actions:

- **Calendar / Add Calendar** (to add a calendar)
- **Calendar / Modify Calendar Year** (to modify a calendar)
- **Calendar / Add Calendar Year** (to be able to modify the year for the calendar)

Procedure

1. From the list of calendars, click **Add**.

You can also add a calendar using the characteristics of an existing calendar. Select the check box of a calendar and click **Add As**.

The **Calendar Details** window opens.

2. In the **Name** field, type a name for the calendar.
This name must be unique.
3. The current year is indicated in the **Year** field. You can change it if needed.
4. In the **Displayed Month** drop-down list, select the month that you need to display.
5. To define a day as a weekend or as a normal working day, use the **Weekend Definition** list. The days selected are considered as weekends. The changes apply throughout the year. For example, you can redefine every Friday as a weekend, or every Saturday as a normal working day.
6. To define a day as a peak day or as a holiday, select the check boxes for one or several days in the **Month Details** list and click **Set Peak** or **Set Holiday**.
Click **Set Normal** to set the day or days selected back to normal.
The changes apply only within the month currently displayed.
7. Click **Save**.
An information message opens.
8. Click **OK**.
9. Click **Close**.

The **Calendar Details** window closes.

Important If you modify a calendar to include changes that affect the current day, then restart Alliance Access for your changes to take effect. Otherwise, changes take effect automatically at midnight.

5.11.6 Set a Calendar as Default

Purpose

This procedure enables you to set a calendar as default.

If you have only one calendar defined, then it is automatically set as the default one. If you have more than one however, then you can select which one is to be used as the default. It is only possible to have one default calendar.

Users and permissions

To display the list or the details of calendars, your operator profile must have these actions:

- **Calendar** (to display the list)
- **Calendar / Open/Print Calendar** (to display the details)

To set a calendar as default, your operator profile must have the following additional action:

- **Calendar / Default Calendar**

Procedure

1. From the list of calendars, select the check box of a calendar in the left column.

2. Click **Set Default**.

The **Default Calendar Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

Important If you want the new default calendar to be activated immediately, then restart Alliance Access. Otherwise, the new default calendar will be activated on the next day.

5.11.7 Delete a Calendar

Purpose

This procedure enables you to delete a calendar.

Default calendars or years belonging to a default calendar cannot be deleted. If you have multiple calendars defined and you want to delete the calendar currently set as the default, then you must first change the default calendar.

Users and permissions

To display the list or the details of calendars, your operator profile must have these actions:

- **Calendar** (to display the list)
- **Calendar / Open/Print Calendar** (to display the details)

To delete a calendar, your operator profile must have the following additional actions:

- **Calendar / Remove Calendar** (to delete a calendar)
- **Calendar / Remove Calendar Year** (to be able to delete a specific year for a calendar)

Procedure

1. From the list of calendars, select the check box for one or several calendars in the left column.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

The **Delete Confirmation** window closes.

A status popup message appears.

5.12 Reporting - BIC Selection

5.12.1 Reporting - BIC Selection

Overview

Your Reporting license determines the number of BICs that you can select, either 5, 10, 20, 50, or all BICs.

After activating Reporting, you must explicitly select the BICs to be covered by reporting, from the live and T&T destinations that are licensed in the Alliance Access instance. To do so, select the desired set of BICs by moving them from the **Available** list box to the **Selected** list box.

- During the evaluation period (whether or not a Reporting licence is present), you can select any (or all) licensed live and T&T BICs.
 - Outside of the evaluation period, you can select any number of licensed T&T BICs (regardless of your Reporting band), but the number of live licensed BICs that you can select is limited by your Reporting band. For example, if you have 10 licensed live BICs and 8 licensed T&T BICs, and you have a Reporting band for 5 BICs, you can select a maximum of 5 live BICs in addition to as many T&T BICs as you wish.

Click **Save** to save your BIC selection. The new BIC selection will be effective the next time you start Alliance Access.

You can change your selection of BICs (subject to your licence) at any time, but you need to restart Alliance Access before any new BIC selection is effective.

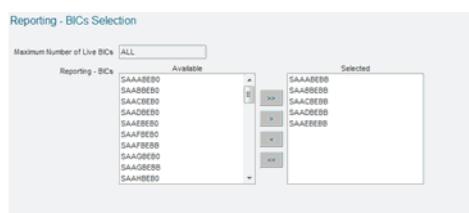
5.12.2 Reporting - BIC Selection Page

Content

The **Reporting - BIC Selection** page contains these elements:

- Details of the available BICs
See "Details" on page 111
 - Functions for managing your BICs
See "Functions" on page 111

Display



Details

Element	Description
Maximum number of live BICs	The maximum number of live BICs that will be covered by reporting. Select either 5, 10, 20, 50 or all BICs.
Reporting - BICS (Available and Selected)	You can explicitly select the BICS to be covered by reporting by moving BICs (using the arrow buttons) from the Available to the Selected list box.

Functions

Function	Description
Save	Saves your BIC selection
Cancel	Cancels any changes you have made since saving
Report	Creates a report whose output contains the BICs you have selected

5.13 Parameters

5.13.1 Classes of Configuration Parameters

Overview

Alliance Access contains a number of system parameters that you can configure. You can change the values of these parameters only if the permissions of your operator profile permit you to change them.

Configuration parameters are grouped by class.

Note Some parameters described in this section are only available if you have licensed the relevant option for your system.

IPLA configuration parameters

In addition to the classes listed here, configuration parameters resulting from installing components for IPLA may also appear. The bundle symbolic name appears as the value for Class. The value for Component is `IPLA`.

5.13.1.1 Activation

List of activation parameters

Parameter	Description
Start evaluation	Enter an activation code, which SWIFT has provided, to start the evaluation period for Operational Reporting. This will activate Operational Reporting, which will copy all messages to the Reporting data store. Depending on the number of messages in the database, this

	operation could take a considerable amount of time.
Activate reporting	<p>To activate Operational Reporting, set this parameter to <code>Activate</code>. This will copy all messages to the Reporting data store. Depending on the number of messages in the database, this operation could take a considerable amount of time.</p> <p>To deactivate Operational Reporting, set this parameter to <code>Deactivate</code>. This operation will remove all message data from the Reporting data store.</p>

5.13.1.2 Alarm

List of alarm parameters

Parameter	Description
Maximum	<p>The maximum number of alarms that can be displayed on Alliance Workstation simultaneously:</p> <ul style="list-style-type: none"> • Default: 3 • Minimum: 1 • Maximum: 20 <p>Changes to this parameter take effect at the next login to Alliance Workstation.</p>
Timeout	<p>The number of minutes an alarm popup remains on screen:</p> <ul style="list-style-type: none"> • Default: 15 • Minimum: 1 • Maximum: 120 <p>Changes to this parameter take effect at the next login to Alliance Workstation.</p>

Note Alliance Access on Linux does not support Alliance Workstation.

5.13.1.3 Alarm Message

List of alarm message parameters

Parameter	Description
Sender LT	<p>Specifies the logical terminal (BIC12: LT followed by XXX) that is used to send alarm messages to Internal Correspondents.</p> <p>Changes to this parameter take effect at the next Alarm Message/Frequency check.</p>
Frequency	<p>Alarm Message/Frequency check (in minutes). Default value: 5.</p> <p>Changes to this parameter take effect at the next Alarm Message/Frequency check.</p>

5.13.1.4 Backup

List of backup parameters

Parameter	Description
Archive Backup Dir Object	The Oracle database requires this parameter to create the Data Pump files containing the backups of archives. Maximum value: 30. Changes to this parameter take effect at the next backup or restore operation. This parameter is only available when the Alliance Access database is hosted.
DB Backup Dir Object	The Oracle database requires this parameter to create the Data Pump files containing the backups of the Alliance Access database. Maximum value: 30. Changes to this parameter take effect at the next backup or restore operation. This parameter is only available when the Alliance Access database is hosted.
Location Backups	This parameter defines the file directory wherein the Alliance Access backups are created. This directory must be shared between the Alliance Access host and the database host. If the parameter has no value, then no backup or restore can take place. The parameter has no value by default. Changes to this parameter take effect at the next backup or restore operation. This parameter is only available when the Alliance Access database is hosted.
Location Backups DB Host	This parameter defines the file directory remotely accessed from the database host wherein the Alliance Access backups are created. If this parameter has no value, then the value specified for the Location Backups parameter is used. The parameter has no value by default. Changes to this parameter take effect at the next backup or restore operation. This parameter is only available when the Alliance Access database is hosted.

5.13.1.5 Batch Input

List of batch input parameters

Parameter	Description
Automatic - Backup Dir	Automatic Input Backup Directory. All files in this directory that are older than the Batch Input History Period are deleted. Default: C:\Alliance\Access\usrdata\FTA\back Changes to this parameter take place at the next poll.
Automatic - Disabling	Specifies whether the status of a message partner is set automatically to Disabled if the message partner receives an invalid batch file. Possible values are Yes and No . Default: Yes Changes to this parameter take effect the next time the MXS component is started. This parameter has an effect on File Transfer message partners only.
Automatic - Error Dir	Automatic Input Error Directory. All files in this directory that are older than the Batch Input History Period are deleted. Default: C:\Alliance\Access\usrdata\FTA\error Changes to this parameter take place at the next poll.

Parameter	Description
Automatic - Polling Timer	The Session Autostarter Polling Timer in seconds. Default value: 60. Changes to this parameter take place at the next poll.
History Period	The number of days to keep history records for batch duplication check and to keep the files in the file transfer adapter backup and error directories. Default value: 10. Changes to this parameter take place at the next poll.
Log Directory	The location where report files generated for XML version 2 (MT/MX) input are stored.

5.13.1.6 Batch Output

List of batch output parameters

Parameter	Description
Include payload in LTA	Specifies whether or not the payload (full) path must be automatically added to the LTA command parameters by Alliance Access, for File messages sent over a File Transfer Message Partner. If this parameter is on and the message partner <small>Maximum number of messages per session</small> is set to 1, then Alliance Access automatically adds the payload full path as the last parameter of the LTA command (after the XML file) for File messages. If this parameter is on and the message partner <small>Maximum number of messages per session</small> is greater than 1, then Alliance Access automatically adds the path to the payload location as the last parameter of the LTA command (after the XML file).
LTA Timeout	Defines the Local Transfer Agent completion time in minutes. This is the time that Alliance allows for the Local Transfer Agent to process a batch output file. If the Local Transfer Agent has not finished its task within this time, then an event is written to the event log. Default value: 5.
LTA waiting mode	Specifies whether Alliance can wait for Local Transfer Agent completion before closing the session. Default value: off.

5.13.1.7 Database

List of database parameters

This parameter is not available when the licence package **13:HOSTED DATABASE** is present.

Parameter	Description
Location Messages	Location of the daily Messages database files. Changes to this parameter take effect when the next database file is created. Note: if the user enters an invalid path or if the server processes have no write access to the specified location, then the new database files are created in the following directory: <ul style="list-style-type: none"> • On UNIX or Linux: \$ALLIANCE/database/datafiles/MESG • On Windows: %ALLIANCE%\database\datafiles\MESG

Parameter	Description
Location Journal Events	<p>Location of the daily Journal Events database files. Changes to this parameter take effect when the next database file is created.</p> <p>Note: if the user enters an invalid path or if the server processes have no write access to the specified location, then the new database files are created in the following directory:</p> <ul style="list-style-type: none"> • On UNIX or Linux: \$ALLIANCE/database/datafiles/JRNL • On Windows: %ALLIANCE%\database\datafiles\JRNL

5.13.1.8 Alliance Developers Kit

List of Alliance Developers Kit parameters

Parameter	Description
ADK Storage	<p>This parameter defines the directory in which Alliance Developers Kit applications can store their specific information. The contents of this directory are considered during the backup and restore operations.</p> <p>The default path for this directory is as follows:</p> <ul style="list-style-type: none"> • On Windows: %ALLIANCE%\data\ADK_DIR • On UNIX or Linux: \$ALLIANCE/data/ADK_DIR
Operational Trace	<p>When this parameter has a value On, a journal entry is written for every call that is made to an Alliance Developers Kit (Toolkit) function. The journal entry describes in full the call made by the Alliance Developers Kit function. Default value: Off.</p> <p>You must restart an application in the Alliance Developers Kit, to apply the changes to this parameter.</p>

5.13.1.9 Disk Space

List of disk space parameters

Parameter	Description
Frequency	<p>The interval in seconds (in multiples of 60) at which disk space is checked.</p> <p>Default value: 300. Minimum: 120. Maximum: 3600.</p> <p>Change to this parameter take effect at the next disk-space check.</p> <p>A warning will be given if free disk space drops below a Warning parameter. Repeat warnings are given at 10 times the interval.</p>
Recovery Shutdown - MB	<p>Alliance Access shuts down when the free space of the Recovery Backup Disk becomes less than this number of megabytes. If the value is 0, then no action is taken.</p> <p>Default value: 1000. Minimum: 0. Maximum: 4190000.</p> <p>This parameter is available when 14:DATABASE RECOVERY is licensed.</p>
Recovery Warning - MB	<p>Alliance Access issues a warning when the free space of the Recovery Backup Disk becomes less than this number of megabytes. If the value is 0, then no action is taken.</p> <p>Default value: 5000. Minimum: 0. Maximum: 4190000.</p> <p>This parameter is available when 14:DATABASE RECOVERY is licensed.</p>

Parameter	Description
Shutdown - MB	<p>Sets the absolute minimum free disk space (in MB) that must be available on the file systems hosting the database. If the free disk space available for one of these file systems falls below this value, then Alliance Access shuts down.</p> <p>Default value: 1000, to which the system automatically adds (for recovery purposes) the size of the largest database file stored in the database, plus the size of the database index file. Minimum: 0. Maximum: 4190000.</p> <p>The frequency at which this parameter is checked is set using the Disk Space - Frequency parameter.</p> <p>You must restart Alliance Access, to apply the changes to this parameter.</p>
Shutdown - Release Dir	<p>Shutdown Alliance Access when the available space on the disk of the source tree is less than this value (in Kbytes). Default value: 20000.</p> <p>Changes to this parameter take effect at the next disk-space check.</p>
Warning - MB	<p>Alliance Access issues a warning when the free space of one of the monitored file systems hosting the database becomes less than this number of megabytes. The file system is set in an exception state in the resources monitoring.</p> <p>Default value: 5000. Minimum: 0. Maximum: 4190000.</p> <p>If the value is 0, then no action is taken.</p> <p>Changes to this parameter take effect at the next disk-space check.</p>
Warning - Release Dir	<p>Alliance Access issues a warning when available space on the disk of the Release Directory is less than this value.</p> <p>Default value: 50000 (Kbytes).</p> <p>Changes to this parameter take effect at the next disk-space check.</p>
UNIX or Linux only: Warning - Printer Spool	<p>Alliance Access issues a warning when available space on the /tmp disk is less than this value (in Kbytes).</p> <p>Default value: 10000. Minimum: 1024. Maximum: 200000.</p> <p>Changes to this parameter take effect at the next disk-space check.</p>

5.13.1.10 Display Format

List of display format parameters

Parameter	Description
Amount	<p>Specifies the convention used to separate decimals and units of a thousand:</p> <ul style="list-style-type: none"> • Decimal-Comma/Thousand-Nothing, which corresponds to the ISO format. This is the default value. • Decimal-Point/Thousand-comma, which corresponds to the American format. • Decimal-Comma/Thousand-Point, which corresponds to the European format.
Date	<p>The display format of the date: American date format is MM/DD/YY, European date format is DD/MM/YY, ISO date format is YY/MM/DD. Default: European.</p> <p>You must restart Alliance Workstation, to apply the changes to this parameter.</p>
Time	<p>Specifies the time format:</p> <ul style="list-style-type: none"> • Day of 24 Hours, which uses 24-hour clock notation, for example, 13:15:00. This is the default option. • Day of 12 Hours, which uses 12-hour clock notation, for example, 01:15:00 p.m.

See also "Display/Print" on page 117.

5.13.1.11 Display/Print

Display/Print parameter

Parameter	Description
FIN User Header	<p>Specifies whether to display or print the FIN User Header (block 3) of MT messages. The allowed values are:</p> <ul style="list-style-type: none"> • Yes - display block 3 in the message details in the Text tab of the Message Details area, and in the results of a message search. In addition, print block 3 in the printed reports of message details, both from the GUI and from a Print message partner. • No - do not display block 3 in the message details, and do not print it in reports that provide message details. <p>The default value is No.</p>

5.13.1.12 Emission

List of emission parameters

Parameter	Description
Corr. on hold criteria	<p>Indicates the period of time (in minutes) after which a correspondent is put on hold for a real-time service if all emission attempts for that correspondent/real-time service have failed during that period.</p> <p>If set to 0, correspondents are never put on hold for a real-time service.</p> <p>The possible values are numbers from 0 to 999. The default value is 10.</p> <p>Any changes to this parameter take effect immediately.</p>
EP Polling Timer	<p>Indicates the period (in seconds) according to which the Alliance Access polls the database for the next message to send:</p> <ul style="list-style-type: none"> • Maximum value: 300 • Minimum value: 1 • Default value: 30 <p>You must restart the SWIFTNet Interface Services (SNIS) component, to apply the changes to this parameter.</p>
Retry Timer	<p>Indicates the timeout period (in seconds) between two attempts to emit a message:</p> <ul style="list-style-type: none"> • Maximum value: 120 • Minimum value: 0 • Default value: 60 <p>You must restart the SWIFTNet Interface component, to apply the changes to this parameter.</p>

5.13.1.13 Event

Event parameter

Parameter	Description
SNMP Max Event Size	Indicates the maximum size of the event text distributed to SNMP managers. 0 means that there is no maximum size. Default value: 2000.

5.13.1.14 File

File parameter

Parameter	Description
File Digest Algorithm	Indicates the default file digest algorithm that Alliance Access uses to compute the digest on the payload file of the FileAct message if no file digest algorithm is provided by the back-office application. The following values exist: SHA-1 and SHA-256. Default value: SHA-256. Changes to this parameter take effect immediately.

5.13.1.15 Message

List of message parameters

Parameter	Description
Check EP/LT existence	Activates the rejection of MT messages submitted with LTX when there is no LT defined for the LTX BIC8 and the rejection of IA/FA messages when there is no Emission Profile for the message Requestor DN/Service. Possible values are <code>on</code> (activates the check) or <code>off</code> (no check). The default value is <code>off</code> . Changes to this parameter take effect immediately.
Default emission expiry	Indicates the default time (in minutes) to be added to the message creation date and time to calculate its emission expiry date and time. This parameter applies only to messages submitted without an emission expiry date and time. Possible values are integers from 1 to 43200. The default value is 28800. Changes to this parameter take effect immediately. This parameter impacts InterAct and FileAct messages (RT or SnF). If a message fails transmission, it is retried until the message expires (that is, until it reaches the expiration date and time) or until the emission is manually cancelled.
Expansion Language	Specifies the language that message expansion fields are displayed in. Default value: English. Changes to this parameter take effect when an application is restarted.
LT load balancing	Starts the automatic allocation of logical terminal allocation. Possible values are: <ul style="list-style-type: none"> <code>on</code> - the messages originated by a destination can be transmitted by any logical terminal which is logged in and assigned to that destination. <code>off</code> - the logical terminal specified in the message transmits the message. Default value: <code>off</code> . You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.

Parameter	Description
Maximum File Size	<p>Indicates the maximum size of a file in Mbytes (Mb) that a back-office application can send to Alliance Access.</p> <ul style="list-style-type: none"> • Maximum value: 2048 • Minimum value: 1 • Default value: 250 <p>You must restart the Application Interface Services (MXS) component, to apply the changes to this parameter.</p>
RMA authorisation for T&T	<p>Specifies whether RMA Authorisation is required for FIN Test and Training messages. Possible values are:</p> <ul style="list-style-type: none"> • Not required • Required <p>Default value: Not required.</p> <p>You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.</p>
RTV Routing	<p>Controls the RTV routing information in a retrieved message. When this parameter is set to:</p> <ul style="list-style-type: none"> • off - the routing_code field for a retrieved message is set to RTV • on - the disposition_address_code field for a retrieved message is set to RTV. <p>You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.</p> <p>Default value: off.</p>
Common Ref Calculation	<p>Controls the calculation of the Common Reference, which is part of field 22 of Block 4, in FIN messages that are input through message partners and that have the data format CAS, RJE, DOS-PCC, or XML version 2. Alliance Access always calculates the Common Reference in messages that a user enters manually.</p> <p>The values are:</p> <ul style="list-style-type: none"> • Yes - Alliance Access calculates the Common Reference, even it exists in field 22. • No - does not calculate the Common Reference in field 22. In this case, the values of Validation level and Message Modification allowed are ignored, and a NAK may be received if field 22 of the message contains incorrect information. <p>Default value: Yes.</p> <p>You must restart the Application Interface Services (MXS) component to apply the changes to this parameter.</p>

Parameter	Description
FT Monitoring Retention	<p>The number of days during which a file transfer with the status <code>Completed</code> or <code>Aborted</code> remains visible in the list of File Transfers in the Monitoring package.</p> <p>The list can contain a maximum of 1000 completed or aborted file transfers. This limit ensures that the performance of Alliance Access remains optimal. Therefore, if the list contains 1000 completed or aborted file transfers, then Alliance Access Configuration removes the oldest of those file transfers.</p> <p>You must restart the SWIFTNet Interface component to apply the changes to this parameter.</p> <p>Maximum value: 30</p> <p>Default value: 0</p> <p>Regardless of the value set for this parameter, a restart of the servers will clear file transfer records from Message Management > File Transfer Monitoring or Monitoring > File Transfers.</p>
Activate cold start	<p>Determines if cold start processing should be automatically started upon receipt of an MT 082 report (with cold start indication) for FIN, or an xsys.005.002 report for InterAct and FileAct.</p> <p>Possible values are <code>Activate</code> and <code>Deactivate</code>. The default value is <code>Activate</code>.</p> <p>Changes to this parameter take effect immediately.</p>
FIN CS Time Margin	<p>Time margin (in minutes) applied by Alliance Access when performing cold start MT082 post-processing.</p> <p>The minimum value is 0 and the maximum value is 780. The default value is 15.</p> <p>Changes to this parameter take effect immediately.</p>
W3C - Primary SAG list	<p>List of primary SWIFTNet connections to be used for handling W3C signature computation and verification requests submitted with no SWIFTNet connections.</p> <p>This is a comma-separated list of SWIFTNet connections, which is by default empty.</p> <p>This parameter is applicable in the context of W3C signature Web services, either exposed by means of a Web service or the Connector for T2S. For more information, see the Alliance Access T2S Web Services Developer Guide or the Connector for T2S Release Letter.</p>
W3C - Secondary SAG list	<p>List of secondary SWIFTNet connections to be used to handle W3C signature computation and verification requests submitted with no SWIFTNet connections, when none of the SWIFTNet connections in the W3C - Primary SAG list is available.</p> <p>This is a comma-separated list of SWIFTNet connections, which is by default empty.</p> <p>This parameter is applicable in the context of W3C signature Web services, either exposed by means of a Web service or the Connector for T2S. For more information, see the Alliance Access T2S Web Services Developer Guide or the Connector for T2S Release Letter.</p>

5.13.1.16 Network

List of network parameters

Parameter	Description
SWIFTNet Batching Timeout	<p>Maximum delay (in seconds) that Alliance buffers an input message before it is sent. SWIFT determines the final value used. Default value: 2.</p> <p>You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.</p>
SWIFTNet Max batch count	<p>Maximum number of FIN APDUs that can be sent in a single DATA PDU. SWIFT determines the final value used. Default value: 30.</p> <p>You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.</p>

Parameter	Description
Reconnect Timer	Indicates the time (in minutes) after which the SWIFTNet Interface component (SNIS) attempts to reconnect an interrupted profile. Default value: 20. Minimum: 1. Maximum: 300. You must restart the SWIFTNet Interfaces Services (SNIS) component, to apply the changes to this parameter.
Preferred Order	Used by the Message Preparation application to propose a default value for the preferred network when the receiver is a wild address, that is, the network address is not in the correspondent file. The default display order is SWIFT, APPLI, OTHER, IPLA . Changes to this parameter take effect when the application is restarted.
Usersync - Max Retries	Specifies the number of attempts that are allowed to reconnect a failed communication session with the SWIFT network. Default value: 20. You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.
Usersync - Max Time	Specifies the duration (in minutes) for which attempts to reconnect a failed communication session with the SWIFT network are made. Default value: 30. You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.
Usersync - Retry Timer	Specifies the time-out period (in seconds) between reconnect retries. Default value: 120. You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.

5.13.1.17 Performance

List of performance parameters

Parameter	Description
Active Correspondent	Controls whether correspondents are checked to see whether they have an active status, before sending a message. The possible values are "On" or "Off". Default value: On. You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.
FIN Keyword Extraction	Controls whether keywords are extracted from incoming (output) MT messages. The possible values are "On" or "Off". Default value: On. You must restart the SWIFT Interfaces Services (SIS) component, to apply the changes to this parameter.
Maximum Read Rate	Disk I/O in MB/sec used to read from the database disks when a Recovery Backup is created. Minimum: 0. Maximum: 1024. Default value: 0. If the value is 0, then maximum disk I/O is used. Change to this parameter take effect at the next recovery backup creation. This parameter is ignored unless the Alliance servers are running and option 14:DATABASE RECOVERY is licensed.
MQSA Interventions	Controls whether the writing of some interventions is suppressed. The possible values are "None", "All", or "System". Default value: None. You must restart the SMQS component, to apply changes to this parameter. This parameter applies to the WebSphere MQ Interface for Alliance Access (MQSA). It does not apply to the WebSphere MQ Host Adapter.

Parameter	Description
MX Keyword Extraction	Controls whether keywords are extracted from incoming (output) MX messages. The possible values are "On" or "Off". Default value: On. You must restart the SWIFTNet Interfaces Services (SNIS) component, to apply the changes to this parameter.
Routing Intervention	Controls what types of interventions are suppressed. The possible values "All", "System generated only", or "None". Default value: None.

5.13.1.18 Print

List of print parameters

Parameter	Description
Message Search Results	Specifies the maximum number of items that can be printed in a Message Search Report. Default value: 1024. The value "0" means that no limit is set.
Skip Interventions	Specifies whether Printer message partners print notifications without system or user interventions. This does not apply to transmission notifications. The default value is No, with notifications being printed with system or user interventions. Setting this parameter to Yes saves paper when notifications are printed.
ST200-like Format	Specifies whether Printer message partners print messages in an ST200-like format, with an eye-catcher and warning banner. This parameter has no effect when messages are printed to a file. Default value: No.

See also "Display/Print" on page 117.

5.13.1.19 Queue

Queue parameter

Parameter	Description
Threshold	Frequency of alarm generation - the number of messages that can be added above a queue threshold or the number of overdue message instances before a new alarm will be generated. Minimum: 20. Maximum: 100. Default value: 20. Changes to this parameter take effect at the next alarm.

5.13.1.20 Receiver

List of receiver parameters

Parameter	Description
Default HQ for MT074	Specifies the receiver for system messages 074. Default value: SWHQBEBBBCT.
Default HQ for MT090	Specifies the receiver for system messages 090. Default value: SWHQNLNLXXX.

5.13.1.21 Reception

Reception parameter replaced by GUI option

As of Alliance Access 7.0.75, the **SnF RProf Resequencing** global system configuration parameter has been discontinued. It is replaced by an **OSN Resequencing** GUI option at the individual Store-and-Forward reception profile level. As a result, Alliance Access applies OSN

resequencing to a Store-and-Forward reception profile if its **OSN Resequencing** option is selected or if its `SAA_DO_RESEQ_<RPName>` environment variable is set to `On`. Alliance Access does not apply OSN resequencing to a Store-and-Forward reception profile only when both indicators are off.

For more information on the **OSN Resequencing** GUI option, see the section on the **Configuration** tab of the **Reception Profile Details** window in the [Configuration Guide](#).

5.13.1.22 Reporting

Reporting parameters

Parameter	Description
Mail server address	Defines the <code>HOST:PORT</code> that will be used by the Operational Reporting mail server. <code>HOST</code> can be either an IP address or a hostname. Changes to this parameter take effect immediately.
Activate Reporting	If set to Activate , Operational Reporting is activated. This will copy all messages to the reporting data store, which may take some time, depending on the number of messages. Set this parameter to Deactivate to deactivate Operational Reporting, which will remove all message data from the reporting data store.

5.13.1.23 RMA

RMA parameter

Parameter	Description
Auto Refresh	If this parameter is set to <code>No</code> , then the automatic refresh of the view lists is disabled in the Relationship Management application. Default value: <code>Yes</code> . You must restart the Relationship Management Application (RMA) component, to apply the changes to this parameter.

5.13.1.24 Shutdown

List of shutdown parameters

Parameter	Description
Delayed	After a request to stop the servers, this is the number of seconds delay before the GUI applications are terminated. Default value: 120.
Forced	After a request to stop the servers, this is the number of seconds delay before the server processes are terminated. Normally the server processes stop before this time has elapsed. Default value: 240.

5.13.1.25 System

System parameter

Parameter	Description
Startup Mode	<p>This parameter enables Alliance Access to start automatically after the machine where the Alliance Access instance is installed is rebooted.</p> <p>On UNIX or Linux, this parameter can have the following values:</p> <ul style="list-style-type: none"> • <code>Automatic</code> - Alliance Access starts as a result of starting the Alliance Access bootstrap • <code>Manual</code> - An operator must explicitly start Alliance Access. <p>Default value: <code>Manual</code>.</p> <p>On Windows, this parameter can have the following values:</p> <ul style="list-style-type: none"> • <code>Service</code> - Alliance Access runs as a Windows service under control of the Alliance Access Bootstrap service. <p>In Service mode, mapped network drives cannot be used.</p> <p>Tip To start Alliance Access automatically after a reboot, select <code>Service</code> and use the Windows Service Management interface to configure the Alliance Access Bootstrap service to start automatically</p> <ul style="list-style-type: none"> • <code>Normal</code> - Alliance Access does not run as a Windows service. <p>Default value: <code>Normal</code>.</p>
SNMP Heartbeat Interval	<p>This parameter enables you to activate/deactivate the SNMP heartbeat functionality and, if activated, to define the number of seconds between two SNMP heartbeats.</p> <p>Possible values are 0 and 120-900 (the number of seconds between two SNMP heartbeats). 0 means that the heartbeat functionality must not be activated.</p> <p>All values less than 120 mean the heartbeat is not active.</p> <p>Changes to this parameter will take effect at the next heartbeat or at most 900 seconds later if the heartbeat is not active.</p>
SNMP Heartbeat Dist. List	<p>This parameter enables you to provide the name of the distribution list to be used for sending SNMP heartbeat trap to SNMP servers.</p> <p>Create this distribution list and populate it with the SNMP server(s) to which the SNMP heartbeat must be sent.</p> <p>The list name can be up to 15 characters long.</p> <p>Changes to this parameter will take effect at the next heartbeat.</p>

5.13.1.26 Traffic Recon

Traffic Recon parameter

Parameter	Description
Delivery Notif	If set to Yes, then Traffic Reconciliation generates notifications for each matched message instance. Default value: Yes.
FIN Mult. reconciliation	If set to yes, FIN messages can be reconciled multiple times. Default value: No.

Parameter	Description
Msg reconciliation cycle	Interval (in seconds) at which Alliance Access reconciles messages. Possible values 60-600. Default value: 300. Changes to this parameter take effect at the next reconciliation poll.

5.13.1.27 WebSphere MQ

List of WebSphere MQ parameters

If the licence package **13:MQ HOST ADAPTER** is installed, then the following parameters are available:

Parameter	Description
Connection Mode	<p>Specifies the mode that the Web Sphere MQ interface of Alliance Access uses to connect to a Queue Manager. The options are:</p> <ul style="list-style-type: none"> • Client - The WebSphere MQ interface can connect at the same time to multiple Queue Managers which are located on the same host or on a different host as the MQ Adapter. <p>Note See the WebSphere MQ client and WebSphere MQ server components in the WebSphere MQ Interface User Guide for information about setting the environment variables for "MQSERVER" and "MQ channel table".</p> <ul style="list-style-type: none"> • Server - The WebSphere MQ interface can connect to one Queue Manager located on the same host as Alliance Access. <p>Default value: Server.</p> <p>You must restart the Application Interface Services (MXS) component, to apply the changes to this parameter.</p>
Input Message Rate Limit	<p>Limits the number of messages that Alliance Access reads per second from all the WebSphere MQ queues that are configured in Alliance Access.</p> <p>The default value is 0, which means that the incoming WebSphere MQ traffic is not limited. Minimum: 0. Maximum: 999.</p> <p>Before you change this parameter, you must disable all the Websphere MQ message partners.</p>
Recovery Time - Initial	The time interval, in seconds, after which the first attempt to reopen the communication session with WebSphere MQ is made in case of a broken connection. Default value: 60.
Recovery Time - Increment	The increase of the time interval, in seconds, between consecutive attempts to reopen a WebSphere MQ session. Default value: 30.
Recovery Time - Max	The maximum time interval, in seconds, between consecutive attempts to reopen a WebSphere MQ session. Default value: 600.

Required permissions for WebSphere MQ

Following are the permissions that are required for WebSphere MQ:

Type	Permissions
Queue Manager	<ul style="list-style-type: none"> • connect • inq

Type	Permissions
	<ul style="list-style-type: none"> • setid
Input Queues	<ul style="list-style-type: none"> • get • inq
Output Queues	<ul style="list-style-type: none"> • put • setid

To set the access rights, use the `setmqaut` command on the WebSphere MQ server.

To display the access rights, use the `dspmqaut` command on the WebSphere MQ server.

5.13.2 Parameters Page

Content

The **Parameters** page contains these elements:

- A filtering criterion and filtering functionality that enable you to filter the list entities on the **Parameters** page:
 - See "Details" on page 126
 - See "Functions" on page 22
- Details of the available parameters
See "Details" on page 126

Display

The screenshot shows the 'Parameters' page with the following interface elements:

- Parameters** header.
- Filtering Criteria** section with a **Name** input field and **Submit** and **Report** buttons.
- Parameters** list table with columns: **Component**, **Class**, **Name**, and **Value**. The table shows 20 rows in total, with 1 selected.
- Buttons for **Change View** and **Report**.
- Navigation buttons for **Previous** and **Next**.
- Information text: **Rows in list: 20, in selection: 1**.

The list table data:

Component	Class	Name	Value
BSA	Display Format	Amount	Decimal-Comma/Thousand-Nothing
BSA	Display Format	Date	European
BSA	Display Format	Time	Day of 24 Hours
BSA	Alarm	Maximum	3

Details

Column	Description	Filtering criteria
Component	The component the parameter belongs to	
Class	The class the parameter belongs to	
Name	The name of the parameter For filtering, the wildcard characters % and _ enable you to search for a group of names.	✓

Column	Description	Filtering criteria
Value	The value of the parameter	

5.13.3 Parameter Details Window

Content

The **Parameter Details** window contains these elements:

- Details of the parameters
See "Details" on page 127
- Functions that enable you to manage the parameters
See "Functions" on page 127

Display



Details

Field	Description
Component	The component the parameter belongs to
Class	The class the parameter belongs to
Name	The name of the parameter
Description	The description of the parameter
Value	The value of the parameter. See the Description to have an indication of the possible values.

Functions

Function	Description
Reset to Default	Enables you to reset the parameter to its default value Procedure: "Reset a Parameter to its Default Value" on page 128

5.13.4 Modify a Parameter

Purpose

This procedure enables you to modify the value of a parameter.

If the modification has an impact on the layout of some screens, the operators currently logged on have to log off and log on again to see the changes.

Users and permissions

To display the list or the details of parameters, your operator profile must have this action:

- **System Management**

To modify a parameter, your operator profile must have this action:

- **System Management / Mod Config. Param.**

Security officers can modify parameters.

Procedure

1. From the list of parameters, click the row of the parameter that you want to modify.

The **Parameter Details** window opens.

2. Change the value in the **Value** field as needed.

3. Click **Save**.

A status popup message appears.

4. Click **Close**.

The **Parameter Details** window closes.

5.13.5 Reset a Parameter to its Default Value

Purpose

This procedure enables you to reset the value of a parameter.

If the modification has an impact on the layout of some screens, the operators currently logged on have to log off and log on again to see the changes.

Users and permissions

To display the list or the details of parameters, your operator profile must have this action:

- **System Management**

To reset a parameter to its default value, your operator profile must have this action:

- **System Management / Mod Config. Param.**

Security officers can reset the values of parameters.

Procedure

1. From the list of parameters, click the row of the parameter that you want to reset.

The **Parameter Details** window opens.

2. Click **Reset to Default**.
3. Click **Save**.
A status popup message appears.
4. Click **Close**.
The **Parameter Details** window closes.

5.14 Security Parameters

5.14.1 Security Parameters

Overview

Alliance Access contains a number of security parameters that control system security. Only security officers can modify these parameters. Both security officers must approve any modifications.

IPLA security configuration parameters

In addition to the classes listed here, security configuration parameters resulting from installing components for IPLA may also appear. The bundle symbolic name appears as the value for Class. The value for Component is `IPLA`.

5.14.2 Classes of Security Parameters

5.14.2.1 Alarm

List of Alarm parameters

Component	Parameter	Description
BSS	Path of Script File	<p>Full pathname of the user-defined script that Alliance Access runs when an Alarm Event occurs.</p> <p>It must be:</p> <ul style="list-style-type: none"> • owned by the Alliance Administrator • located in a directory accessible by this user • UNIX or Linux: it must be compliant with the requirements of the UNIX or Linux exec system call, regarding the execution of an interpreter file. <p>Maximum length: 255</p> <p>Default value: none</p>

5.14.2.2 Backup integrity

List of Backup integrity parameters

Component	Parameter	Description
BSS	Backup integrity	<p>Specifies the type of digest that is calculated to ensure the integrity of archive backups.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Fast - integrity of the backup is based on a digest covering the metadata. • Full - a second digest is added, covering the data in the backup. <p>Default value: Full</p>

5.14.2.3 Mesg Archive

List of Mesg Archive parameters

Component	Parameter	Description
BSS	Archive Method	<p>Possible values are:</p> <ul style="list-style-type: none"> • Normal - create the archive (all messages must be completed). • Destructive - do not create archive, all messages must be completed, and are deleted from the database. <p>Default value: Normal.</p>

5.14.2.4 Message

List of Message parameters

Component	Parameter	Description
BSS	Check authorisation exist	<p>Indicates whether the existence of an RMA authorisation is checked during message entry or message modification.</p> <p>Note: If you have the licence option 07:STANDALONE REC, then this parameter indicates whether an RMA check is performed whatever the network is (OTHER included).</p> <p>Default: Yes.</p>

Component	Parameter	Description
MXS	Continue on LAU failure	<p>This parameter is only applicable for message partners configured with the WebSphere MQ connection method.</p> <p>When this parameter is set to off, Alliance Access will reject a message that arrives on an input message partner if the LAU check fails. At the same moment, the message partner sessions will be stopped.</p> <p>When the parameter is set to on, messages arriving from an input message partner that fail the Local Authentication check will still be accepted by Alliance Access, and the message partner will continue to process messages, while a specific event is generated. In such a situation, you should check the routing rules of all message partners ensure that the appropriate behaviour is achieved (for example, to move the messages to the <code>_MP_emi_sec</code> queue and force them to pass through authorisation). Assigning the messages to a specific UNIT can help you to control who can handle these exceptions, as well as locating them back in the message database.</p> <p>To change the default behaviour, the routing rule(s) handling the LAU failure using the new <code>LAU_RESULT_FAILURE</code> routing keyword should be set as first routing rule(s) of <code>_AI_from_APPLI</code>.</p> <p>For changes to this parameter to take effect, the Application Interface component must be restarted.</p>
BSS	FIN CS time margin	<p>Time margin (in minutes) applied by Alliance Access when performing cold start MT082 post-processing.</p> <p>The minimum value is 0 and the maximum value is 780. The default value is 15. Changes to this parameter take effect immediately.</p>
BSS	Journalise Msg Text	<p>If this parameter is set, then the text block from the message is included in the message event description. A change to this parameter takes effect after the SWIFT Interface component is restarted.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Message Text Journalised • Message Text Not Journalised <p>Default value: Message Text Journalised</p>
BSS	Message Repair Action	<p>Indicates the type of action that is performed by default on the outstanding live messages, which are flagged with possible duplicate emission (PDE), if the database is partially recovered.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Prompted: the user can select an option when the tool is launched. • None: the messages are routed as defined • Complete: the messages are completed • Investigate: the messages are routed to the <code>_MP_recovery</code> queue for investigation. <p>Default value: Prompted</p> <p>This parameter appears when either 14:DATABASE RECOVERY or 13:HOSTED DATABASE are licensed.</p>

Component	Parameter	Description
SIS	MT398 message extraction	<p>Specifies whether the SWIFT Interface component performs a proprietary authentication code (PAC) verification on messages embedded in the MT 398. A change to this parameter takes effect after the SWIFT Interface component is restarted.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Off • On <p>Default value: Off.</p>
BSS	Re-activation Scope	<p>Determines whether completed messages are re-activated at a routing point.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Full: all the allowed routing and exit points appear. • Partial: only exit points appear. • Restricted: The target re-activation queue is selected automatically, as follows: <ul style="list-style-type: none"> – input messages: Text Modification queue – output messages: Modification After Reception queue <p>Default value: Full.</p>
SIS	Retrieved message extract	<p>Indicates whether the SWIFT Interface component extracts the contents of MT 021 of output messages into separate messages. A change to this parameter takes effect after the SWIFT Interface component is restarted.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • On • Off <p>Default value: Off.</p>

5.14.2.5 Operator

List of Operator parameters

Component	Parameter	Description
BSS	Prefix Operator Name	<p>If this parameter is activated, then Alliance Access validates the BIC8 prefix of an operator name when the operator is created. If an operator name is modified, then the name is validated only if the operator name already has a BIC8 prefix.</p> <p>The prefix must meet the following conditions to be valid:</p> <ul style="list-style-type: none"> • The prefix must be a BIC8 (upper case) followed by an underscore (_) character. • The BIC8 must be one of the licensed destinations of the Alliance Access instance (either production, or Test and Training). • If the <i>creating</i> operator has one or more restricted BIC delegations, then the prefix must be a BIC that is delegated to the <i>creating</i> operator. • If the <i>created</i> operator has one or more restricted BIC delegations, then the prefix must be a BIC that is delegated to the <i>created</i> operator. • If the <i>created</i> operator has one or more restricted profile delegations, then the names of the selected profiles must start with a BIC8 that is delegated to the <i>creating</i> operator. <p>This parameter is useful for institutions that use or manage multiple BICs.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Yes: Validate the prefix of an operator name • No: Deactivate the validation of the prefix <p>Default value is No.</p>
BSS	Restrict Delegation	<p>The left security officer and right security officer of a service bureau use this feature when creating local security officers. Indicates whether restrictions are applied for operator profiles, units, and destinations.</p> <p>This parameter does not affect the left security officer and right security officer because they always have unrestricted access to operator functions.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Yes: An operator who is adding a new operator can only select operator profiles, units, and licensed destinations from a restricted list. <p>If set to Yes, then this parameter overrides the Restrict Functions parameter.</p> <p>No: Delegation is not possible.</p> <p>Default value: No.</p>

Component	Parameter	Description
BSS	Restrict Functions	<p>Specifies whether the operator-related functions (open, print, add, modify, approve, or remove) are restricted.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Yes: <p>An operator with the appropriate entitlements can only perform these functions on the operators that belong to a subset of the same units as the operator performing out the action.</p> <p>For more information, see "Definition of Units and Restrict Functions" on page 236.</p> <ul style="list-style-type: none"> • No: these functions are not restricted, and an operator with the appropriate entitlements can search for, open, print, add, modify, approve, or remove operators belonging to any unit. <p>Default value: No.</p> <p>This parameter does not affect the left security officer and right security officer because they always have unrestricted access to operator functions.</p>
BSS	Software Owner Profile	<p>Specifies the operator profile that is assigned as the owner of the software. An operator with that profile can perform specific actions on Alliance Access, such as exporting configuration data or querying the database for messages or events.</p> <p>If this parameter is empty or invalid, then the software owner operator is disabled.</p> <p>The servers must be restarted for changes to this parameter to take effect.</p>

5.14.2.6 Password

List of Password parameters

Component	Parameter	Description
BSS	Illegal Patterns	<p>Specifies the patterns of characters that are not allowed in passwords. An error message appears if any operator tries to create a password which contains one of the defined characters or character strings.</p> <p>Both security officers must approve any changes to this parameter.</p> <p>Type a string consisting of patterns separated by . Changes to this parameter take effect the next time an operator changes a password.</p> <p>Maximum length: 255</p> <p>For example, @ \$ Bob prohibits the use of the following characters in passwords:</p> <p>@, \$, or Bob</p>
BSS	Master Period	<p>Specifies the number of days after which the security officers have to change the Master Passwords.</p> <p>The possible values are 0 through 365.</p> <p>Default value: 100.</p> <p>A value of 0 means that the security officers are never forced to change their passwords.</p>

Component	Parameter	Description
BSS	Max Bad Pwd	<p>Specifies the maximum number of times that a user can enter incorrect passwords before the sign-on action is refused. Both security officers must approve any changes to this parameter.</p> <p>Alliance Access monitors invalid password entries. A parameter can be used to disable an operator who has not entered a valid password within a defined number of attempts. When disabled, an operator cannot sign on to Alliance Access (even with the correct password) until a security officer or an operator with the correct permissions re-enables it.</p> <p>If a security officer exceeds the specified number of attempts (when signing on or when changing their password), they are disabled for a period of 10 minutes.</p> <p>Possible values are 0 through 100</p> <p>Default value: 5.</p> <p>If the value is set to 0, then an unlimited number of password entry attempts is allowed (this is not recommended for security reasons).</p>
BSS	Min Pwd Length	<p>Specifies the minimum length of the user password.</p> <p>Possible values are 4 through 20.</p> <p>Default value: 6.</p>
BSS	Nbr Retained Pwd	<p>Specifies the number of user passwords that Alliance Access keeps track of.</p> <p>Whenever a user password is successfully updated, the old user password is written to that user's password history file. Alliance Access can check a user's password history file and prevent the user from changing the password to one that has been used before.</p> <p>Both security officers must approve any changes to this parameter.</p> <p>Possible values are 0 through 20.</p> <p>Default value: 10.</p>
BSS	Reset Peer Officer Passwo	<p>Specifies whether the left security officer can reset the right security officer's password to the Master Password which was valid at the time of installation, and vice versa. This is useful if a security officer forgets a password. An event is written to the Event Log each time that a password is reset.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Yes • No: the security officers cannot reset each other's password. <p>Default value: No.</p>

Component	Parameter	Description
BSS	Sec Officer One Time Pwd	<p>Activates the use of one-time passwords for the security officers. The value of this parameter applies to both security officers.</p> <p>Both security officers must approve a change to this parameter before it takes effect. Until both security officers have not approved the change, the security officers must log on using their user-defined password.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Yes: If the Sec Officer OTP Srv Group parameter is correctly set and approved, then the left security officer and right security officer can use one-time passwords. • No: the master passwords have to be used at the next sign-on of the left security officer and the right security officer, and their password must be changed as if it was the first logon. <p>Default value: No.</p>
BSS	Strong Validation	<p>Specifies whether passwords are validated as being strong from a security perspective. Changes to this parameter become effective when an operator changes the password. If the new password fails the strong validation test, then an appropriate error appears to the operator indicating that the password is not compliant with the strong validation rules.</p> <p>Both security officers must approve any changes to this parameter.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Yes: validates that the user password contains a combination of alphabetic and numeric characters, with at least 1 numeric character. • No <p>Even if the value is set to No, all the other validation rules (such as illegal pattern verification and minimal number of characters) remain applicable.</p> <p>Default value: No.</p>
BSS	User Period	<p>Specifies the number of days that a user can use a password before the password must be changed. Both security officers must approve any changes to this parameter.</p> <p>Possible values are 0 through 120.</p> <p>If the value is set to 0, then passwords are valid indefinitely (this is not recommended for security reasons).</p> <p>Default value: 30.</p>
BSS	Sec Officer OTP Srv Group	<p>Specifies the authentication (OTP) server group that is assigned to a security officer if both security officers are configured to use authentication by means of the Sec Officer One Time Pwd parameter.</p> <p>This is a textual parameter. By default, this value is empty.</p>

5.14.2.7 Reports

List of Reports parameters

Component	Parameter	Description
BSS	Root Path for Report File	<p>The path name which is the top level of the directory tree where report files are stored.</p> <p>Maximum length: 64</p> <p>The default location is:</p> <ul style="list-style-type: none"> • UNIX or Linux: \$ALLIANCE/usrdata/report • Windows: C:\Alliance\Access\usrdata\report

5.14.2.8 RMA

List of RMA parameters

Component	Parameter	Description
RMS	Auto Accept Updates	<p>Indicates whether Alliance Access automatically applies the updates that it receives for an Enabled authorisations-to-send.</p> <p>A change to this parameter is immediately taken into account.</p> <p>Default value: No</p>
RMS	Clean up Stale Auth.	<p>Specifies the minimum number of days that an authorisation or a query must be kept before it can be removed.</p> <p>A change to this parameter becomes effective immediately.</p> <p>Possible values are 1 through 365.</p> <p>Default value: 180</p>
RMS	Needs Status Confirmation	<p>Indicates whether an operator must confirm the revocation or rejection of an authorisation.</p> <p>A change to this parameter becomes effective immediately.</p> <p>Default value: Yes</p>

5.14.2.9 Signoff

List of Signoff parameters

Component	Parameter	Description
BSA	Timeout	<p>Specifies the number of seconds after a Signon Timeout occurs that an operator can be inactive on Alliance Workstation before the operator is logged off automatically from Alliance Workstation.</p> <p>Possible values are 0 through 3600.</p> <p>Default value: 1800</p> <p>If the value is set to 0, then the Alliance Workstation is not signed off automatically.</p>
BSS	WS Session Timeout	<p>The number of seconds that a web-service operator session can remain inactive before the session is stopped and removed.</p> <p>The possible values are 1800 through 5400. Default value: 2700.</p>

5.14.2.10 Signon

List of Signon parameters

Component	Parameter	Description
BSS	Multiple	<p>Specifies the numbers of concurrent sign-ons to Alliance Access that the same operator is permitted to perform.</p> <p>Possible values are 1 through 10.</p> <p>Default value: 1</p> <p>For example, if the value is set to 2, then the operator can sign on to the same instance of Alliance Access from two different Alliance Workstations. However, an attempt to log on from a third Workstation will be rejected.</p> <p>If a login attempt fails because the maximum number of sessions for the operator has been exceeded and the operator attempts to log in again, a prompt is displayed that asks if Alliance Access can terminate the session that has been idle for the longest time. If the operator accepts, the login proceeds. Otherwise, the login is rejected.</p>
BSA	Timeout	<p>Specifies the number of seconds that an operator can be inactive, before the operator has to re-enter the password. For more information, see "Use of timeout parameters".</p> <p>Possible values are 60 through 28800.</p> <p>Default value: 600</p>

Use of timeout parameters

Following a successful sign-on to Alliance Access, an inactivity timer is started, which is reset each time an operator performs some activity within Alliance Access. When the inactivity timer expires, all windows on the screen are frozen. The same operator must re-enter a password before being allowed to continue. Having re-entered the correct password, all windows are reinstated and the operator can continue work.

This feature helps to prevent unauthorised users from using Alliance Access, if an operator is called away. It is not intended to replace the normal practice of signing off from Alliance Access, for example, when an operator leaves to take a break.

Alliance Access uses a total of four session timeout parameters related to operator sign-on, three of which are global security configuration parameters:

- **Signon Timeout**
- **Signoff Timeout**
- **WS Session Timeout**

In addition, the operator profile definition contains the following parameter: **Access Control > Signon > WS Session Timeout**.

Alliance Web Platform contains the **Session Expiry Timeout** parameter, which is found in the configuration of the Alliance Web Platform 7.0 package.

On Alliance Web Platform, when the value of the **Session Expiry Timeout** parameter is smaller than the value of the **WS Session Timeout** parameter, and when an operator is inactive for a time period equal to the parameter **Session Expiry Timeout**, Alliance Web Platform ends the session. The message "You have been logged out because the user session expired" is displayed and you must re-enter the operator name and password. This is the recommended set-up and behaviour.

On Alliance Web Platform, when the value of the **WS Session Timeout** parameter is smaller than the value of the **Session Expiry Timeout** parameter, and when an operator is inactive for a time period equal to the value of the **WS Session Timeout** parameter, Alliance Access ends the session. The operator does not see this until he tries to perform an action, when a message pop-up is displayed, as follows:

- For the RMA or Configuration GUI package, the following message is displayed: "Your Alliance Access/Entry session is no longer valid. Please logout and login again."
- For the Message Management GUI package, the following message is displayed: "Failed to communicate with Alliance Access/Entry. The connection to Alliance Access/Entry has dropped." In this case, it is also necessary to log out and log in again.
- For the Monitoring GUI package, there is a built-in mechanism to keep the session alive, therefore the sessions never expire.

Note If the value of the **WS Session Timeout** parameter in the operator profile is set to 0, then the value of the global **WS Session Timeout** parameter is taken into account. If the value of the **WS Session Timeout** parameter in the operator profile is other than 0, then this value is used by the application.

On Alliance Workstation, when an operator is inactive for a time period equal to the value of the **Signon Timeout** parameter, a pop-up is displayed that prompts the operator to re-enter his password. If the operator does not provide his password, then the pop-up disappears after a period of time equal to the value of the **Signoff Timeout** parameter.

5.14.2.11 System

List of System parameters

Component	Parameter	Description
IPLA	Allow Starting IPLA	<p>Indicates if the Integration Platform (IPLA) component can be started. Possible values are Yes and No. Default value: No</p> <p>Changing the value from Yes to No is considered the next time that there is an attempt to start IPLA, either manually or when Alliance Access starts. Changing the value from No to Yes allows starting the IPLA component manually.</p> <p>If the IPLA component has been stopped, it must be started manually even if the value is set to Yes. Afterwards, the IPLA component will start automatically.</p> <p>The security mechanisms of Alliance Access (such as the calculation of a database signature per data record) protect the messages and files processed by IPLA.</p>
SSS	Authenticate MT971	<p>Indicates whether MT971 must be authenticated. A change to the parameter will be taken into account immediately.</p> <p>Default value: Yes</p>

Component	Parameter	Description
BSS	Disable Period	<p>The number of calendar days during which an enabled operator must sign on to Alliance Access. Otherwise, the status is changed to disabled.</p> <p>Possible values are 0 through 999.</p> <p>Default value: 0</p> <p>If this parameter is set to 0, then operators are not disabled automatically, if they do not sign on.</p> <p>A value of 0 cancels automatic disable. Changes to this parameter will take effect at midnight or at the next restart of the Alliance servers.</p>
BSS	RPC Authentication	<p>Communication with Alliance Web Platform is always started with SSL enabled, and server authentication is required. Therefore, changes to this parameter do not affect the communication with Alliance Web Platform.</p> <p>For Alliance Workstation, this parameter specifies whether the communication between Alliance Access and Alliance Workstation is encrypted. Only when the parameter is set to "Data Integrity" or "Data Confidentiality" can the Alliance Access servers initialise the communication process with SSL enabled. If SSL is enabled, then Alliance Workstation can also use Server Authentication. For more information, see the System Management Guide.</p> <p>This parameter provides additional security checks on client processes that make Remote Procedure Calls (RPC) to server processes.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> Off - processes making RPCs are not checked to ensure that they are authenticated. Process Authentication - processes making RPCs are checked to ensure that they are authenticated. Data Integrity - in addition to Process Authentication, Alliance calculates a check value based on the character field data in the RPC call. The check value and the RPC call are passed to the server. The server recalculates the check value from the RPC data, and compares it to the check value that it received. This ensures the integrity of the RPC data. If any changes have been made to the data, then the check values will not match. Data Confidentiality - in addition to Data Integrity, the following RPC call data is encrypted to ensure confidentiality: <ul style="list-style-type: none"> all fields that are currently encrypted in the database (such as the operator password). all message details that are derived from the message text. <p>Default value: Process Authentication.</p> <p>Alliance Access must be restarted for changes to this parameter to take effect.</p>
BSS	Software Check at Startup	<p>Indicates whether the system runs the Integrity Verification Tool to check the integrity of the software when Alliance Access is started.</p> <p>Default value: Yes</p>

Data confidentiality

If a large number of message templates are assigned to a unit, then using the higher levels of RPC authentication affects the performance of the Message Creation entity. When the Data Confidentiality option is used, an operator who belongs to that unit will find that the Message Creation entity opens very slowly. If more than 50 message templates are in use, then it is recommended that you use the low speed mode setting, which allows fewer items to be displayed more quickly. At this setting, only 50 records are retrieved each time that a list of items appears.

Warning The Data Confidentiality mode is CPU-intensive. When selected, it significantly decreases the overall throughput of Alliance Access. Therefore, this mode is not recommended for high-throughput configurations.

5.14.2.12 User Mode

List of User Mode parameters

Component	Parameter	Description
BSS	Housekeeping User Mode	<p>In housekeeping mode either a single operator is allowed to sign on or multiple operators are allowed to sign on.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Single • Multiple <p>Default value: Single.</p> <p>Alliance Access must be restarted for changes to this parameter to take effect.</p>

5.14.2.13 User Space

List of User Space parameters

Component	Parameter	Description
BSS	Root Path for User Space	<p>Location where the User Space directories are to be created. These directories are associated to operators using the Web Platform.</p> <p>Maximum length: 64</p> <ul style="list-style-type: none"> • Windows: C:\Alliance\Access\usrdata\userspace • UNIX or Linux: \$ALLIANCE/usrdata/userspace

5.14.3 Security Parameters Page

Content

The **Security Parameters** page displays the security parameters.

The **Security Parameters** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Security Parameters** page:
 - See "Details" on page 142
 - See "Functions" on page 22
- Details of the available parameters
See "Details" on page 142
- Functions that enable you to manage the parameters
See "Functions" on page 144

Display

Security Parameters

Filtering Criteria

Name	<input type="text"/>	Status	Approved
<input type="button" value="Clear"/>		<input type="button" value="Submit"/> <input type="button" value="Report"/>	

Security Parameters Rows in list: 20, in selection: 1

<input type="checkbox"/>	Component	Class	Name	Value	Future Value	Status
<input type="checkbox"/>	BSA	Signon	Timeout	600		Approved
<input checked="" type="checkbox"/>	BSA	Signoff	Timeout	1800		Approved
<input type="checkbox"/>	BSS	Alarm	Path of Script File			Approved
<input type="checkbox"/>	BSS	Backup integrity	Backup integrity	Full		Approved
<input type="checkbox"/>	BSS	Msg Archive	Archive Method	Normal		Approved

Details

Security Parameters		
Field	Description	Filtering criteria
Component	The component the security parameter belongs to	
Class	The class the security parameter belongs to	
Name	The security parameter name. For filtering, the wildcard characters % and _ enable you to search for a group of names.	✓
Value	The current value of the security parameter	
Future Value	The future value of the security parameter	

Security Parameters		
Field	Description	Filtering criteria
Status	<p>The status of the security parameter</p> <p>For filtering, these are the possible values:</p> <ul style="list-style-type: none"> Approved Wait RSO Approval Wait LSO Approval Unapproved 	✓

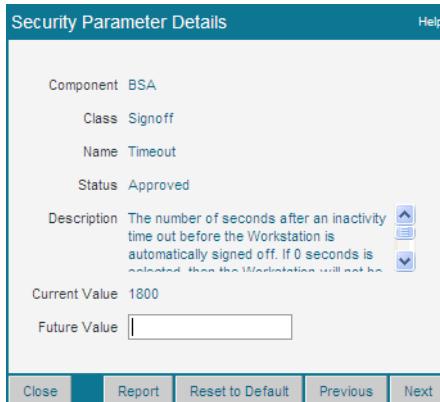
5.14.4 Security Parameters Details Window

Content

The **Security Parameter Details** window contains these elements:

- Details of the security parameters
See "Details" on page 143
- Functions that enable you to manage the security parameters
See "Functions" on page 144

Display



Details

Field	Description
Component	The component the security parameter belongs to
Class	The class the security parameter belongs to
Name	The name of the security parameter

Field	Description
Status	<p>The status of the security parameter</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Approved • Wait RSO Approval • Wait LSO Approval • Unapproved
Description	The description of the security parameter
Current Value	The current value of the security parameter. See the Description to have an indication of the possible values.
Future Value	The future value of the security parameter

5.14.5 Security Parameter Functions

Overview

These functions enable you to manage the security parameters.

Functions

Function	Description	Security Parameters page	Security Parameters Details window
Approve	Enables you to approve the security parameter Procedure: "Approve a Security Parameter" on page 145	✓	✓
Reset to Default	Enables you to reset the security parameter to its default value Procedure: "Reset a Security Parameter to its Default Value" on page 145	x	✓

5.14.6 Modify a Security Parameter

Purpose

This procedure enables you to modify the value of a security parameter.

If the modification has an impact on the layout of some screens, the operators currently logged on have to log off and log on again to see the changes.

Users and permissions

Only security officers can modify security parameters. Both the left security officer and the right security officer must approve the changes for them to become active.

Standard operators cannot modify security parameters.

Procedure

1. From the list of security parameters, click the row of the security parameter that you want to modify.

- The **Security Parameter Details** window opens.
2. Change the value in the **Future Value** field as needed.
 3. Click **Save**.

A status popup message appears.

4. Click **Close**.

The **Security Parameter Details** window closes.

The **Status** field displays the current status which is **Unapproved**.

The new value of the security parameter has to be approved by both security officers. See "Approve a Security Parameter" on page 145 for more details.

5.14.7 Reset a Security Parameter to its Default Value

Purpose

This procedure enables you to reset the value of a security parameter.

If the modification has an impact on the layout of some screens, the operators currently logged on have to log off and log on again to see the changes.

If you reset the value of a security parameter, its status becomes **Unapproved**. Both security officers have to approve the new value.

Users and permissions

Only security officers can reset the values of security parameters. Both the left security officer and the right security officer must approve the changes for them to become active.

Standard operators cannot reset the values of security parameters.

Procedure

1. From the list of security parameters, click the row of the security parameter that you want to reset.

The **Security Parameter Details** window opens.

2. Click **Reset to Default**.

3. Click **Save**.

A status popup message appears.

4. Click **Close**.

The **Security Parameter Details** window closes.

The **Status** field displays the current status which is **Unapproved**.

The new value of the security parameter has to be approved by both security officers. See "Approve a Security Parameter" on page 145 for more details.

5.14.8 Approve a Security Parameter

Purpose

This procedure enables you to approve a security parameter.

If the modification has an impact on the layout of some screens, the operators currently logged on have to log off and log on again to see the changes.

If you reset the value of a security parameter, its status becomes **Unapproved**. Both security officers have to approve the new value.

Users and permissions

Only security officers can approve security parameters. Both the left security officer and the right security officer must approve the changes for them to become active.

Standard operators cannot approve security parameters.

Procedure

1. From the list of security parameters, select the check box of one or several security parameters in the left column.
2. Click **Approve**.

A status popup message appears.

The **Status** field displays the current status which is **Wait RSO Approval** or **Wait LSO Approval**.

The other security officer must now sign on and approve the security parameter or security parameters. When both security officers have approved the changes, the status changes to **Approved** and the changes become active.

5.15 SNMP Heartbeat

Description

Alliance Access can be configured to send a heartbeat SNMP trap to one or more SNMP servers at regular intervals.

The heartbeat will be sent to all SNMP servers specified in the distribution list specified in the **SNMP Heartbeat Dist. List** global system configuration parameter.

If the list does not exist or does not contain any SNMP servers, then the SNMP trap is not sent.

The frequency that the heartbeat is sent is specified in the **SNMP heartbeat interval** global system configuration parameter.

This parameter enables you to activate/deactivate the SNMP heartbeat functionality and, if activated, to define the number of seconds between two SNMP heartbeats. All values less than 120 mean the heartbeat is not active. Changes to this parameter will take effect at the next heartbeat.

In addition to the Alliance Access IP address which is by construction part of the trap, the trap contains the following information:

- Alliance Access instance name
- Alliance Access instance status (always 'started' in lower case)
- SNMP heartbeat interval

The permission required to activate/configure/deactivate the SNMP heartbeat functionality is the System Management application.

Activating the heartbeat

1. Create a Distribution list containing the server(s) to which the heartbeat is to be sent (see "Add a Distribution List").
2. Modify the system parameter **SNMP Heartbeat Dist. List** to refer to the Distribution list created in step 1.

See "System" for more details.

3. Modify the system parameter **SNMP Heartbeat Interval** to the value required (0 to 900 seconds).

All values less than 120 mean the heartbeat is not active.

Changes to this parameter will take effect at the next heartbeat, or at most 900 seconds later if the heartbeat is not active.

Deactivating the heartbeat

- Modify the system parameter **SNMP Heartbeat Interval** to a value less than 120.

The heartbeat will be stopped after the next heartbeat.

6 Event Log

6.1 Distribution Lists

6.1.1 Alarm Distribution

Alarm Distribution list

It is possible to configure an event to trigger an alarm if the event occurs. Alliance Access can broadcast the alarm to a pre-defined list of operators, internal correspondents, or applications. The list of recipients is called an alarm distribution list.

Applications include the SNMP Manager applications (such as, HP OpenView or Tivoli products) which allows external applications to monitor the alarms that occur on Alliance Access.

Alliance Access sends the alarms automatically to any operator who is logged on to Alliance Workstation or the Alliance Monitoring GUI. Unlike Alliance Workstation, which generates a pop-up for an alarm, the Alliance Monitoring GUI on Alliance Web Platform does not generate a pop-up for an alarm. To mimic the Alliance Workstation behaviour, the Alliance Monitoring GUI on Alliance Web Platform informs you of the occurrence of a new alarm by means of the dashboard for events (Exceptions and Alarms).

Distribution of events

It is possible to customise the event distribution for each event. For more information, see "Event Distribution" on page 154.

If an event is marked as an alarm to be distributed, and the assigned distribution list has been defined to distribute the alarm to internal correspondents, then Alliance Access creates an MT 999 containing the alarm.

This allows Alliance Access to route the MT 999 to the inbound queue of the preferred network that is assigned to the internal correspondent. For example, if the network is APPLI, then Alliance Access routes the MT 999 to a predefined exit point.

SNMP Manager applications

The alarms that Alliance Access sends to an SNMP Manager application include the Enterprise ID 18494 (which is the identification given to SWIFT by the Internet Assigned Numbers Authority) and the additional identifying information "2" for Alliance Access.

You can find a description of the alarms that Alliance Access sends to an SNMP manager in the file **saatrap.mib**. Depending on the platform, the file is located in the following directory:

- on AIX: \$ALLIANCE/BSS/data/AIX
- on Linux: \$ALLIANCE/BSS/data/RHEL
- on Solaris: \$ALLIANCE/BSS/data/SunOS
- on Windows: %ALLIANCE%\BSS\data\win32

All information concerning a single event is mapped to a structure that can be interpreted by the SNMP Manager based on the object identifier (or OID).

Note Version 1 of the SNMP protocol does not offer specific protection such as encryption.

The structure of each alarm includes the following information:

Field	OID	Description
Unique identifier of the Alliance Access instance	. 1	Differentiates events coming from more than one Alliance instance
Date	. 2	Date, expressed as dd/mm/yyyy
Time	. 3	Time, expressed as hh:mm:ss
Generated by	. 4	Component (as per the event template)
Event number	. 5	32 bits
Event severity	. 6	Severity: <ul style="list-style-type: none"> • Fatal • Severe • Warning • Info
Event class	. 7	Class (Backup/Restore, Communication, Data, Message, Network, Operator, Process, Restart/Stop, Security, Software, System)
Event name	. 8	Name (as per the event template)
Event description	. 9	The text describing the event

6.1.2 Distribution Lists Page

Content

The **Distribution Lists** page contains these elements:

- Details of the available distribution lists

See "Details" on page 150
- Functions that enable you to manage the distribution lists

See "Functions" on page 150

Display

Distribution Lists				
Distribution Lists				
Rows in list: 13, in selection: 1				
Change View	Add As	Delete	Report	< Previous Next >
<input type="checkbox"/>	Name	Operators	Internal Correspondents	SNMP
<input type="checkbox"/>	Backup/Restore	All	No	No
<input checked="" type="checkbox"/>	Communication	All	No	No
<input type="checkbox"/>	Data	All	No	No
<input type="checkbox"/>	Message	All	No	No
<input type="checkbox"/>	Network	All	No	No

Details

Column	Description
Name	The name of the distribution list, which describes the class of the selected event. The default distribution lists are based on the event classes.
Operators	Indicates whether operators are included in the distribution list, as follows: <ul style="list-style-type: none"> All: All operators are included Specific: Specific operators are included None: No operators are included
Internal Correspondents	Indicates whether internal correspondents are included in the distribution list.
SNMP	Indicates whether SNMP Manager applications are included in the distribution list.

Functions

Function	Description
Add / Add As	Enables you to add a distribution list You can also create a distribution list using the characteristics of an existing distribution list with the Add As button. Procedure: "Add a Distribution List" on page 152
Delete	Enables you to delete a distribution list Procedure: "Delete a Distribution List" on page 153

6.1.3 Distribution List Details Window

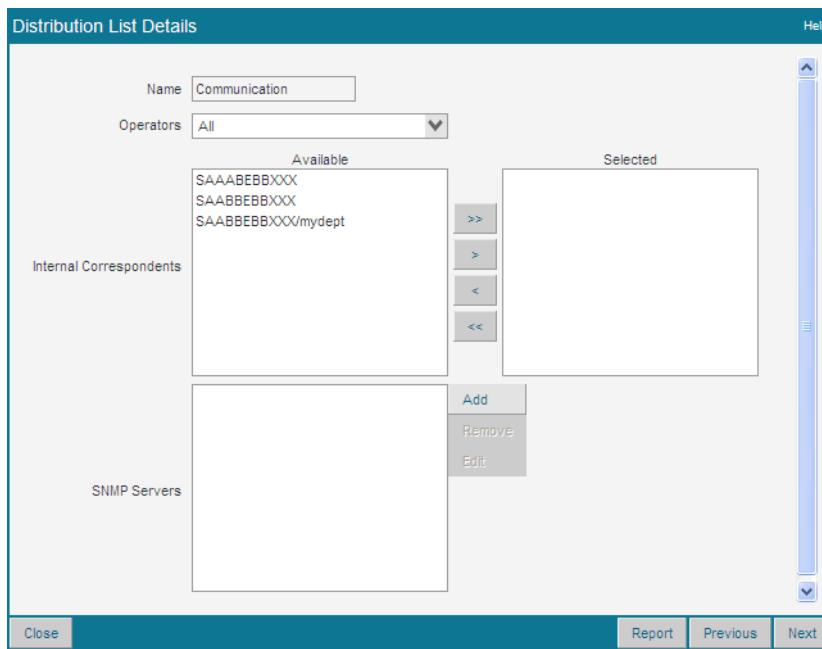
Content

The **Distribution List Details** window contains these elements:

- Details of the available distribution lists

See "Details" on page 151

Display



Details

Field	Description
Name	The name of the distribution list
Operators	<p>Specifies whether operators are included in the distribution list:</p> <ul style="list-style-type: none"> All: All operators are included. The alarms are sent to all operators who are signed on. Specific: The Distribution list includes specific operators. The alarms are sent to the operators who are signed on, and specified as selected in the Operator List in the Distribution List Details window. None: No operators are included
Internal Correspondents	<p>Specifies the internal correspondents that are included in the distribution list. The Available list contains a list of all the internal correspondents. The Selected list contains the internal correspondents that are included in the distribution list.</p>

Field	Description
SNMP Servers	<p>Specifies the identifiers of the SNMP Manager applications that are included in the distribution list.</p> <p>The ID of the SNMP server is either:</p> <ul style="list-style-type: none"> • <IP_address>:<port> <p>The IP address is in the format: nnn.nnn.nnn.nnn, where nnn is a number from 0 through 255.</p> <ul style="list-style-type: none"> • <hostname>:<port> <p>The hostname must start with a letter. Do not use a number as the first character.</p> <p>The port number is a number from 1 through 65535.</p> <p>You can specify up to 16 SNMP servers.</p> <p>Any changes to the ID of the SNMP server are effective immediately.</p>

6.1.4 Add a Distribution List

Purpose

This procedure enables you to add a distribution list.

Users and permissions

To display the list or the details of the existing distribution lists, your operator profile must have this entity:

- **System Management**

To create or modify a distribution list, your operator profile must have these actions:

- **System Management / Add Dist. List**
- **System Management / Mod Dist. List**

Security officers can create distribution lists.

Procedure

1. From the list of distribution lists, click **Add**.

You can also create a distribution list using the characteristics of an existing list. Select the check box of a distribution list and click **Add As**.

The **Distribution List Details** window opens.

2. In the **Name** field, type the name of the distribution list (15 characters maximum).

Once created, you cannot change the name of the distribution list.

3. From the **Operators** drop-down list, select one of the following values:

- **All**: include all operators in the list.

The alarms are sent to all operators who are signed on.

- **Specific**: select specific operators to add to the list.

The alarms are sent to these selected operators if they are signed on.

- None: no operators are included in the list.
4. If required, select the internal correspondents from the **Internal Correspondents/ Available** list, to include them in the distribution list.
 5. If required, specify the SNMP Manager applications for the distribution list, as follows:
 - a. Click **Add**.
The **Add SNMP Server** window appears.
 - b. In **Host Address** field, enter one of following values:
 - IP address of the SNMP server
 - host name of the SNMP server. The maximum length of the host name is 255 characters.

Warning The first letter of the host name must not be a number.
 - c. In the **Port Number** field, enter the port number on which the SNMP Manager listens for events. Enter a value between 1 and 65536.
 - d. In the **Community Name** field, optionally enter a community name, which is a password that can be shared by multiple SNMP agents and one or more SNMP managers. An SNMP agent only accepts request from SNMP managers that are on the agent's list of acceptable community names. The name is case-sensitive and is a text string of no more than 64 characters. All US ASCII characters are accepted, except for ":" , " , and "\".
 - e. Click **OK**.
The identifier of the SNMP server is the <hostname:port> or the <IP_address:port> of the SNMP server.
 6. Click **Save**.
 7. Click **Close**.

6.1.5 Delete a Distribution List

Purpose

This procedure enables you to delete a distribution list.

Users and permissions

To display the list or the details of the existing distribution lists, your operator profile must have this entity:

- **System Management**

To delete a distribution list, your operator profile must have this action:

- **System Management / Rem Dist. List**

Security officers can delete distribution lists.

Procedure

1. From the list of distribution lists, select the check box of one or several distribution lists in the left column.
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
A status popup message appears.
The **Delete Confirmation** window closes.

6.2 Event Distribution

6.2.1 Event Distribution

Overview

Events are reports about actions in Alliance Access. Each event contains detailed information about the action. Events are grouped into event types, according to the Alliance Access function that generated the event.

Alarms are events which have been promoted so that they have an alarm status. Alarms are classified as either **For Action** or **For Information**.

Once an event has been set as an alarm, it is always recorded in the event log and details of the alarm can be distributed to internal correspondents or SNMP Manager applications (such as HP OpenView or Tivoli products) so that external applications can monitor events.

6.2.2 Event Distribution Page

Content

The **Event Distribution** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Event Distribution** page:
 - See "Details" on page 155
 - See "Functions" on page 22
- Details of the available events
 - See "Details" on page 155
- Functions that enable you to manage the events
 - See "Functions" on page 158

Display

Event Distribution

Filtering Criteria

Name	Severity	Alarm
Number	Distribution	
<input type="button" value="Clear"/> <input type="button" value="Submit"/> <input type="button" value="Report"/>		

Event Distribution

Rows in list: 20 , in selection: 1

	Name	Component	Severity	Class	Security	Config. Mngt	Number	Distribution	Alarm
<input type="checkbox"/>	Successful signon	BSA	INFO	Operator	Yes	No	3000	Fixed Journalise	None
<input type="checkbox"/>	Signoff	BSA	INFO	Operator	Yes	No	3001	Fixed Journalise	None
<input type="checkbox"/>	Inactivity Time out	BSA	INFO	Operator	No	No	3002	Journalise	None
<input checked="" type="checkbox"/>	Invalid signon attempt	BSA	WARNING	Operator	Yes	No	3003	Journalise	For Information
<input type="checkbox"/>	Change password	BSA	INFO	Operator	Yes	No	3004	Fixed Journalise	None

Details

Event Distribution		Filtering criteria
Field	Description	Filtering criteria
Name	The name of the event. For filtering, the wildcard characters % and _ enable you to search for a group of names.	✓
Component	The component in Alliance Access for which the event occurred	
Severity	The level of severity of the event These are the possible values: <ul style="list-style-type: none"> • FATAL • SEVERE • WARNING • INFO 	✓
Class	The functional domain to which the event belongs	
Security	Specifies whether the event is related to security or not. This value cannot be modified. In the event log, it is possible to search on events based on this criterion.	
Config. Mngt	Specifies whether the event is related to configuration management or not. In the event log, it is possible to search on events based on this criterion.	
Number	A unique number that identifies the event in Alliance Access	✓

Event Distribution		
Field	Description	Filtering criteria
Distribution	<p>Specifies whether the event is logged</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Ignore: The event is not logged in the event log • Journalise: The event is logged • Fixed Journalise: Events set as Fixed Journalise are always logged. If an event has Fixed Journalise as its default setting, then it cannot be modified. <p>The default distribution for each event is set during the installation.</p>	✓
Alarm	<p>Specifies whether the event has the status of an alarm or not</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • None: The event is not considered as an alarm • For Information: The event has the status of an alarm for information • For Action: The event has the status of an alarm for action 	✓

6.2.3 Event Distribution Details Window

Content

The **Event Distribution Details** window contains these elements:

- Details of the available events
See "Details" on page 157
- Functions that enable you to manage the events
See "Functions" on page 158

Display

Event Distribution Details Help

Name: Template Rejected
Text: Template %s was rejected : %s

Component: MPA
Severity: INFO
Class: Message
Number: 23020

Distribution:

Security:

Configuration Management:

Alarm:

Distribution List:

Details

Field	Description
Name	Indicates the name of the event
Text	Indicates the detailed description of the system or operator action that generated the event
Component	Indicates the component in Alliance Access for which the event occurred
Severity	<p>Indicates the level of severity of the event</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • FATAL • SEVERE • WARNING • INFO
Class	The functional domain to which the event belongs
Number	A unique number that identifies the event in Alliance Access
Distribution	<p>Specifies whether the event is logged</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Ignore: The event is not logged in the event log • Journalise: The event is logged • Fixed Journalise: Events set as Fixed Journalise are always logged. If an event has Fixed Journalise as its default setting, then it cannot be modified.

Field	Description
Security	Specifies whether the event is related to security or not. This value cannot be modified. In the event log, it is possible to search on events based on this criterion.
Configuration Management	Specifies whether the event is related to configuration management or not. In the event log, it is possible to search on events based on this criterion.
Alarm	Specifies whether the event has the status of an alarm or not These are the possible values: <ul style="list-style-type: none"> • None: The event is not considered as an alarm • For Information: The event has the status of an alarm for information • For Action: The event has the status of an alarm for action If For Information or For Action is selected, then the Distribution List drop-down list is displayed.

6.2.4 Event Distribution Functions

Overview

This function enables you to manage the event distribution.

Functions

Function	Description
Reset Distribution	Enables you to reset the event distribution to the default values Procedure: "Reset the Event Distribution" on page 159

6.2.5 Modify the Distribution of an Event

Purpose

This procedure enables you to modify the distribution of an event.

You can do the following:

- Give an alarm status to an event. This means that the event will be automatically sent to the event log and an alarm will be broadcast.
- Determine whether the event should be logged in the event log.

Modifying attributes of an event affects all future instances of the selected event, but not those already logged in the event log.

Users and permissions

To display the list or the details of events, your operator profile must have this entity:

- **System Management**

To modify the distribution of an event, your operator profile must have this action:

- **System Management / Mod Event Dist.**

Security officers can modify the event distribution.

Procedure

1. From the list of events, click the row of the event that you want to modify.
- The **Event Distribution Details** window opens.
2. In the **Distribution** drop-down list, select one of the following values:
 - **Journalise:** To log the event in the event log
 - **Ignore:** If this value is selected, then the event is not logged.

Note Events set as **Fixed Journalise** are always logged.

3. If the event is related to configuration management, then you can mark the event by selecting the **Configuration Management** check box.
 4. In the **Alarm** drop-down list, select one of the following values:
 - **None**
 - **For Information**
 - **For Action**
 5. If you selected **For Information** or **For Action**, then you can select a distribution list in the **Distribution List** drop-down list.
 6. Click **Save**.
- A status popup message appears.
7. Click **Close**.
- The **Event Distribution Details** window closes.

6.2.6 Reset the Event Distribution

Purpose

This procedure enables you to reset the attributes for event distribution back to their default settings.

At installation, each event has a default distribution value.

The values are:

- **Ignore:** The event is not logged in the event log
- **Journalise:** The event is logged
- **Fixed Journalise:** Events set as **Fixed Journalise** are always logged. If an event has **Fixed Journalise** as its default setting, then it cannot be modified.

Events already logged in the event log are not affected by this command.

Users and permissions

To display the list or the details of events, your operator profile must have this entity:

- **System Management**

To reset the default event distribution, your operator profile must have this action:

- **System Management / Reset Event Dist.**

Security officers can reset the event distribution.

Procedure

1. From the list of events, select the check box of one or several events in the left column.

2. Click **Reset Distribution**.

The **Reset Confirmation** window opens.

3. Click **OK**.

The **Reset Confirmation** window closes.

A status popup message appears.

6.3 Event Log Archives

6.3.1 Event Log Archives

Overview

Archiving is used to freeze events from the event log. You must archive regularly as you can only back up events to an external storage after they have been archived. You can either archive events manually, or you can schedule archiving to occur automatically.

When you archive events manually, the events are archived immediately.

6.3.2 Event Log Archives Page: Configuration Tab

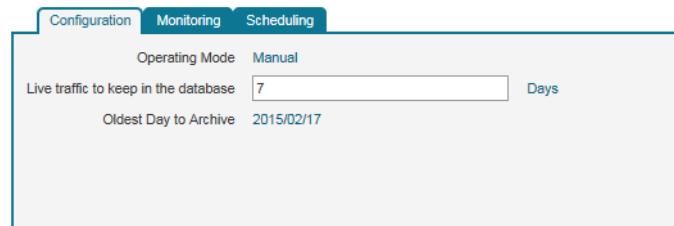
Content

The **Configuration** tab contains these elements:

- Details of the current archiving configuration
See "Details" on page 161
- Functions that enable you to manage the archiving
See "Functions" on page 162

Display

Event Log Archives



Details

Field	Description
Operating Mode	These are the possible values: <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
Live traffic to keep in the database	The number of days for which to keep events available in the database. All other events are archived.
Oldest Day to Archive	The date of the oldest event to be archived

6.3.3 Event Log Archives Page: Monitoring Tab

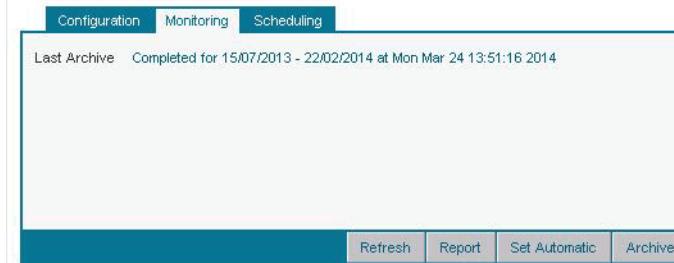
Content

The **Monitoring** tab contains these elements:

- Details of the last event archive
See "Details" on page 162
- Functions that enable you to manage the archiving
See "Functions" on page 162

Display

Event Log Archives



Details

Field	Description
Last Archive	Date and time when the last event archive was created

6.3.4 Scheduled Action Details Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Tabs with Scheduled Actions Lists" on page 28.

6.3.5 Event Log Archive Functions

Overview

These functions enable you to manage the event log archives.

Functions

Function	Description
Set Automatic / Set Manual	Enables you to set the operation mode to Automatic or to Manual Procedure: "Change the Operation Mode" on page 163
Archive	Enables you to archive the events manually Procedure: "Configure and Launch a Manual Archiving of Events" on page 162

6.3.6 Configure and Launch a Manual Archiving of Events

Purpose

This procedure enables you to archive events manually.

Since events are archived for a full day, it is not possible to archive the events from the current day.

If there are any untreated alarms for the events that you are archiving, then these alarms are also archived and can no longer be treated.

You can run only one event archive at a time. An error message appears if you try to start an archive while another archive is still running.

Users and permissions

To display the archiving configuration details and archive events manually, your operator profile must have this action:

- **Event Journal / Archive**

Procedure

1. From the **Configuration** tab, in the **Live traffic to keep in the database** field type the number of days for which you want to keep events available in the database.

All other events are archived. For example, if you type 2, Alliance Access keeps today's events and the events from the previous day in the live database, and archives all events with earlier dates.

2. Click **Save**.

In the **Oldest Day to Archive** field, the date of the oldest event to be archived appears.

3. Click **Archive**.

A status popup message appears.

If archiving is successful, then an archive is created in the database. You can check the status of the last archive from the **Monitoring** tab.

6.3.7 Change the Operation Mode

Purpose

This procedure enables you to change the operation mode.

Users and permissions

To change the operation mode, your operator profile must have this action:

- **Event Journal / Archive**

The **Modify operating mode** permission must be set to Yes.

Procedure

- From the **Configuration** tab, the **Monitoring** tab, or the **Scheduling** tab, given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

6.3.8 Monitor the Archiving of Events

Purpose

This procedure enables you to monitor the status of the last archiving process.

Users and permissions

To display the archiving configuration details and the status of the last event archive, your operator profile must have this action:

- **Event Journal / Archive**

Procedure

1. Click the **Monitoring** tab.
2. You can click  to refresh the list.

6.4 Event Archive Backups

6.4.1 Event Archive Backups

Overview

Once archived, events can be backed up to an external storage. You cannot back up archives to a network drive.

You can launch the backup process manually or create a schedule.

A backup is the only way to free the space that the archives use. If you do not have to use the archives on a daily basis, then you are advised to make regular backups of the archives and remove the original archives. This action makes disk space available and enables data to be recovered efficiently in the event of a major problem, such as, disk failure.

You can also restore the contents of archive backup files into the Alliance Access database. The restore process can only be launched manually.

Note You cannot create backups of archives that were created using Alliance Access 6.0 or earlier.

6.4.2 Event Archive Backups Page: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details of the backup configuration
See "Details" on page 165
- Functions that enable you to manage the backups
See "Functions" on page 166

Display

Event Archive Backups

Configuration Monitoring Scheduling

Operating Mode: Manual

Backup Directory: C:\Alliance\Access\usrdata\backup\leja

Live or archived traffic to keep in the database: 7 Days

Details

Field	Description
Operating Mode	These are the possible values: <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
Backup Directory	The location where Alliance Access stores archive backup files. The default location is: <software dir>\usrdata\backup\leja where <software dir> is the directory in which Alliance Access is installed. Note: On Windows only: If you have a hosted database configuration, you can access remote file directories by specifying UNC paths. Do not use a mapped drive
Live or archived traffic to keep in the database	The minimum number of days between the event creation date and the date on which the archived event is backed up and removed or the date on which the archived and backed-up event is removed. Specify an integer, which represents the number of days.

6.4.3 Event Archive Backups Page: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details of the last event archive backup or restore
See "Details" on page 166
- Functions that enable you to manage the backups
See "Functions" on page 166

Display

Event Archive Backups

Configuration Monitoring Scheduling

Last Archives Backup Status: Completed for JRAR_20130715 at Mon Mar 24 14:00:36 2014

Last Archives Restore Status: Completed for JRAR_20130715 at Mon Mar 24 14:01:08 2014

Refresh Report Set Automatic Restore Backup

Details

Field	Description
Last Archives Backup Status	The status of the last event archive backup and date and time when it was carried out
Last Restore Status	The status of the last restore process and date and time when it was carried out

6.4.4 Event Archive Backups Page: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Scheduled Action Details Window" on page 29.

6.4.5 Event Archive Backup Functions

Overview

These functions enable you to manage the event archive backups.

Functions

Function	Description
Set Automatic / Set Manual	Enables you to set the operation mode to <code>Automatic</code> or to <code>Manual</code> Procedure: "Change the Operation Mode" on page 168
Restore	Enables you to restore an archive backup Procedure: "Restore an Event Archive Backup" on page 168
Backup	Enables you to launch an archive backup manually Procedure: "Configure and Launch a Manual Event Archive Backup" on page 167

6.4.6 Change the Default Directory for Event Archive Backups

Purpose

This procedure enables you to change the location where Alliance Access stores archive backup files.

The default location is: `<software dir>\usrdata\backup\ejab` where `<software dir>` is the directory in which Alliance Access is installed.

If you are using a hosted database, the directory cannot be changed manually. The path is deduced from the value of a system parameter. After installation, the parameter is not initialised. You have to change its value before being able to perform a backup.

Name of event archive backups

Alliance Access creates a directory for every archive backup.

The following naming convention is used: **<JRAR>_<ArchiveName>**

Where:

- **<JRAR>** represents the type of item being archived (here event log archives)
- **<ArchiveName>** represents the name of the archive that Alliance Access backed up

Example: JRAR_20101215

Users and permissions

To display the configuration details and the status of the last event archive backup, your operator profile must have this entity:

- **System Management**

To change the default directory, your operator profile must have this action:

- **System Management / Backup**

Security officers can change the default directory.

Procedure

1. From the **Configuration** tab, modify the path in the **Backup Directory** field.
2. Click **Save**.

A status popup message appears.

6.4.7 Configure and Launch a Manual Event Archive Backup

Purpose

This procedure enables you to back up event archives manually.

Users and permissions

To display the configuration details and the status of the last event archive backup, your operator profile must have this entity:

- **System Management**

To launch manual backups, your operator profile must have this action:

- **System Management / Backup**

Security officers can launch manual backups.

Procedure

1. From the **Configuration** tab, click **Backup**.
The **Backup Archives** window opens.
2. In the **Mode** drop-down list, select one of the following options:
 - **Backup**: To create a backup of the archive, without deleting the archive
 - **Backup and Remove**: To create a backup of the archive, and then delete the original archive after the backup is complete

Note The Remove option enables you to delete an archive that has the status **DONE**, without creating a backup for the archive.

3. Select the **Overwrite Existing Archives Backup** check box if you want to replace the oldest backup contained in the directory.
 4. In the **Archives (Backup Status)/Available** list, select the archives to back up.
-

Note An archive must have the status **READY** (Alliance Access has archived data successfully, and the archive is ready to be backed up) or **DONE** (Alliance Access has created a backup of the archive successfully) before you can create a backup for it.

5. Click **Backup**.

A status popup message appears.

The **Backup Archives** window closes.

The information message informs you about the status of the backup request. If the request is accepted, the backup is launched as a background task. You have to monitor the status of the backup from the **Monitoring** tab.

6.4.8 Change the Operation Mode

Purpose

This procedure enables you to change the operation mode.

Users and permissions

To display the configuration details and the status of the last event archive backup, your operator profile must have this entity:

- **System Management**

To change the operation mode, your operator profile must have this action:

- **System Management / Backup**

The **Modify operating mode** permission must be set to **Yes**.

Procedure

- From the **Configuration** tab, the **Monitoring** tab, or the **Scheduling** tab, given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

6.4.9 Restore an Event Archive Backup

Purpose

This procedure enables you to restore event archives manually. The restore procedure imports the contents of an archive backup file into the Alliance Access database. The backup archive file remains in the backup directory.

Note	You can restore and view an archive backup from a previous release of Alliance Access even if the current release of 7.1.10 runs on an operating system that is different from the operating system with which the archive backup was made.
-------------	---

Users and permissions

To display the configuration details and the status of the last event archive backup, your operator profile must have this entity:

- **System Management**

To restore an event archive backup, your operator profile must have this action:

- **System Management / Restore**

Security officers can restore backups.

Procedure

1. From the **Configuration** tab, click **Restore**.

The **Restore Archives** window opens.

2. In the **Backup Directory** field, verify the backup path.

Click **Change Location** and modify the path in the **Change Location** window if needed.

3. Select the **Overwrite Existing Archives** check box, if you want to replace the last archive.

4. In the **Archives to be Restored/Available** list, select the backups to restore.

5. Click **Restore**.

The **Restore Archives** window closes.

A status popup message appears.

If an archive already exists in the database, an error message appears.

The information message informs you about the status of the restore request. If the request is accepted, the restore process is launched as a background task. You have to monitor the status of the last restore from the **Monitoring** tab.

6.4.10 Monitor an Event Archive Backup

Purpose

This procedure enables you to monitor the status of the last archive backup or the last restore process.

Users and permissions

To display the configuration details and the status of the last event archive backup, your operator profile must have this action:

- **System Management / Backup**

Security officers can monitor backups.

Procedure

1. Click the **Monitoring** tab.
2. You can click **Refresh** to refresh the list.

6.5 Event Log

6.5.1 Event Log

Overview

All successful and unsuccessful actions performed by operators, and by the Alliance Access system, are identified and recorded as events in the event log. This data provides a detailed audit trail of all actions performed in Alliance Access.

Each record in the event log includes details of:

- the date and time that the event occurred
- the identity of the operator (or system) that caused the event
- the class and severity of the event. Events relating to the same area in Alliance Access are grouped in a class - for example, all communication-related events belong to the Communication event class. The severity indicates the importance of an event. For example, it is a more severe event if a message fails authentication than if an operator signs on.
- a text description of the event

You use the event log for audit and investigation purposes by searching the events stored based on a specific criterion. You can then display or print the search results.

6.5.2 Alarm Scripts

Description

An operator with permission to change security parameters can configure Alliance Access to collect all alarms and copy them to a file, from which they can be processed further. An alarm script is used to collect the alarms and store them in a file, and Alliance Access runs the script whenever an alarm occurs.

Note	An incorrect script may cause major problems on your system as processing an unusual number of alarms may cause a timing problem, and consequently, the system to hang. Instead of sending all alarms to a file, you may consider using event distribution to send specific alarms to a file. You can then use an external program to process this file.
-------------	--

Alarm script

The following example script shows where alarms are copied to a file **alarm.out** in the **tmp** directory:

- On Windows:

```
@echo off
echo %* >> c:\temp\alarm.out
```

Note	@echo off is mandatory as the first line to get all events in the alarm script.
-------------	---

- On UNIX or Linux:

```
#! /bin/ksh -p
echo $@ >> /tmp/alarm.out
```

Script and directory constraints

The **Path of Script File** security parameter specifies the full pathname of the directory that contains the script to collect alarms. For more information about this parameter, see "Alarm" on page 129.

The directory must be owned by the Alliance Administrator.

On UNIX or Linux, the script must be compliant with the requirements of the UNIX exec system call, regarding the execution of an interpreter file.

6.5.3 Event Log Page: General Tab

Content

The **General** tab contains these elements:

- Search criteria and filtering functionality that enable you to filter the list entities on the **General** tab
 - See "Search criteria" on page 172
 - See "Functions" on page 22
- Details of the events
 - See "Details" on page 175
- Functions that enable you to manage the events
 - See "Functions" on page 179

Display

Event Log

Search Criteria

General Specific Location

From Date: 13/08/2010 From Time: 00:00:00
To Date: 13/08/2010 To Time: 23:59:59

Severity: Available FATAL, SEVERE, WARNING
Selected: INFO

Class: Available Communication, Data, Message, Network, Operator, Process, Restart/Stop
Selected: Backup/Restore

Search Report

Event Log Rows in list: 10, in selection: 1

Change View Treat Alarm Report Previous Next

Date & Time	Severity	Class	Application	Name	Operator	Description	Security	Config Mgmt	Alarm	Location
13/08/2010 11:11:20	INFO	Backup/Restore	Alliance System	Backup/Restore	System	Backup of journal archive JRAR_201...	No	No	None	Live Days
13/08/2010 11:11:08	INFO	Backup/Restore	Alliance System	Backup/Restore	System	Restore of journal archive JRAR_201...	No	No	None	Live Days
13/08/2010 11:10:24	INFO	Backup/Restore	Alliance System	Backup/Restore	System	Manual Backup of journal archive(s) ...	No	No	None	Live Days
13/08/2010 11:09:57	INFO	Backup/Restore	Alliance System	Backup/Restore	System	Manual Backup of journal archive(s) ...	No	No	None	Live Days

Search criteria

Criterion	Description
From Date / To Date	The date range when the event occurred
From Time / To Time	The time range when the event occurred
Severity	<p>The degree of importance of the event</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • FATAL • INFO • SEVERE • WARNING

Criterion	Description
Class	<p>The class of the event</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Backup/Restore • Communication • Data • Message • Network • Operator • Process • Restart/Stop • Security • Software • System

6.5.4 Event Log Page: Specific Tab

Content

The **Specific** tab contains these elements:

- Search criteria and filtering functionality that enable you to filter the list entities on the **Specific** tab
 - See "Search criteria" on page 174
 - See "Functions" on page 22
- Details of the events
 - See "Details" on page 175
- Functions that enable you to manage the events
 - See "Functions" on page 179

Display

The screenshot shows the 'Event Log' search interface. At the top, there is a 'Search Criteria' section with tabs for 'General', 'Specific', and 'Location'. The 'Location' tab is selected. It contains fields for 'Operator' (a dropdown menu), 'Search Text' (a text input field), 'Event Type' (a dropdown menu set to 'Alarm Events'), and 'Alarm Type' (a dropdown menu set to 'All Alarms'). Below these are two lists: 'Available' (containing 'Application') and 'Selected' (containing 'ADK', 'Access Control', 'Advanced Load BIC', 'Alliance Control', 'Alliance System', 'Aplic. Interface', and 'Archive Server'). Below the lists are buttons for 'Clear', 'Search', and 'Report'. The main area is titled 'Event Log' and shows a table of events. The table has columns: Date & Time, Severity, Class, Application, Name, Operator, Description, Security, Config Mgmt, Alarm, and Location. The table contains 599 rows, with the last row visible showing a timestamp of 2014/02/19 00:00:32, Severity of WARNING, Class of Data, Application of Calendar, Name of No current year for System, Operator of System, Description of No current year has been defined for calendar DEFAULT. Define!, Security of Yes, Config Mgmt of No, Alarm of Not Treated, and Location of Archives.

Search criteria

Criterion	Description
Operator	To search on an operator's login. Events can also be generated by the system.
Search Text	To search for specific words in the description of events
Event Type	<p>To search on the types of events</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • All Events • Security Events • Alarm Events • Security Alarm Events (both security events and alarm events) • Config Mgmt Events <p>If Alarm Events or Security Alarm Events is selected, then the Alarm Type drop-down list is displayed.</p>
Alarm Type	<p>To search on the status of the events marked as alarms</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • All Alarms • Not Treated Alarms • Treated Alarms
Application	To search on the application that generated the event

6.5.5 Event Log Page: Location Tab

Content

The **Location** tab contains these elements:

- Search criteria and filtering functionality that enable you to filter the list entities on the **Location** tab

- See "Search criteria" on page 175
- See "Functions" on page 22
- Details of the events

See "Details" on page 175
- Functions that enable you to manage the events

See "Functions" on page 179

Display

Search criteria

Criterion	Description
Location	<p>These are the possible values:</p> <ul style="list-style-type: none"> • Live Days: to search the events currently logged • Archives: to search the event log archives <p>If Archives is selected, then the Archives list is displayed.</p>
Archives	The list of event log archives on which you can do a search

6.5.6 Event Log Details

Overview

The event log details are described below.

Details

Column	Description
Date & Time	The date and time when the event occurred

Column	Description
Severity	<p>The degree of importance of the event</p> <p>These are the possible values:</p> <ul style="list-style-type: none">• FATAL: reserved for the unlikely case of a fatal system error, serious enough to cause Alliance to stop working.• INFO: the event is generated to confirm that an action has taken place. Info events are for information only and do not require operator intervention.• SEVERE: the event is considered serious and requires immediate investigation. For example, a message has failed authentication or a session was unexpectedly aborted. Such events definitely require operator intervention.• WARNING: the event is a warning that a process has returned an error code. For example, a checksum or format error was found. Warnings may require investigation by the operator before trying the same function again.

Column	Description
Class	<p>The class of the event</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Backup/Restore: Events triggered by the backup and restore commands. The class also includes events related to archiving. • Communication: Events related to the transfer of messages (not the message itself) and associated transmission errors, that is, start and stop of sessions, Login and Select, Login Acks, and Nacks, Select Acks and Nacks, sequence number errors, protocol errors, and so on. • Data: Any action performed on an Alliance object such as add, modify, or delete. The objects are: routing rules, authentication keys, operator definitions, profiles, configuration and security parameters, message partner profiles, exit point profiles, APC/FIN related definitions such as for example logical terminals, delivery subsets, and lines. • Message: Messages are logged in the event log when they are sent to or received from APC/FIN, message partners or when they are manually completed. The class also includes Acks and Nacks of FIN messages (except Quit). • Network: Network-related events, including any modifications to logical terminals and SWIFT communication connections. • Operator: The class includes access control activities such as signon (normal and after inactivity time-out), signoff and password modification, and the creation or modification of operator profiles and definitions. <p>Other events are related to the use of commands such as:</p> <ul style="list-style-type: none"> – Activate routing schema – Enable/disable message partner profiles – Start/stop Alliance – Hold/release queues • Process: Successful start and termination of internal processes. • Restart/Stop: Automated (scheduled) stops and restarts of the system. • Security: All security-related events, such as Login and Select authentication failures. • Software: Abnormal software behaviour and internal failures. • System: Monitoring activities performed by the system and not covered by any of the other classes, that is for example, queue overflow conditions, system recoveries, or disk space availability.
Application	The application that generated the event
Name	The name of the event
Operator	The operator's login. Events can also be generated by the system.
Description	The description of the event

Column	Description
Security	Determines whether the event is considered to be significant from a security point of view Security events are usually related to the security of access to Alliance software, such as when an operator is disabled after too many failed attempts to sign on; or to abnormal events, such as local authentication failures. Security events are pre-defined in Alliance and their status cannot be changed.
Config Mgmt	Specifies whether the event is related to configuration management or not. Events defined as configuration management events can be used to identify database entity changes.
Alarm	Defines whether the event is treated as an alarm. If the event has been marked as an alarm, the status of the event is either Treated or Not treated.
Location	These are the possible values: <ul style="list-style-type: none">• Live Days: to search the events currently logged• Archives: to search the event log archives

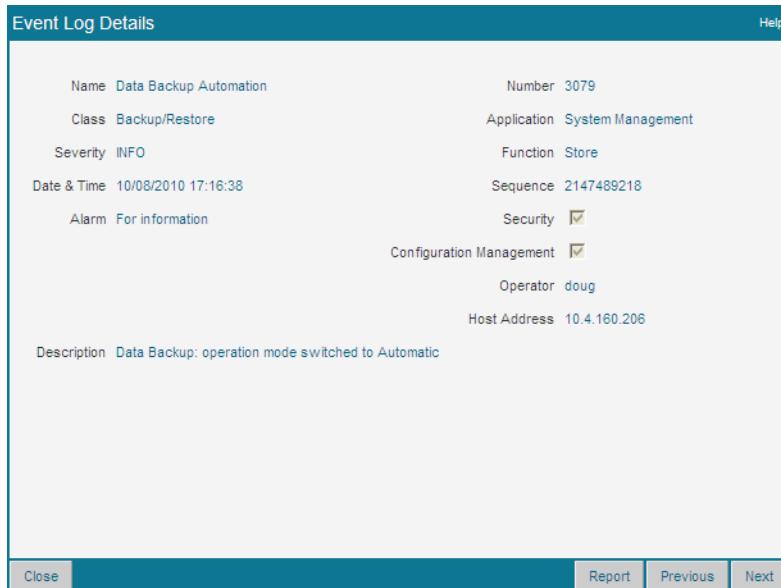
6.5.7 Event Log Details Window

Content

The **Event Log Details** window contains these elements:

- Details of the event selected
See "Details" on page 179
- Functions that enable you to manage the events
See "Functions" on page 179

Display



Details

Column	Description
Name	The name of the event
Class	The class of the event
Severity	The degree of importance of the event
Date & Time	The date and time when the event occurred
Alarm	Defines whether the event is treated as an alarm. If the event has been marked as an alarm, the status of the event is either Treated or Not treated.
Number	The unique identification number of the event
Application	The application that generated the event
Function	The function that generated the event
Sequence	The sequential number assigned to the event for auditing purposes
Security	Determines whether the event is considered to be significant from a security point of view
Configuration Management	Specifies whether the event is related to configuration management or not
Operator	The operator's login. Events can also be generated by the system.
Host Address	The host that generated the event
Description	The description of the event

6.5.8 Event Log Functions

Overview

This function enables you to manage the event log.

Functions

Function	Description
Treat Alarm	Enables you to treat the events marked as alarms Procedure: "Treat Alarms" on page 179

6.5.9 Treat Alarms

Purpose

If an operator who receives an alarm for action fails to treat the alarm within a specified period of time, then the alarm is recorded in the event log and is flagged as Not Treated.

This procedure enables you to treat alarms from the event log.

Users and permissions

To display the list or the details of events, filter the list or treat alarms, your operator profile must have this entity:

- **Event Journal**

Security officers can treat alarms.

Procedure

1. From the event log list, select the check boxes for one or several events in the left column.
2. Click **Treat Alarm**.

The **Treat Alarm Confirmation** window opens.

3. Click **OK**.

The **Treat Alarm Confirmation** window closes.

A status popup message appears.

The status of the event or events is changed to Treated.

7 Messages

7.1 Syntax Versions

7.1.1 Message Syntax Tables

Introduction

Correspondents on the SWIFT network can understand each other's messages because the syntax used in the messages is standardised.

A message syntax table is assigned to each logical terminal and the message syntax table describes the syntax that is used in all the message types sent through the SWIFT network. When a logical terminal sends or receives a message, it checks the syntax of the message automatically. The logical terminal compares the contents of the message with the syntax defined by the message syntax table and informs you of any inconsistencies.

Message syntax table

The message syntax table contains details of the following:

- message types that can be sent and received
- length and type of character strings in fields
- character sets
- field expansion

Every message within Alliance Access has a unique message identifier (UMID) that is created from information in its header and its text. The unique message identifiers in Alliance Access are built from either the transaction reference number or the message user reference of the related message. When a message syntax table is installed, an operator can select which to use to build the unique message identifier.

New versions of a message syntax table

SWIFT releases a new message syntax table version every year, which must be installed and assigned to the logical terminals on Alliance Access.

7.1.2 Syntax Versions Page

Content

The **Syntax Versions** page contains these elements:

- Details of the available message syntax tables

See "Details" on page 182

Display

Syntax Versions

Message Syntax Versions

Rows in list: 2, in selection: 1

	Syntax Table	Message Identifier	Default Live	Default T&T
<input type="checkbox"/>	0905	TRN	No	No
<input checked="" type="checkbox"/>	1005	TRN	Yes	Yes

Details

Column	Description
Syntax Table	The syntax version of the message syntax table
Message Identifier	<p>The element from which the unique message identifier is built</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • MUR (message user reference) • TRN (transaction reference number)
Default Live	Indicates whether the message table is set as default for the validation of Live messages
Default T&T	Indicates whether the message table is set as default for the validation of Test & Training messages

7.1.3 Syntax Version Details Window

Content

The **Syntax Version Details** window contains these elements:

- Details of the message syntax tables

See "Details" on page 183

Display

Syntax Version Details

Syntax Version: 1005

Message Types

Rows in list: 229

MT	Description
101	Request for Transfer
102	Mult Customer Credit Transfer
102.STP	Mult Customer Credit Transfer
103	Single Customer Credit Transfer
103.REMIT	Single Customer Credit Transfer
103.STP	Single Customer Credit Transfer

Close Report Previous Next

Details

Field	Description
Syntax Version	The syntax version of the message syntax table
Message Types	Message types defined in the message syntax table

7.1.4 Install a New Message Syntax Table

Purpose

This procedure enables you to install a new message syntax table.

Users and permissions

To display the list or the details of message syntax tables, your operator profile must have this action:

- **SWIFT Support**

To install a new message syntax table, your operator profile must have this action:

- **SWIFT Support / Install Syntax**

Prerequisites

To install the message syntax table, the message syntax table data must have already been downloaded into the system. The message syntax table valid at the time of the software release is automatically loaded during the installation of Alliance Access. Any new release of message syntax tables contains clear instructions in the related release letter.

You must restart the Alliance Access servers in housekeeping mode to be able to install a new message syntax table.

Procedure

1. From the list of message syntax versions, click **Install**.
The **Install Syntax Version** window opens.
2. From the **Syntax Version** drop-down list, select the message syntax table version.
3. From the **Message Identifier (UMID)** drop-down list, select the element from which the unique message identifier will be built:
 - MUR (message user reference)
 - TRN (transaction reference number)

Every message within Alliance Access has a unique message identifier that is created from information in its header and its text.

4. Click **Install**.
5. Click **Close**.

The **Install Syntax Version** window closes.

The new message syntax table is installed.

7.1.5 Set a Default Message Syntax Table for Live and Test & Training Operations

Purpose

This procedure enables you to set a message syntax table as default.

When you have multiple message syntax tables installed, you can set which are used by default for the validation of Live or Test & Training input messages with sender logical terminal code X. See "Load Balancing FIN Messages over Logical Terminals" on page 346 for more details.

Users and permissions

To display the list or the details of message syntax tables, your operator profile must have this action:

- **SWIFT Support**

To set a message syntax table as default, your operator profile must have these actions:

- **SWIFT Support / Set Default Live**
- **SWIFT Support / Set Default T&T**

Prerequisites

You must restart the Alliance Access servers in housekeeping mode to be able to set a message syntax table as default.

Procedure

1. From the list of message syntax versions, select the check box for the message syntax table that you want to set as default in the left column.
2. Click **Set Default Live** or **Set Default T & T** as needed.

The message syntax table is set as default.

7.2 Message Standards

Overview

SWIFT provides standards for FIN message deployment packages and MX message services (Standards XML) through its message standards deployment packages.

As of Alliance Access 7.1.10, you can install, manage, and use deployment packages from MyStandards.

When you download the message standards, you are provided with a digest, which you must use this when installing the Message Standards to ensure that you are installing valid standards.

7.2.1 Message Standards Page

Content

The **Message Standards** page contains these elements:

- Details of the message syntax versions defined for the current Alliance Access instance

See "Details" on page 185

Display

Configuration						
Message Standards		Message Standards				
		Change View	Install	Delete	Mark as Obsolete	Report
<input type="checkbox"/>	Name		Service Name	Description	Creation Date	Obsolete
<input type="checkbox"/>	Clearing	swift.secl	Clearing Release 2.0	2011/09/21	No	
<input type="checkbox"/>	CollateralManagement	swift.colr	Collateral Management Release 2.0	2011/09/07	No	
<input type="checkbox"/>	Derivatives - MX	swift.fpmi.st	Derivatives - MX Release 3.1	2011/03/03	No	
<input type="checkbox"/>	Derivatives - MX (VF)	swift.fpmi.st.vf	Derivatives - MX Release 3.1	2011/06/17	No	
<input type="checkbox"/>	FIN Category 1	swift.fin	FIN Category 1 - Customer Payments & Cheques	2014/06/10	No	
<input type="checkbox"/>	FIN Category 2	swift.fin	FIN Category 2 - Financial Institution Transfers	2014/06/10	No	
<input type="checkbox"/>	FIN Category 3	swift.fin	FIN Category 3 - Treasury Markets Foreign Exchange, Money	2014/06/10	No	
<input type="checkbox"/>	FIN Category 4	swift.fin	FIN Category 4 - Collections & Cash Letters	2014/06/10	No	
<input type="checkbox"/>	FIN Category 5	swift.fin	FIN Category 5 - Securities Markets	2014/06/10	No	
<input type="checkbox"/>	FIN Category 6	swift.fin	FIN Category 6 - Treasury Markets	2014/06/10	No	
<input type="checkbox"/>	FIN Category 7	swift.fin	FIN Category 7 - Documentary Credits & Guarantees	2014/06/10	No	
<input type="checkbox"/>	FIN Category 8	swift.fin	FIN Category 8 - Travellers Cheques	2014/06/10	No	
<input type="checkbox"/>	FIN Category 9	swift.fin	FIN Category 9 - Cash Management & Customer Status	2014/06/10	No	
<input type="checkbox"/>	FIN System	swift.fin	Category 0 - FIN System	2014/06/10	No	
<input type="checkbox"/>	GPA(APC) System	swift.fin	Category 0 - GPA(APC) System	2014/06/10	No	
<input type="checkbox"/>	JASDEC BETS CP	jasdec.bets.cp	JASDEC BETS CP Release 1.0	2012/02/24	No	
<input type="checkbox"/>	JASDEC BETS IT	jasdec.bets.it	JASDEC BETS IT Release 1.0	2012/02/24	No	
<input type="checkbox"/>	JASDEC BETS SB	jasdec.bets.sb	JASDEC BETS SB Release 1.0	2012/02/24	No	
<input type="checkbox"/>	JASDEC BETS ST	jasdec.bets.st	JASDEC BETS ST Release 1.0	2012/02/24	No	
<input type="checkbox"/>	JASDEC Settlement Mtchng Domestic	jasdec.psms.dam	JASDEC Settlement Mtchng Domestic Release 1.0	2012/02/24	No	

Details

Column	Description
Name	The name of the message standard
Service Name	The service name
Description	The description of the message standard
Creation Date	The creation date
Obsolete	Whether the message standard has been marked as obsolete

7.2.2 Message Standards Details Window

Content

The **Message Standards Details** window contains these elements:

- Details for the message standards

See "Details" on page 186

Display

Message Standard Details

Name: Derivatives - MX (VF)
 Service Name: swift.fpml.st.vf
 Description: Derivatives - MX Release 3.1.1
 Creation Date: 2011/06/17

Help

Message List

Rows in list: 7, in selection: 1

<input type="checkbox"/> Name	Identifier	Description	Version	Patch	Delivery Mode	Obsolete
<input type="checkbox"/> ResolutionOfInvestigationV03	camt.029.001.03	Resolution Of Investigation V03	03		Real-Time	No
<input type="checkbox"/> CustomerPaymentCancellationRequestV01	camt.055.001.01	Customer Payment Cancellation Request V01	01		Real-Time	No
<input type="checkbox"/> NotificationToReceiveV02	camt.057.001.02	Notification To Receive V02	02		Real-Time	No
<input checked="" type="checkbox"/> NotificationToReceiveCancellationAdviceV02	camt.058.001.02	Notification To Receive Cancellation Advice V02	02		Real-Time	No
<input type="checkbox"/> NotificationToReceiveStatusReportV02	camt.059.001.02	Notification To Receive Status Report V02	02		Real-Time	No
<input type="checkbox"/> FIToFIPaymentStatusReportV03	pacs.002.001.03	FIToFI Payment Status Report V03	03		Real-Time	No
<input type="checkbox"/> FinancialInstitutionCreditTransferV02	pacs.009.001.02	Financial Institution Credit Transfer V02	02		Real-Time	No

Change View Close

Details

Column	Description
Name	The name of the message
Identifier	The identifier of the message
Description	The description of the message
Version	The version of the message
Patch	The patch level of the message
Delivery Mode	The delivery mode of the message
Obsolete	Whether the message has been marked as obsolete

7.2.3 Install a Message Standard

Purpose

A message standards deployment package contains the message standards, and the online help for the message standards. Use this procedure to install the message standards and online help.

The Message Standards Deployment Package and Online Help document accompanies the deployment package and provides information about the file names that contains the standards, and also the keywords per message type.

Note Message standards online help is not provided for FpML messages.

The deployment package file is signed, and the digital signature is made available to you so that you can verify that the data was not tampered with. After installation, the message standards information is stored in the Alliance Message Management database.

Users and permissions

To display the list or the details of message standards, your operator profile must have this entity:

- **SWIFT Support**

To install message standards, your operator profile must have this action:

- **SWIFT Support / Install Msg Standard**

To use the **Install** button to install new deployment packages, your operator profile must have this action:

- **Access Control / Files on User Space**

Prerequisites

You must have the following items:

- a message standards deployment package for the message standard that you want to install. You can download message standards deployment packages from www.swift.com > support > [Tools](#). Select **Download Centre**, and then **Alliance - Standards Packages**.
- a digest for the message standard deployment package, to ensure that you are installing message standards that are valid.

Procedure

1. From the **Messages** menu, select **Message Standards**.

2. Click **Install**.

The **Message Standard Installation** window opens.

3. Next to the **Message Standards Package File Name** field, click **Browse**.

The **Choose file to upload** window opens.

4. Select the message standards package that you require and click **Open**.

The **Choose file** window closes and the path name of the message standards package appears in the **Message Standard Installation** window.

5. Similarly, if a help package file is available with the deployment package, next to the **Help Package File Name** field, click **Browse**.

The **Choose file to upload** window opens.

6. Select the help package file that you require and click **Open**.

The **Choose file** window closes and the path name of the help package file appears in the **Message Standard Installation** window.

7. Click **Install**.

The **Message Standard Installation** window closes and the **Install** window opens.

8. If the digest in the **Install** window matches the digest that you have received, then click **Confirm**.

The **Install** window closes.

A status popup message appears.

An information message opens.

9. Click **OK**.

If the installation is successful, then the standard contained in the message standards package appears in the list.

The installation is complete.

Note

- When a new version of a FIN (either base or MyStandards) message standard is installed, its previous version is not automatically marked as obsolete.
 - When a new version of an MX base message standard is installed, its previous version is automatically marked as obsolete.
 - When a new version of an MX MyStandards message standard is installed, its previous version is not automatically marked as obsolete.
 - For information on making a message standard obsolete, see "Make Message Standards Obsolete" on page 192.
 - Any change to a message type (for example, its verifiable field definition) is only effective in Message Management after two minutes or after a logout/login of Message Management, whichever comes first.
-

User-defined verifiable fields

Operators with the SWIFT Support, Install Msg Standard permission can overwrite the Standards list of verifiable fields for MT message types and MX service/request types and define their own selection of verifiable fields.

Operators can enter their own definition of verifiable fields in the **Verifiable fields** section at the bottom of the detailed view of an MT or MX message standard. In practice, operators must enter the XPath expression of the fields they want to define as verifiable. Following is an example of the syntax of an XPath expression for a currency field:

Body/Document/St1mOblgtnRpt/RptDtls/St1mOblgtnDtls/St1mAmt/Amt/@Ccy.

Tip

The XPath expression of a field can be copied and pasted from the field-level help that is available when creating a new message of that type. The operator can target ALL of the instances of a repeated field by removing the **[n]** in the path. In addition, qualifier values can contain (or be replaced by) wildcards, such as *****.

Both mandatory and optional fields can be defined as verifiable. When a optional field defined as verifiable field is not present and is moved to the verification queue, the optional (empty) field is not displayed as there is no value to be retyped in/verified.

When saving their changes, operators overwrite the verifiable fields of that particular MT or MX message standard in the Message Management deployment package. Changes to verifiable fields take effect immediately on all MT/MX messages that arrive in the verification queue.

Operators can add or remove verifiable fields in any MT or MX standard irrespective of whether or not the message is enterable and irrespective of whether or not the default standard from SWIFT contains verifiable fields for that MT or MX standard.

If a new version of a FIN MT or MX standard is installed and contains a different set of verification fields than the set of verifiable fields (including user-defined verifiable fields) contained in the previous version of the standard, the previous version is not updated (and retains its set of verifiable fields) and the new version is installed with its own set of verifiable fields. The new version is not automatically updated with the previous set of user-defined verifiable fields.

Alliance Access also supports the definition of verifiable fields in some MX and MT message header fields, including:

- For MX messages:
 - Requestor DN
 - Responder DN
 - User Reference
- For MT messages:
 - Receiving Institution
 - MUR

The definition of verifiable fields by operators does not require four-eyes approval.

Note Changes to a message type take effect after 2 minutes or after the operator logs out.

7.2.4 View the Message Standards

Overview

You can display descriptive information about the message standards that are installed.

Permissions required

You can only view message standards properties if the permission has been defined in your Alliance Access operator profile, that is, having the **SWIFT Support - Install Msg Standard** permission.

Procedure

To view the message standard:

1. From the **Messages** menu, select **Message Standards**.

The **Message Standards** page appears, displaying the message standards that are installed.

2. Select a message standard in the list, and click to open it.

The **Message Standards Details** page appears with a list of the messages contained in this standard.

For more information about the details of a message in the message standards, see "View the Properties of a Message in a Message Standard" on page 190.

7.2.5 View the Properties of a Message in a Message Standard

Overview

This procedure explains how to view the properties of a message standard, and details of the messages that it contains.

Permissions required

You can only view the properties and message details if your Alliance Access operator profile includes the permissions, **SWIFT Support - Install Msg Standard**.

Procedure

To view the details of a specific message:

1. From the **Messages** menu, select **Message Standards**.

The **Message Standards** page appears, displaying the list of message standards that are installed. See an example in "Message Standards Page" on page 184.

2. Select a message standard in the list to open it.

The **Message Standard Details** page appears, which shows a list of the messages in the selected message standard. It also displays the properties of the message standard.

3. Click a message in the **Messages List**.

The message properties for the selected message appear. The properties that are displayed are different for each messaging service.

Tip

To navigate easily through the list of messages use the **Previous** or **Next** buttons. This enables you to view the properties of the previous or next message in the message standard.

4. Click the **Edit Properties** button to edit the properties of the message standard. For more information, see "Edit the Properties of a Message in a Message Standard" on page 191.
5. Click the **Edit Verifiable Fields** button to edit the verifiable fields of the message standard. For more information on verifiable fields, see "Install a Message Standard" on page 186.
6. Click **Close** button to return to the list of message standards in the **Message Standards** page.

Reporting of message standards

You can generate printable reports that contain the verifiable fields of MT or MX message types, from either the Message Standards view or the Message List view.

To generate a report from the **Message Standards** view, perform the following steps:

1. Select one or more of the installed standards, then select **Report**.
2. Select the desired report output settings, such as report type (for example, Summary) and output format (for example, PDF).
3. Using the **>** or **>>** buttons, move the columns that you want to appear in the report from the **Available** to the **Selected** list box.

4. If you select the **Include message type details** check box, the report will contain all of the details from the deployment package, of the message types that are included in the selected message standard(s), including their verifiable fields. The report does not indicate whether the verifiable fields are derived from the official SWIFT Standards definition or if they were user-defined. If you do not select this option, the report will contain only the list of message types for the selected message standard(s) (and no details from the deployment package).
5. Click **OK**. The report will be displayed on-screen when complete.

To generate a detailed report from the **Message List** view, perform the following steps:

1. Select one or more of the message types for the message standard displayed, then select **Report**.
2. Select the desired report output settings, such as report type (for example, Summary) and output format (for example, PDF).
3. If you select the **Include message type details** check box, the report will contain all of the details from the deployment package, of the message types that are included in the selected message standard, including their verifiable fields. The report does not indicate whether the verifiable fields are derived from the official SWIFT Standards definition or if they were user-defined. If you do not select this option, the report will contain only the list of message types for the selected message standard displayed (and no details from the deployment package).
4. Click **OK**. The report will be displayed on-screen when complete.

7.2.6 Edit the Properties of a Message in a Message Standard

Overview

You can edit the properties of an MX message in a message standard, to set default values for the **Requestor DN** and **Responder DN** fields for a specific message.

Note You cannot edit the properties of FIN or APC messages.

Properties required

You can only edit the properties of an MX message in a message standard if your Alliance Access operator profile includes the permissions, **SWIFT Support - Modify Msg Standard**.

Procedure

To configure the properties of an MX message standard:

1. From the **Messages** menu, select **Message Standards**.

The **Message Standards** page appears, displaying the list of message standards that are installed. See an example in "Message Standards Page" on page 184.

2. Click a message standard in the list, to open it.

The **Message Standard Details** page appears, which shows a list of the messages in the selected message standard. It also displays the properties of the message standard.

3. Click a message in the **Messages List**.

The message properties for the selected message appear.

4. Click **Edit Properties**.
5. Provide values for either or both of the **Requestor DN** and the **Responder DN** fields.
6. Click **Save**.

Tip To undo a property change, repeat Step 4 of this procedure and enter the correct value.

7.2.7 Make Message Standards Obsolete

Overview

You can only make message standards obsolete if the permission has been defined in your Alliance Access operator profile, that is, having the **SWIFT Support - Install Msg Standard** permission.

You can specify that all messages for an MX or FpML message standard are obsolete, or that a particular message for an MX or FpML message standard is obsolete. Operators are not allowed to create new messages or message templates based on obsolete information. However the Alliance Access Configuration database retains the information for an obsolete message, so that corresponding messages (already created by operators or applications) can still be processed.

To make a message standard obsolete:

1. From the **Messages** menu, select **Message Standards**.
The **Message Standards** page appears, displaying the list of message standards currently installed.
 2. Select the appropriate MX message standard by checking the box in the left-most column. You can select all the standards on the page by checking the box in the column heading line.
 3. Click **Mark as Obsolete**. A confirmation window appears.
- Note** The only way to restore a message standard that was marked as obsolete is to install it again.
-
4. Click **OK** to confirm or **Cancel**.

To make a specific MX or FpML message obsolete:

1. From the **Messages** menu, select **Message Standards**.
The **Message Standards** page appears, displaying the list of message standards currently installed.
2. Select the relevant message standard in the list and click to open it. The list of messages contained in this standard appears.
3. Select the message(s) to be marked as obsolete by checking the box in the left-most column. You can select all the messages on the page by checking the box in the column heading line.
4. Click **Mark as Obsolete**. A confirmation window appears.
5. Click **OK** to confirm or **Cancel**.

7.2.8 Delete a Message Standard

Purpose

This procedure enables you to delete an MX message standard.

Users and permissions

To display the list or the details of message standards, your operator profile must have this entity:

- **SWIFT Support**

To delete message standards, your operator profile must have this action:

- **SWIFT Support / Remove Msg Standard**

Procedure

1. From the list of message standards, select the check box of one or several standards in the left column.
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
A status popup message appears.

7.3 Message Templates

7.3.1 Message Templates

Definition

A template is a message where some fields are pre-filled with relevant values. You can create message templates for FIN, APC, and MX messages.

The content of a message template can be modified, if needed.

Users and permissions

To import and export MT and MX message templates, your operator profile must have these actions:

- **Access Control / Files on User Space**
- **SWIFT Support / Export Template and Import Template**

Benefit of using a message template

You can use message templates to create messages that you send on a regular basis.

A message template contains values that do not change often, such as the sender and the receiver of the message. When you create a message from a template, then you only need to enter values for fields that are variable, such as dates and amounts. You can use one template to create any number of new messages.

A template can be assigned to a unit within the business. A unit is a group of operators within an organisation that has common requirements, such as the need to deal with the same

confidential information. Templates that are assigned to the unit **None** are available to everyone. If a template is assigned to a unit, then that template is only available to operators who have that unit assigned in their operator definition. For more information about unit definition and assignment, see the "Units" on page 236.

Import and export of message templates

It is possible to export and import MT, MX, and APC message templates, which are then saved in a single file. For example, you can export the templates from a previous release of Alliance Access, and then import them to the current release.

7.3.2 Message Template Guidelines

Overview

This section provides information about managing and migrating your message templates in Alliance Access. This can help you with preparing for new FIN Message Standards, or if you are planning to start using the Message Management GUI package.

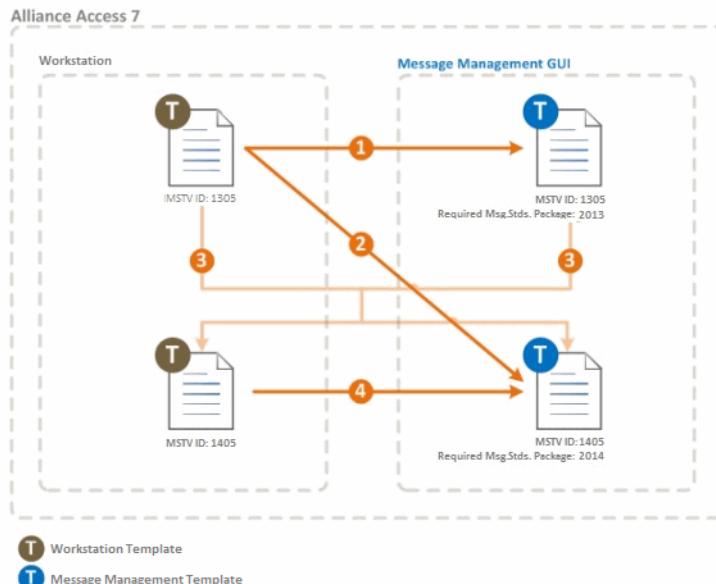
Whenever you open a template created with a previous message standard, a warning pop-up is displayed. Alliance Access will try to resolve the template with the new standard or indicate that the resolution had failed and manual actions are required. This pop-up will appear each time the template is opened, until it is updated.

If you open a template in Message Management and update it, then it can no longer be used in Alliance Workstation. If you still need the template available in Alliance workstation, then it is recommended to use the Template Import Tool.

Updating and migrating templates

Message templates created in Alliance Workstation must be migrated before they can be used in the Message Management GUI.

The following diagram illustrates the different paths that can be followed in order to update or migrate message templates either by using the Message Management GUI package or the Template Import Tool in Alliance Access. Each path has been numbered and is explained:



1. The Workstation template assigned to MSTV ID 1305 is opened in the Message Management GUI. The template will then be migrated to a Message Management message on MSTV ID 1305.

Note You must have the "*FIN SR2013 for Message Management and Online Help*" Standards Package installed for the Message Management GUI to successfully open and migrate the template. Also, the MSTV ID assigned to the LT (for the sending BIC) must be set to 1305 in order to trigger the migration to the FIN Standards Release 2013. The newly migrated message can then be saved as a template in the Message Management GUI for future use as a template. It is also possible to modify this template and save it after it has been migrated which will then not generate an additional template (duplicate avoidance).

2. The Workstation template assigned to MSTV ID 1305 is opened in the Message Management GUI (2014). The template is then migrated to a Message Management message on MSTV ID 1405. The newly migrated message can now be saved as a template in the Message Management GUI for future use as a template.

Note In order to migrate the template, the Standards packages "*FIN SR2013 for Message Management and Online Help*" and "*FIN SR2014 for Message Management and Online Help*" for the Message Management GUI must be installed. Also, the MSTV ID assigned to the LT (for the sending BIC) must be set to 1405. If the Standards packages "*FIN SR2013 for Message Management and Online Help*" has not been installed, an error may occur when opening the template stating that it cannot be read. It is also possible to modify the existing template and save it after it has been migrated which will then not generate an additional template (duplicate avoidance).

3. All the existing templates are exported from Alliance Access to a file (based on the criteria specified during the export). When the exported templates are imported again into Alliance Access, they will be converted to the MSTV ID that has been specified during the import (MSTV ID 1405). The newly imported templates can then be accessed by Message Management GUI and also by Workstation (if the option to preserve compatibility with Workstation is selected) respectively when the MSTV ID assigned to the LT (for the sending BIC) has been set to 1405 and the Standards packages "*FIN SR2013 for Message Management and Online Help*" and "*FIN SR2014 and Online Help*" have been installed.

Note In some cases certain Message Management templates that have been imported and converted to MSTV ID 1405 might not have been converted properly due to too many syntax changes (between MSTV ID 1405 & 1305). You will be able to open the template but the resulting message will only appear in Fast mode. In such cases, the template either needs to be updated in Fast mode, manually recreated or it has to be migrated from a Workstation template based on either MSTV ID 1305 or 1405 (See steps 2 & 4).

4. The template assigned to MSTV ID 1405 is opened in the Message Management GUI (2014). The template is then migrated to a Message Management message. The newly migrated message can now be saved as a template in the Message Management GUI for future use as a template.

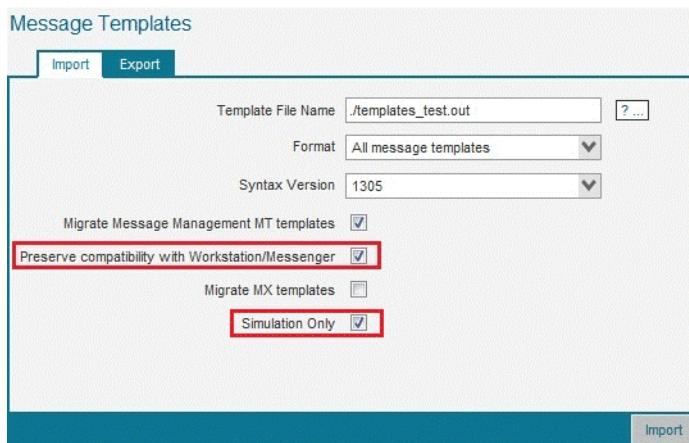
Bulk operations

By doing bulk processing, you can avoid having the pop-up every time you open a template created on Alliance Workstation or that is still resolved with a previous message standard.

In the Message Management GUI package you can:

- do a bulk resolution of templates and, if created in Alliance Workstation, you have the option to preserve or not the compatibility with them.
- do a bulk simulation resolution of templates to see which ones will be properly resolved and which ones will require manual intervention. A report is generated in your user space, listing the templates that were in the simulation and the corresponding simulated result.

You can launch the simulation of resolution of templates (at the time of import), whether you are importing templates into Message Management with the same message standards or with new message standards. The resulting report will provide information on which templates can be migrated successfully versus the ones that did not and will require manual intervention. In addition, compatibility with Workstation can be kept:



If you are uncertain about the MSTV ID version that is currently assigned to your message template, then open the template in the Message Search Application in your Workstation, select the **Other** tab and verify the **Version** in the **Format & Validation** section.

Recommendations

- When migrating your templates, please ensure that you choose a good naming convention for your templates to differentiate which ones can be used by Alliance Workstation and Message Management. This is because Alliance Access does not provide any visual aids to indicate which template is intended for Alliance Workstation or Message Management. By choosing descriptive names, for example appending the templates for the Message Management GUI with "_MM", will help operators to choose the appropriate templates when using either Alliance Workstation or Message Management (if you are using both).
- When importing an exported set of templates from (an) older FIN Standards Release(s), it is possible that Alliance Access is unable to fully convert the template in accordance with the new message syntax. In such cases, the template will only appear in Fast mode. The template then either needs to be updated in Fast mode by adding/removing/modifying the relevant fields or manually recreated from a new FIN message (which is saved as a template)

Checking the Message Standards version in Alliance Workstation

If you are uncertain about the MSTV ID version that is currently assigned to your message template, then open the template using Alliance Workstation and in the Message Search application go to the **Other** tab and verify the **Version** in the **Format & Validation** section.

If this proves inconclusive (due to discrepancies between the Workstation & the Message Management GUI), you can also export your templates and open the exported file in your favourite editor. Locate the desired template within the export file using the

msg_template_name field. Once you have located the template entry, check the **text_swift_prompted** field and if it starts with **XML#**. If so, then this template has been migrated to the Message Management format, otherwise it is still in the old format:

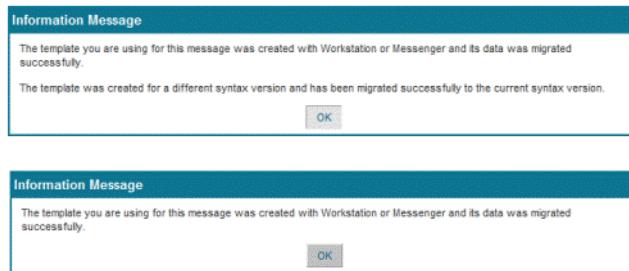
```

inst_receiver_network_iapp_name,5,SWIFT
text_s_umid,16,7C3EF7CCFFFFFADF
text_data_block,$2,
:20:
:23B:CRED
:32A:EUR
:59A:BANKAABOXXX
:71A:
text_swift_prompted,292,XML#H4sIAAAAAAAAFA2R0QqCMBSGXyV8ALcp
msg_s_umid,16,7C3EF7CCFFFFFADF
msg_validation_requested,13,No Validation

```

Checking if a template has been migrated

If you are uncertain if a template has been converted to the Message Management format (if you cannot open/access a template export), you can open the template in the Message Management GUI. If no Information window appears informing you that the content of the template will be migrated, then it has already been converted:



7.3.3 How an MT Message Template Is Imported

Overview

It is important to understand the relationship between exported templates and how the import function extracts data to create prompt templates in Alliance Access. Therefore, the following examples are important to understand if you import fast templates created using an earlier release of Alliance Access, which you import and then open in prompt mode.

Importing an MT message template

When Alliance Access imports a template the fields in block 4 of the template are compared to the syntax description for that message type. The syntax of messages is provided in a message syntax table.

Alliance Access starts from the first field of the template and compares each field with the message syntax description.

The outcome of import depends on the results of the comparison:

- all template fields match the message syntax description: a prompt template is created.
- at least one template field is incompatible with the message syntax description, or a field varies from the message syntax description: a fast template is created

If you export a valid template, then the results of it importing it can vary depending on the message syntax description. For more information, see the examples provided:

- "Message syntax samples" on page 198
- "Examples of invalid templates after import" on page 198

- "Examples of valid templates but incorrect mapping" on page 199

In addition if you export a fast template, and import it and open it as a prompt template, then inconsistencies can result.

Message syntax samples

Consider the following message syntax description as an example:

```
MF20
OF21
Start of loop; minimum 1 maximum 10
MF32A
OF53A, B, D
End of loop
```

The following rows in the table show the result of a comparison based on the syntax description:

Example	Fields in template	Notes about the comparison	Template type
1	:20:TRN :32A:980228USD100, :53B:SWIFT :32A:980303NOK250,	The order and syntax of the fields match the message syntax description.	prompt template
2	:20:TRN : 32A:980228 :53B:SWIFT : 32A:980303NOK250 ,	The syntax of field 32A does not match the message syntax description.	fast template
3	:20:TRN :32A:980228USD100, :53B:SWIFT :53B:SWIFT	The second occurrence of the loop is incorrect.	fast template
4	:20:TRN	The required minimum occurrence of the loop is missing. However, templates can exist without all required fields being completed.	prompt template
5	:20:TRN :32A:980228USD100, :53B:SWIFT :53C:/SWIFT	The syntax description is complete. However, the field 53C is incompatible with the message syntax description.	fast template

Examples of invalid templates after import

The following example describes the results of importing the following message template fields:

Message syntax	Input template fields	Results
Start of loop MF35B ... OF18A End of loop MF18A	:35B:<correct syntax> :18A:<correct syntax>	As soon as the import program finds field 18A, it maps it to the first occurrence of that field in the expected syntax. In this example, OF18A, which is an optional field. The mandatory field is missing in this example. Therefore, the input template is valid. However, the resulting prompt template is invalid.

The following example describes the results of importing the following message template fields:

Message syntax	Input template fields	Results
Start of optional sequence B MF32F MF87 A, B or D MF34P OF53A, B or D MF57A, B or D End of sequence B Start of optional sequence C MF32F MF87A, B or D MF34R MF57A, B or D End of sequence C	:32F:<correct syntax> :87A:<correct syntax> :34R:<correct syntax> :57A:<correct syntax>	Fields 32F and 87A match the beginning of sequence B. However, the mandatory field 34P is missing from the template. Therefore, the input template is valid. However, the resulting prompt template is invalid.

Examples of valid templates but incorrect mapping

Extracting the data for block 4 can result in some fields being mapped differently in the newly created template, compared to their relative positions in the exported template. Some of the mapping differences can also result in invalid templates. The circumstances under which mapping differences may occur are best illustrated with a few examples.

The following example shows how ambiguities in message syntax can result in a template that is valid, but where the data is mapped to a different position after the template is imported:

Message syntax	Input template fields	Results
Start of mandatory sequence A MF30 OF31F OF87A, D ... some optional fields End of sequence A Start of optional sequence B ... some optional fields OF87A, D End of sequence B	:30:<correct syntax> :87A:<correct syntax>	The template would be in prompt mode with field 87A in sequence B. After exporting and then importing the template, field 87A would be part of sequence A instead.

The following example shows how ambiguities in message syntax can result in a template that is valid, but in which the data is mapped to a different position after the template is imported:

Message syntax	Input template fields	Results
Start of repetitive optional sequence B MF35B Start of loop OF83A, C or D OF23 End of loop End of sequence B Start of repetitive optional sequence C MF23	:35B:<correct syntax> :23:<correct syntax> :83A:<correct syntax>	Before exporting the template, field 35B was in sequence B, and fields 23 and 83A were in sequence C. After export and import the template would still be valid, but fields 23 and 83A would be in sequence B.

Message syntax	Input template fields	Results
Start of loop OF83A, C or D OF35B End of loop End of sequence C		

7.3.4 Internal Format of MT Message Template

FIN trailer - Block 5

FIN adds trailers to a message for control purposes, to convey additional information, and to indicate that special circumstances apply to the handling of the message. One or more trailers may appear in Block 5 of a FIN message. FIN formats trailers as a global block (with Block Identifier 5) that contains one or more blocks. Each block contains a given trailer. Each trailer begins with a 3-letter code, which is followed by a colon, and then by the trailer information.

It is possible to prevent the mapping of exported and imported template fields from being inconsistent by exporting and importing the internal formats of prompt templates. The internal format is stored in block 5 and is identified with tag {TMPI:<internal format>}. Block 5 contains the tag {TMPQ:<mesg_template_name>} to identify the name of each template.

The internal format is not exported for fast templates. Therefore, block 5 contains only the name of the template. If a template created in fast mode is imported and then opened in prompt mode, then mapping inconsistencies can result, as described in the section "Message Templates" on page 193.

Using this structure, even obsolete templates can be exported and imported exactly as they were created.

Internal format tag values

The structure of the internal format consists of the following elements:

Tag value	Element	Description
\144	BLOCK_SEPARATOR	Indicates another block of data, or indicates in which subfield data was entered
\145	FIELD_INDICATOR	Indicates a field
\146	LOOP_INDICATOR	Indicates the start of the first occurrence of a loop
\147	LOOP_OCC_INDICATOR	Indicates another occurrence of a loop
\148	LOOP_END_INDICATOR	Indicates the end of a loop
\149	SEQUENCE_INDICATOR	Indicates the start of a sequence
\150	SEQUENCE_END_INDICATOR	Indicates the end of a sequence
\151	OPTION_FIELD_INDICATOR	Indicates a field where letter options are chosen, such as 56A, B or D
\152	ALTERNATE_FIELD_INDICATOR	Indicates an alternative choice (system messages)

Example of the internal format in Block 5

For example, consider the following invalid example for an MT 103 template (the currency subfield is empty):

```
:20:REF
:23B:CRED
:32A:980620 1000, (the currency subfield is empty)
:50K:CLIENT
:59:BENEF
:71A:SHA
```

The resulting internal format would be a string as follows (line breaks are added to the example string here for readability purposes):

```
\128\00283\144\145F20\144REF\144\145F23B\144CRED\144
\145F32A\144980620\144\1441000,\144
\145F50K\144CLIENT\144\145F59
\144BENEF\144\145F71A\144SHA\144
```

Where:

- \128: the internal format for a prompt template
- \00283: this is the second prompt version (002) and 83 widgets must be created

Even though the currency subfield has no value, all the fields and data in this example would be mapped to the expected positions after importing the template.

7.3.5 Message Templates Page: Import Tab

Content

The **Import** tab contains these elements:

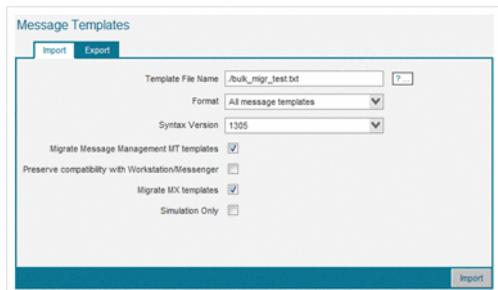
- Details that relate to the import of message templates
 - See "Details" on page 202
- Functions that enable you to manage the import of message templates
 - See "Functions" on page 203

The MT and MX message standards used by the template import functionality to migrate template data must be installed in Message Management. The message standards installed in Configuration are only used internally by Alliance Access and have no impact on the template import.

An XML report is produced in the user space folder next to the template file to be imported, with the name **<template_file_name>_report_<timestamp>.xml**. This report specifies for each template if the data migration was successful, the kind of migration that was performed, and the reason for any failure. If the data migration for a template fails, all of its data is imported as-is into Alliance Access.

Note	If the option selection is such that no migration is required for any templates, a report file is not produced and the Simulation Only option is not available.
-------------	--

Display



Details

Field	Description
Template File Name	The file name of the template
Format	<p>Filters the available templates according to the message format</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • All message templates • FIN message templates • MX message templates
Syntax Version	<p>Alliance Access compares the imported template to the selected message syntax version, to create the new templates.</p> <p>This option is not available when Format is set to MX message templates</p>
Migrate Message Management MT templates	<p>This option is only available when the Format selected includes FIN message templates. When available, it is selected by default.</p> <p>When the option is selected, the internal format of Message Management MT templates is migrated to the import target syntax version. A base template is migrated to the base schema with the same service code/message UID and with the import target version. A MyStandard template is migrated to the MyStandard schema with the same message UID and the target import version. If multiple such schemas are installed, the template is not migrated and the result code is set to VERSION_MIGRATION_MULTIPLE_TARGET_MESSAGE_TYPES.</p> <p>This option should always be selected under normal circumstances. When not selected, the internal format of Message Management MT templates will not be migrated to the import target syntax version, which will cause them to open in fast mode in Message Management. This occurs regardless of whether the template is associated with a base schema or a MyStandard schema.</p>
Preserve compatibility with Workstation	<p>This option is only available when the Format selected includes FIN message templates. When available, it is selected by default.</p> <p>When the option is selected, the internal format of Workstation templates is not migrated to the Message Management internal format. As a consequence, they can still be used by Workstation users. Message Management users who open one of these templates after the import are presented with a pop-up stating that the template was created with Workstation and that its data was migrated as part of the template opening process. The template can still be used by Workstation users as long as no Message Management user edits and saves the template.</p> <p>When the option is not selected, the internal format of Workstation templates is migrated to the Message Management internal format. Workstation users can no longer use the migrated templates. Message Management users who open one of these migrated templates are not presented with a pop-up.</p>

Field	Description
Migrate MX templates	<p>This option is only available when the Format selected includes MX message templates. When available, it is selected by default.</p> <p>When the option is selected and the template is associated to a base schema, an MX template whose message type is marked as obsolete in Message Management (for example, as the result of installing a new deployment package) is migrated to the latest message type version installed in Message Management (if any).</p> <p>If the template is associated to a MyStandard schema and there is another non-obsolete MyStandard schema with the same message UID, the MX template is migrated to that schema as part of the import. If there are multiple such schemas, the template is not migrated and the result code is set to <code>VERSION_MIGRATION_MULTIPLE_TARGET_MESSAGE_TYPES</code>.</p> <p>Message Management users who open an MX template which was migrated by the import will not be presented with a pop-up.</p> <p>When the option is not selected, MX templates whose message type is marked obsolete in Message Management are not migrated. Message Management users who open an MX template whose message type is marked obsolete are presented with a pop-up stating that the template data was migrated as part of the template opening process (provided a higher message type version is installed).</p> <p>In all other cases, the MX template is imported as-is, without any migration.</p> <p>The new message standard must be installed before running the import.</p>
Simulation only	When this option is selected, the template Import will only produce a report in the user space folder containing the template file to be imported. No template will actually be imported into Alliance Access. This enables you to test that the import produces the expected result before actually storing the templates in Alliance Access.

Functions

Function	Description
 ...	Opens the Choose File window that enables you to select the file that contains the template
 Import	Imports the message template

7.3.6 Message Templates Page: Export Tab

Content

The **Export** tab contains these elements:

- Details that relate to the export of message templates

See "Details" on page 204
- Functions that enable you to manage the export of message templates

See "Functions" on page 204

Display

Message Templates

		Import	Export
Template File Name	<input type="text"/>	? ...	
Format	<input type="button" value="All message templates"/>		
Sender LT BIC12	<input type="text"/>		
Replacement LT BIC12	<input type="text"/>		
<input type="button" value="Export"/>			

Details

Field	Description
Template File Name	The name of the file that contains the message template
Format	Filters the available templates according to the message format These are the possible values: <ul style="list-style-type: none">• All message templates• FIN message templates• MX message templates
Sender LT BIC12	The BIC12 name of the logical terminal that contains the templates to export Optional: If you do not enter a value, then the system exports all templates.
Replacement LT BIC12	The BIC12 name of the logical terminal that receives the templates that the system exports Optional: Valid only if you enter a value for Sender LT BIC12

Functions

Function	Description
? ...	Opens the Choose File window that enables you to select a file that contains the template
<input type="button" value="Export"/>	Exports the template

7.3.7 Import a Message Template

Purpose

This procedure enables you to import a message template for FIN or MX messages.

You cannot import a template for FileAct messages using Alliance Access Configuration. However, you can use the Configuration Replication tool (saa_import) to import File template. For more information, see the *Administration Guide* for [AIX](#), [Linux](#), [Oracle Solaris](#), or [Windows](#).

Users and permissions

To import message templates, your operator profile must have this action:

- **SWIFT Support / Import Msg Templates**

Procedure

1. From the **Import** tab, click .
 2. The **Choose File** window opens.
 3. You can select a file that is already available in your User Space or upload a file. You can also add a folder to the User Space if needed.
 4. Click .
 5. The **Choose File** window closes.
 6. In the **Format** drop-down list, select a message format.
 7. If you selected All message templates or FIN message templates, select a syntax version.
 8. Click .
- A status popup message appears.

7.3.8 Export a Message Template

Purpose

This procedure enables you to export the message template for FIN or MX messages.

Note	You cannot export a template for FileAct messages using Alliance Access Configuration. However, you can use the Configuration Replication tool (saa_export) to export a File template. For more information, see the <i>Administration Guide</i> for AIX , Linux , Oracle Solaris , or Windows .
-------------	--

Users and permissions

To export message templates, your operator profile must have this action:

- **SWIFT Support / Export Msg Templates**

Procedure

1. From the **Export** tab, click .
 2. The **Choose File** window opens.
 3. Select a file in the list (already present in the User Space), or type a path and file name in the **File Name** field.
 4. You can also add a folder for the message templates to the User Space, if needed.
 5. If you select an existing file, then the exported templates are appended to the file.
 6. Click .
- The **Choose File** window closes.

4. In the **Format** drop-down list, select a message format.
5. If you selected All message templates or FIN message templates, you can indicate the BIC12 name of the logical terminal that contains the templates to export in **Sender LT BIC12** and the BIC12 name of the logical terminal that receives the templates that the system exports in **Replacement LT BIC12**.
If you do not enter a value in **Sender LT BIC12**, then the system exports all templates.
6. Click **Export**.

A status popup message appears, and an event is written in the Event log.

7.4 Message File Archives

7.4.1 Archival of Messages

Description

- Archiving moves completed messages from the database into archives. You must archive regularly as you can only back up messages to an external storage after they have been archived.
- Messages of a particular day are only archived if all the messages of that day are completed. If live messages are present for any day in the archival period, then the archival process is not started for that day. Use Message Management to complete those messages, and then start the archival process again.

Archival of FileAct messages

When Alliance Access archives a File message, the payload of the message is archived based on the setting of the **Set FileAct Payload Archival** function. For more information on this function, see the [Application Service Profiles](#) page in the [Configuration Guide](#).

Types of message archival

You can perform the following types of archival:

- **Normal Archive**

This process marks completed messages selected for archive as read only. The archived messages remain in the database.

- **Destructive Archive**

This process removes all completed messages without archiving them. Uncompleted messages remain in the database.

Note This choice is determined by the setting of the **Archive Method** security parameter.

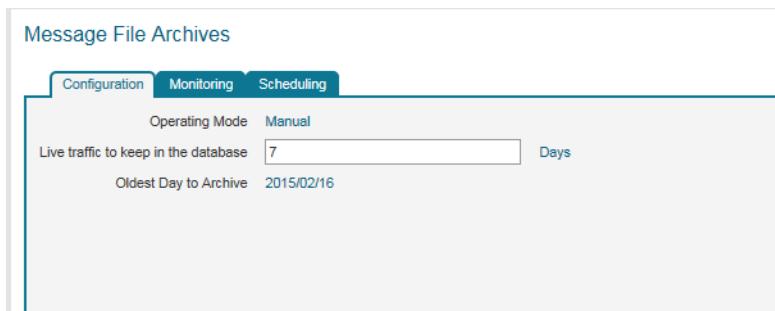
7.4.2 Message File Archives Page: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details that relate to the configuration of the message file archives
See "Details" on page 207
- Functions that enable you to manage the message file archives
See "Functions" on page 208

Display



Details

Field	Description
Operating Mode	These are the possible values: <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
Live traffic to keep in the database	The number of days for which the system keeps the messages in the database
Oldest Day to Archive	The date of the oldest message to be archived

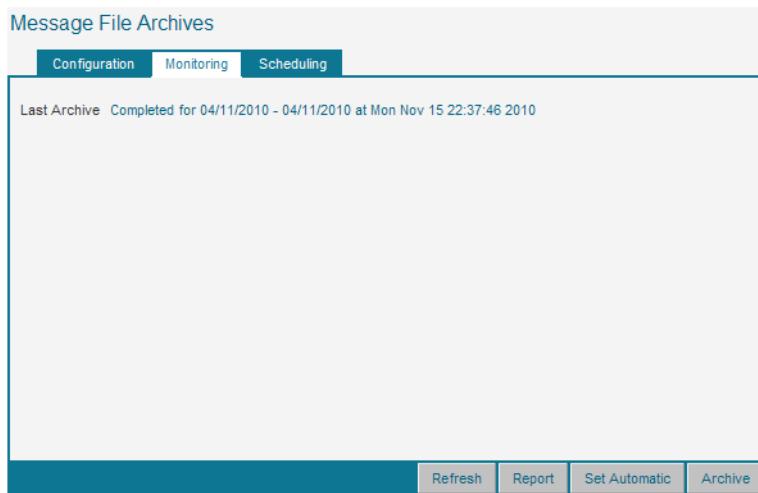
7.4.3 Message File Archives Page: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details of the last message archive
See "Details" on page 208
- Functions that enable you to manage the archiving
See "Functions" on page 208

Display



Details

Field	Description
Last Archive	The status of the last archiving process and date and time when it was carried out

7.4.4 Message File Archives Page: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Scheduled Action Details Window" on page 29.

7.4.5 Message File Archive Functions

Overview

These functions enable you to manage message file archives.

Functions

Function	Description
Set Automatic / Set Manual	Enables you to set the operation mode to Automatic or to Manual Procedure: "Change the Operation Mode" on page 209
Archive	Enables you to archive the messages manually Procedure: "Configure and Launch a Manual Archiving of Messages" on page 208

7.4.6 Configure and Launch a Manual Archiving of Messages

Purpose

This procedure enables you to archive messages manually.

The status of a message can be either "Live" or "Completed". The message is "Live" if any of the message instances associated with it are still being processed. You cannot create an archive for any day that has live messages. Before you begin archiving, you must use Message Management to find any messages that you want to archive, but which still have live message instances. You can then complete the message instances, which also completes the message itself.

Note Messages older than a few days must normally always be complete. If not, this means that the original, a copy or a notification of the message is still queued in Alliance Access. Make sure that you take the necessary business-related actions before completing the message instances.

Users and permissions

To display the archiving configuration details and archive messages manually, your operator profile must have this action:

- **Message File / Archive**

Procedure

1. From the **Configuration** tab, in the **Live traffic to keep in the database** field type the number of days for which you want to keep messages available in the database.

All other messages are archived. For example, if you type 2, Alliance Access keeps today's messages and the messages from the previous day in the live database, and archives all messages with earlier dates.

2. Click **Save**.

In the **Oldest Day to Archive** field, the date of the oldest message to be archived appears.

3. Click **Archive**.

A status popup message appears.

If archiving is successful, then an archive is created in the database. You can check the status of the last archive from the **Monitoring** tab.

7.4.7 Change the Operation Mode

Purpose

This procedure enables you to change the operation mode.

Users and permissions

To change the operation mode, your operator profile must have this action:

- **Message File / Archive**

The **Modify operating mode** permission must be set to **Yes**.

Procedure

- From the **Configuration** tab, the **Monitoring** tab, or the **Scheduling** tab, given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

A status popup message appears.

7.4.8 Monitor the Archiving of Messages

Purpose

This procedure enables you to monitor the status of the last archiving process.

Users and permissions

To display the archiving configuration details and the status of the last message archive, your operator profile must have this action:

- **Message File / Archive**

Procedure

1. Click the **Monitoring** tab.
2. You can click  to refresh the list.

7.5 Message Archive Backups

7.5.1 Message Archive Backups

Overview

Once archived, messages can be backed up to an external storage.

You can launch the backup process manually or create a schedule.

A backup is the only way to free the space that the archives use. If you do not have to use the archives on a daily basis, then you are advised to make regular backups of the archives and remove the original archives. This action makes disk space available and enables data to be recovered efficiently in the event of a major problem, such as, disk failure.

You can also restore the contents of archive backup files into the Alliance Access database. The restore process can only be launched manually.

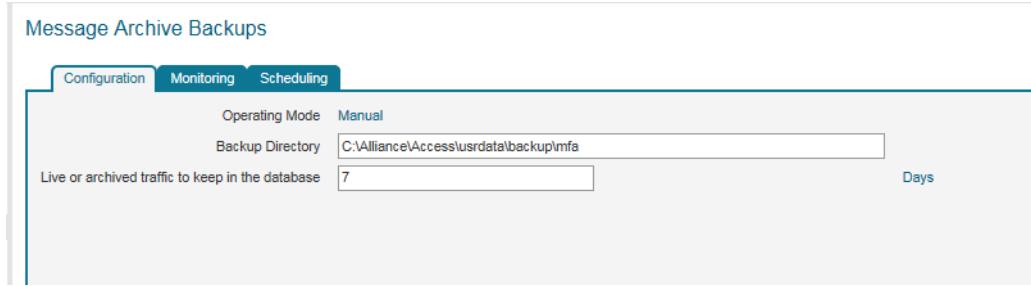
7.5.2 Message Archive Backups Page: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details of the backup configuration
 - See "Details" on page 211
- Functions that enable you to manage the backups
 - See "Functions" on page 212

Display



Details

Field	Description
Operating Mode	These are the possible values: <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
Backup Directory	The location where Alliance Access stores archive backup files. The default location is: <software dir>\usrdata\backup\mfa where <software dir> is the directory in which Alliance Access is installed. Note: On Windows only: If you have a hosted database configuration, you can access remote file directories by specifying UNC paths. Do not use a mapped drive
Live or archived traffic to keep in the database	The minimum number of days between the time a message is created in the Alliance Access database, and the time that the archived message can be backed up and removed or the time that the archived and backed-up message can be removed. Specify an integer, which represents the number of days.

7.5.3 Message Archive Backups Page: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details of the last message archive backup or restore
See "Details" on page 212
- Functions that enable you to manage the backups
See "Functions" on page 212

Display

Details

Field	Description
Last Archives Backup Status	The status of the last message archive backup and date and time when it was carried out
Last Restore Status	The status of the last restore process and date and time when it was carried out

7.5.4 Message Archive Backups Page: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Scheduled Action Details Window" on page 29.

7.5.5 Message Archive Backup Functions

Overview

These functions enable you to manage the message archive backups.

Functions

Function	Description
Set Automatic / Set Manual	Enables you to set the operation mode to Automatic or to Manual Procedure: "Change the Operation Mode" on page 214
Restore	Enables you to restore an archive backup Procedure: "Restore a Message Archive Backup" on page 215
Backup	Enables you to launch an archive backup manually Procedure: "Configure and Launch a Manual Message Archive Backup" on page 213

7.5.6 Change the Default Directory for Message Archive Backups

Purpose

This procedure enables you to change the location where Alliance Access stores archive backup files.

The default location is: **<software dir>\usrdata\backup\mfa** where **<software dir>** is the directory in which Alliance Access is installed.

If you are using a hosted database, the directory cannot be changed manually. The path is deduced from the value of a system parameter. After installation, the parameter is not initialised. You have to change its value before being able to perform a backup.

Name of message archive backups

Alliance Access creates a directory for every archive backup.

The following naming convention is used: **<MEAR>_<ArchiveName>**

Where:

- **<MEAR>** represents the type of item being archived (here message archives)
- **<ArchiveName>** represents the name of the archive that Alliance Access backed up

Example: MEAR_20101215

Users and permissions

To display the configuration details and the status of the last message archive backup, your operator profile must have this entity:

- **System Management**

To change the default directory, your operator profile must have this action:

- **System Management / Backup**

Security officers can change the default directory.

Procedure

1. Modify the path in the **Backup Directory** field.

2. Click **Save**.

A status popup message appears.

7.5.7 Configure and Launch a Manual Message Archive Backup

Purpose

This procedure enables you to back up message archives manually.

Users and permissions

To display the configuration details and the status of the last message archive backup, your operator profile must have this entity:

- **System Management**

To launch manual backups, your operator profile must have this action:

- **System Management / Backup**

Security officers can launch manual backups.

Procedure

1. From the **Configuration** tab, click **Backup**.

The **Backup Archives** window opens.

2. In the **Mode** drop-down list, select one of the following options:

- **Backup**: To create a backup of the archive, without deleting the archive
- **Backup and Remove**: To create a backup of the archive, and then delete the original archive after the backup is complete

Note The Remove option enables you to delete an archive that has the status **DONE**, without creating a backup for the archive.

3. Select the **Overwrite Existing Archives Backup** check box if you want to replace the oldest backup contained in the directory.

4. In the **Archives (Backup Status)/Available** list, select the archives to back up.

Note An archive must have the status **READY** (Alliance Access has archived data successfully, and the archive is ready to be backed up) or **DONE** (Alliance Access has created a backup of the archive successfully) before you can create a backup for it.

5. Click **Backup**.

The **Backup Archives** window closes.

A status popup message appears.

The information message informs you about the status of the backup request. If the request is accepted, the backup is launched as a background task. You have to monitor the status of the backup from the **Monitoring** tab.

7.5.8 Change the Operation Mode

Purpose

This procedure enables you to change the operation mode.

Users and permissions

To display the configuration details and the status of the last message archive backup, your operator profile must have this entity:

- **System Management**

To change the operation mode, your operator profile must have this action:

- **System Management / Backup**

The **Modify operating mode** permission must be set to **Yes**.

Procedure

- From the **Configuration** tab, the **Monitoring** tab, or the **Scheduling** tab, given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

A status popup message appears.

7.5.9 Restore a Message Archive Backup

Purpose

This procedure enables you to restore message archives manually. The restore procedure imports the contents of an archive backup file into the Alliance Access database. The backup archive file remains in the backup directory.

Note You can restore and view an archive backup from a previous release of Alliance Access even if the current release of 7.1.10 runs on an operating system that is different from the operating system with which the archive backup was made.

Users and permissions

To display the configuration details and the status of the last message archive backup, your operator profile must have this entity:

- **System Management**

To restore a message archive backup, your operator profile must have this action:

- **System Management / Restore**

Security officers can restore backups.

Procedure

1. From the **Configuration** tab, click **Restore**.

The **Restore Archives** window opens.

2. In the **Backup Directory** field, verify the backup path.

Click **Change Location** and modify the path in the **Change Location** window if needed.

3. Select the **Overwrite Existing Archives** check box, if you want to replace the last archive.

4. In the **Archives to be Restored/Available** list, select the backups to restore.

5. Click **Restore**.

The **Restore Archives** window closes.

If an archive already exists in the database, an error message appears.

A status popup message appears.

The information message informs you about the status of the restore request. If the request is accepted, the restore process is launched as a background task. You have to monitor the status of the last restore from the **Monitoring** tab.

7.5.10 Monitor a Message Archive Backup

Purpose

This procedure enables you to monitor the status of the last archive backup or the last restore process.

Users and permissions

To display the configuration details and the status of the last message archive backup, your operator profile must have this action:

- **System Management / Backup**

Security officers can monitor backups.

Procedure

1. Click the **Monitoring** tab.
2. You can click  to refresh the list.

8 User Management

Overview

To use Alliance Access, users must have a profile that defines the user's role and entitlements to access the available functionality. SWIFT refers to the end users of Alliance Access as operators. SWIFT delivers Alliance Access with predefined profiles. The left security officer and right security officer assign the profiles to the Alliance Access users. Security officers can modify the profiles or create new ones.

There are three possible authentication methods for users:

- local authentication (default authentication method)
- one-time password
- LDAP (Lightweight Directory Access Protocol) authentication

Each user authentication method can be configured individually.

Local authentication

Alliance Access enables left security officers and right security officers to assign profiles to operators. Operators can use only the BICs that the specified operator profiles allow. Alliance Access uses these operator profiles to segregate the access to message data. The operator profiles govern access for individual Alliance Access users to the entities that control message delivery. The use of operator profiles enables a customer to ensure that the users can only access their own message data.

One-time passwords

If you choose to use one-time passwords, then you need the following components:

- a secure, PIN-protected hardware token that generates one-time passwords
- an authentication server that authenticates the one-time passwords

You can use any authentication server that supports the RADIUS user authentication protocol. You must configure the authentication server before you can use one-time passwords.

Note You must provide the necessary secure hardware tokens and the authentication server.

Alliance Access implementation for one-time passwords includes the following functions for all authentication servers that support the RADIUS protocol:

- Alliance Access forwards the user name and the one-time password to the authentication server for validation.
- Alliance Access locks user accounts after a predefined number of invalid one-time password attempts.

SWIFT provides no support for the RADIUS challenge-response authentication feature.

LDAP authentication

With LDAP authentication, the user authentication (user name and password verification) is provided by an external LDAP server.

Users are still created in the Alliance Access server, but are mapped to an LDAP identifier used for the verification of the credentials. Profiles and units are assigned to users on the Alliance Access server.

Note You must provide the necessary LDAP server.

The administrator must configure the connection to the existing LDAP server, and can optionally configure a backup LDAP server.

Alliance Access can communicate with any existing LDAP server provided by the customer, that is compliant to the LDAP v3 protocol.

8.1 Authentication Server Groups

8.1.1 Authentication Servers and One-Time Passwords

Primary and secondary authentication servers

You must configure at least one authentication server group with a primary authentication server before you can start using one-time passwords. You can also use a secondary authentication server. In this case, the configuration of the primary authentication server must be approved before you can approve the configuration of the secondary server. If two authentication servers are configured and approved, then when the primary server cannot be connected to or if the connection is lost, a switch from the primary authentication server to the secondary one occurs.

One-time passwords for operators

The usage of one-time passwords is set per operator. It is activated when creating the operator.

One-time passwords for security officers

The usage of a one-time password for the security officers is set by the security parameter **Sec Officer One Time Pwd**. The default value of this parameter is **No**.

The value of this parameter applies to both security officers. To activate the usage of one-time password, the parameter must be set to **Yes** and approved by both security officers. As long as the change is not approved by both security officers, they still have to log on using their user-defined password. Before setting this parameter to **Yes** and approving, both security officers must ensure the **Sec Officer OTP Srv Group** parameter is correctly set and approved.

When the parameter is changed to **No**, and subsequently approved by both security officers, the left security officer and the right security officer have to use the master passwords at the next signon, and must change their password as if it was the first login. As long as the change is not approved by both security officers, they still have to log on using their one-time password.

The left security officer and the right security officer have a unique name that is shared over all Alliance Access instances. They can use the same hardware token for signing on to these instances.

Authentication server group for security officers

The authentication server group is set by the security parameter **Sec Officer OTP Srv Group**. Both security officers must be configured to use one-time password through the **Sec Officer One Time Pwd** security parameter.

The **Sec Officer OTP Srv Group** security parameter is a text field and by default the value is empty. Changes to this parameter take effect immediately.

Both the **Sec Officer One Time Pwd** and the **Sec Officer OTP Srv Group** security parameters need to be updated and approved before the security officers attempt to log in to the authentication server.

Recommendations about one-time passwords

The authentication server cannot differentiate between operators who are defined with the same name on different Alliance Access (or even Alliance Gateway) instances. Therefore, operators must have a unique name for each instance, or each instance must have its own dedicated authentication server.

Because an operator that is defined for using one-time passwords can no longer sign in if Alliance Access cannot connect to the authentication server (thereby rendering Alliance Access inaccessible), you must not define all of your operators as needing one-time passwords. This can be achieved by defining a number of operators as not using one-time passwords that are capable of performing day-to-day activities (such as connecting to the SWIFT network).

As of Alliance Access 7.1.10, there is a fallback mechanism for the left security officer and the right security officer if there are issues with the authentication server configuration or connectivity. If the authentication server is unavailable or badly configured, then every attempt to log in as the left security officer or the right security officer will be counted as a failed password attempt, even if the password provided is the correct one. To access Alliance Access, the left security officer and the right security officer can use their private password to log in. They must be careful to not try to enter their one-time password too many times before they try their private password, because the account will become time-disabled and their private password will be rejected as well.

Note If an operator account becomes time-disabled because of too many password attempts, the operator must wait at least 10 minutes before trying to enter the password again.

Both Alliance Access and the authentication server have a policy (set of security parameters on Alliance Access) concerning the maximum number of consecutive wrong passwords before an operator is disabled:

- The configured maximum number of consecutive wrong passwords must be the same on both Alliance Access and the authentication server.
- If you have to enable an Alliance Access operator after they are disabled because of using a wrong password, then the number of consecutive wrong passwords for this operator must be reset on the authentication server at the same time.

Retry and failover mechanism

When a request is sent to an authentication server (originated by an operator login configured to use one-time passwords):

- Alliance Access attempts to connect to the primary server five times. The attempts are made every six seconds.
- If still failing, Alliance Access will fail over to the secondary authentication server (if one is defined) and will send a new request. This is logged via event 2134: Authentication Server switched. Active authentication server changes from <server1:port> to 10<server2:port>.
- Alliance Access attempts to connect to the secondary server four times. The attempts are made every six seconds.

- If still failing, it will then fail over to the primary authentication server. Event 2134 and event 2135 are logged: Not possible to communicate with the Authentication Server(s). Timeout.

For subsequent login attempts (without establishing a connection to either of the servers in the meantime):

- Alliance Access attempts to connect to the primary server five times. The attempts are made every six seconds.
- Alliance Access attempts to connect to the secondary server four times. The attempts are made every six seconds.
- Event 2135 is logged.

8.1.2 Authentication Server Groups Page

Content

The **Authentication Server Groups** page displays information about the primary and secondary authentication servers. If you need to use one-time passwords, then at least one authentication server should be configured.

The **Authentication Server Groups** page contains these elements:

- Details of the available authentication servers

See "Details" on page 220

Display

Authentication Server Groups						
Authentication Server Groups						
Change View		Report		Add		Delete
<input type="checkbox"/>	Server Group Name	Description	Status	Primary Server	Primary Port	Secondary Server Secondary Port

Details

Column	Description
Server Group Name	The name of the authentication server group.
Description	The description of the authentication server group
Status	<p>The status of the authentication server configuration. Both the left security officer and the right security officer must approve the changes to the current configuration for it to become active.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Unapproved • Waiting RSO Approval • Waiting LSO Approval • Approved

Column	Description
Primary Server	The host name or the IP address of the primary authentication server. The maximum length of the host name is 255 characters.
Primary Port	The port number local to the Alliance Access host. This port should be the same for both authentication servers.
Secondary Server	The host name or the IP address of the secondary authentication server. The maximum length of the host name is 255 characters.
Secondary Port	The port number local to the Alliance Access host. This port should be the same for both authentication servers.

8.1.3 Authentication Server Group Details Window

Content

The **Authentication Server Group Details** window contains these elements:

- Details of the authentication server selected

See "Details" on page 222

Display

The screenshot shows the 'Authentication Server Group Details' window. The 'General' tab is active. The 'Server Group Name' field contains 'OTP_GROUP1'. The 'Description' field contains 'Default One-Time Password server group'. The 'Status' field shows 'Approved'. At the bottom of the window are buttons for 'Close', 'Report', 'Clear', 'Previous', and 'Next'.

Authentication Server Group Details

General Primary Server Secondary Server [Help](#)

Current Configuration		Future Configuration	
Host Address	behs0046	Host Address	behs0046
Key Left	*****	Key Left	*****
Key Right	*****	Key Right	*****
Show Clear Text	<input type="checkbox"/>	Show Clear Text	<input type="checkbox"/>
Port Number	1812	Port Number	1812
Local Port Number	0	Local Port Number	0

[Close](#) [Report](#) [Clear](#) [Previous](#) [Next](#)

Authentication Server Group Details

General Primary Server Secondary Server [Help](#)

Current Configuration		Future Configuration	
Host Address		Host Address	
Key Left		Key Left	
Key Right		Key Right	
Show Clear Text	<input type="checkbox"/>	Show Clear Text	<input type="checkbox"/>
Port Number		Port Number	
Local Port Number		Local Port Number	

[Close](#) [Report](#) [Previous](#) [Next](#)

Details

Field	Description
Server Group Name	The name of the authentication server group. This name must be unique within the Alliance Access instance.
Description	The description of the authentication server group.
Status	<p>The status of the authentication server configuration. Both the left security officer and the right security officer must approve the changes to the current configuration for it to become active.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Unapproved • Waiting RSO Approval • Waiting LSO Approval • Approved

Field	Description
Current Configuration	<p>The current configuration of the authentication server group selected:</p> <ul style="list-style-type: none"> Host Address: Hostname or IP address of the authentication server. Key Left: Left part of the secret. The left part of the secret consists of 16 characters. These characters must be US-ASCII encoded characters 32 through 126. Key Right: Right part of the secret. The right part of the secret consists of 16 characters. These characters must be US-ASCII encoded characters 32 through 126. Show Clear Text: If you select this check box, then the left key or right key appear in clear. Port Number: Port number to reach the authentication server. Local Port Number: Port number local to the Alliance Access host. The local port number can be different for both authentication servers.
Future Configuration	<p>The future configuration of the authentication server group selected. See the explanations given for the Current Configuration.</p>

8.1.4 Modify the Configuration of an Authentication Server Group

Purpose

This procedure enables you to modify the configuration of an authentication server group.

Users and permissions

To display the list or the details of authentication servers and modify the configuration, your operator profile must have this action:

- Security Definition / Auth Server Config**

Security officers can modify the configuration.

Left secrets can be displayed by left security officers or operators with "left" entitlements and permissions. Right secrets can be displayed by right security officers or operators with "right" entitlements and permissions.

For operators, one of the following permissions for the **Auth Server Config** action must be set to Yes:

- Left Secret**
- Right Secret**

Procedure

- From the list of authentication servers, click the row of the authentication server that you want to configure.

The **Authentication Server Group Details** window opens.

2. In the **Host Address** field of the **Future Configuration** area, type the hostname or the IP address of the authentication server.
3. In the **Port Number** field, type the port number to reach the authentication server. Enter a value between 1024 and 65535.
4. In the **Local Port Number** field, type the port number local to the Alliance Access host. Enter a value between 1024 and 65535. The local port number can be different for both authentication servers.
5. Click **Save**. You can only save your changes if at least the **Host Address**, **Port Number**, and **Local Port Number** fields contain a value.
The **Status** field displays the current status which is **Unapproved**.
A status popup message appears.
6. Click **Close**.
The **Authentication Server Group Details** window closes.

8.1.5 Approve the Configuration of an Authentication Server Group

Purpose

This procedure enables you to approve the configuration of an authentication server group.

Users and permissions

Only security officers can approve the configuration of an authentication server. Both the left security officer and the right security officer must approve the changes to the current configuration for it to become active.

Standard operators cannot approve the configuration.

Primary and secondary authentication servers

If you are using a secondary authentication server, the configuration of the primary authentication server has to be approved before you can approve the configuration of the secondary server.

Password compliancy rules and recommendations

The left and right parts of the secret each consist of 16 characters. These characters must be US-ASCII encoded characters 32 through 126.

Each part must also comply with the following complexity rules:

- It must contain at least one upper-case and one lower-case alphabetic character.
- It must contain at least one number.
- A character cannot be repeated more than half of the length minus one.

Secrets are stored encrypted within Alliance Access. They have a lifetime of two years, after which they expire.

The following recommendations must be observed for the secrets:

- If you define two authentication servers, then the secrets must be different.
- The secret keys must be renewed every 3 to 6 months.
- An implementation of network access control (firewalls, ACL's) or segregation of message flow (main and management flow) can be considered.

Procedure

1. From the list of authentication servers, click the row of the authentication server that you want to approve.

The **Authentication Server Group Details** window opens.

The **Status** field displays the current status which is **Unapproved**.

Depending on your rights, either the **Key Left** or **Key Right** field is displayed.

Note If you select the **Show Clear Text** check box, then the characters appear in clear.

2. Enter either the left part or the right part of the secret. Each part consists of 16 characters.
3. Click **Approve** to approve the changes.

The **Status** field changes to **Waiting LSO Approval** or **Waiting RSO Approval**.

A status popup message appears.

4. Click **Save**.
5. Click **Close**.

The **Authentication Server Group Details** window closes.

The other security officer must now sign on and approve the changes. When both security officers have approved the changes, the status changes to **Approved** and the **Future Configuration** settings become the **Current Configuration** ones.

8.1.6 Disapprove the Configuration of an Authentication Server Group

Purpose

This procedure enables you to disapprove the configuration of an authentication server group.

Disapproving the future configuration of an authentication server enables you to come back to the previously approved configuration.

Users and permissions

Only security officers can disapprove the configuration of an authentication server group.

Standard operators cannot disapprove the configuration.

Procedure

1. From the list of authentication servers, click the row of the authentication server for which you want to disapprove the configuration.

The **Authentication Server Details** window opens.

The **Status** field displays the current status which is Waiting LSO Approval or Waiting RSO Approval.

2. Click **Disapprove** to disapprove the configuration and come back to the previously approved configuration.

A status popup message appears.

3. Click **Close**.

The **Authentication Server Group Details** window closes.

The **Status** field changes to Approved and the previously approved configuration is restored.

8.2 LDAP Server Groups

8.2.1 LDAP Authentication

Why use LDAP authentication

LDAP allows institutions to use any existing user directories to control access to a range of Alliance products. LDAP directories can be used to authenticate (username and password) users defined in those Alliance products.

How LDAP authentication works

LDAP is used to authenticate the users only (username and password verification). The users are created on the Alliance Access server, but can be mapped to an LDAP identifier used for verification of the credentials. Profiles and units are assigned to users on the Alliance Access server.

The following process occurs when LDAP authentication is used:

1. A user logs on to Alliance Web Platform with the local operator name and the LDAP password.
2. The Alliance Access server receives the logon request and checks whether the operator is authenticated locally, through one-time passwords or through LDAP.
3. If the operator is authenticated through LDAP, then the operator name is mapped to an LDAP identifier, if present. Otherwise, the operator name is forwarded to the LDAP server.
4. The password and the LDAP identifier or operator name are forwarded to the LDAP server.
5. The LDAP server authenticates the user.
6. If the user is authenticated successfully, then the user can log on using the permissions assigned to him in Alliance Access.

What you must set up for LDAP authentication

Configuring Alliance Access for LDAP authentication includes the following:

- 4-eyes approval mechanism requiring both security officers (left security officer and right security officer), or operators with left and right **Approve LDAP** permission (**Security Definition** entity).
- At least one LDAP directory must be available. A primary LDAP server must be configured in Alliance Access. A secondary LDAP server may be configured.
- The host name and port number of the LDAP authentication server or servers must be known to Alliance Access.

Optionally, you can set up the following:

- a secured connection to the LDAP server
- the user DN and password used to connect to the LDAP server (not needed if the LDAP server supports anonymous access)

8.2.2 LDAP Server Groups Page

Content

The **LDAP Server Groups** page contains these elements:

- Details of the available LDAP servers

See "Details" on page 227

Display

LDAP Server Groups

LDAP Server Groups							Rows in list: 1, in selection: 0			
Change View				Report			Add	Delete	Rows in list: 1, in selection: 0	
	Name	Description	Status	Primary Server	Primary Port	Secondary Server	Secondary Port			
	LDAP_GROUP1	Default LDAP server group	Approved	behs0046	389					

Details

Column	Description
Name	The name of the LDAP server group.
Description	The description of the LDAP server group
Status	<p>The status of the LDAP server configuration. Both the left security officer and the right security officer or operators with the necessary entitlements and permissions must approve the changes to the current configuration for it to become active.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Unapproved • Waiting RSO Approval • Waiting LSO Approval • Approved

Column	Description
Primary Server	The host name or the IP address of the primary server. The maximum length of the host name is 255 characters.
Primary Port	The port number local to the primary server.
Secondary Server	The host name or the IP address of the secondary server. The maximum length of the host name is 255 characters.
Secondary Port	The port number local to the secondary server.

8.2.3 LDAP Server Group Details Window

Content

The **LDAP Server Group Details** window contains these elements:

- Details of the LDAP server group selected

See "Details" on page 229

Display

The screenshot shows the 'LDAP Server Group Details' window. The 'General' tab is active. The 'Server Group Name' field contains 'LDAP_GROUP1'. The 'Description' field contains 'Default LDAP server group'. The 'Status' field shows 'Approved'. At the bottom, there are buttons for 'Close', 'Report', 'Clear', 'Previous', and 'Next'.

LDAP Server Group Details

Help

General Primary Server Secondary Server

Current Configuration

Host Address	behs0046
Connection Security	<input type="checkbox"/>
Port Number	389
Connect DN	cn=manager,o=swift.com
Configure Connect Password	<input checked="" type="checkbox"/>
Connect Password	*****
Confirm Connect Password	
User DN	ou=SAG operators,ou=Interface Products
User Object Class	person
User Name Attribute	uid

Future Configuration

Host Address	behs0046
Connection Security	<input type="checkbox"/>
Port Number	389
Connect DN	cn=manager,o=swift.com
Configure Connect Password	<input checked="" type="checkbox"/>
Connect Password	*****
Confirm Connect Password	
User DN	ou=SAG operators,ou=Interface Products
User Object Class	person
User Name Attribute	uid

Buttons: Close, Report, Clear, Previous, Next

LDAP Server Group Details

Help

General Primary Server Secondary Server

Current Configuration

Host Address	
Connection Security	<input type="checkbox"/>
Port Number	
Connect DN	
Configure Connect Password	<input type="checkbox"/>
Connect Password	
Confirm Connect Password	
User DN	
User Object Class	
User Name Attribute	

Future Configuration

Host Address	
Connection Security	<input type="checkbox"/>
Port Number	
Connect DN	
Configure Connect Password	<input type="checkbox"/>
Connect Password	
Confirm Connect Password	
User DN	
User Object Class	
User Name Attribute	

Buttons: Close, Report, Approve, Previous, Next

Details

Field	Description
Server Group Name	The name of the LDAP server group. This name must be unique within the Alliance Access instance.
Description	The description of the LDAP server group

Field	Description
Status	<p>The status of the LDAP server group configuration. Both the left security officer and the right security officer or operators with the necessary entitlements and permissions must approve the changes to the current configuration for it to become active.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Unapproved • Waiting RSO Approval • Waiting LSO Approval • Approved
Current Configuration	<p>The current configuration of the LDAP server group selected:</p> <ul style="list-style-type: none"> • Host Address: Hostname or IP address of the LDAP server • Connection Security: If you are using a secured connection to the LDAP server, this check box should be selected • Port Number: Port number to reach the LDAP server. The value is between 1 and 65535. • Connect DN: User DN (250 characters maximum) to connect to the LDAP server. This field is optional. • Configure Connect Password: If you select this check box, then the connect password becomes editable • Connect Password and Confirm Connect Password: Password (100 characters maximum) to connect to the LDAP server • User DN: DN of the entry point in the user directory (250 characters maximum) In the LDAP search request, Alliance Access specifies that the whole subtree must be searched, starting from the DN specified in User DN. • User Object Class: Type or class of the user nodes within the directory (32 characters maximum). This is useful if there are different types of nodes in the directory (that is, not only users). This field is optional. • User Name Attribute: Name of the attribute containing the user name that is used during the logon operation. This field can contain 32 characters maximum.
Future Configuration	<p>The future configuration of the selected LDAP server.</p> <p>See the explanations given for the Current Configuration.</p>

8.2.4 Modify the Configuration of an LDAP Server Group

Purpose

This procedure enables you to modify the configuration of an LDAP server group.

Users and permissions

To display the list or the details of LDAP server groups and modify the configuration, your operator profile must have this action:

- **Security Definition / Configure LDAP**
- **Security Definition / Approve LDAP**

Security officers can modify the configuration.

Primary and secondary LDAP servers

You must configure the primary LDAP server before you can start using LDAP authentication. You can use a secondary LDAP server. In this case, the configuration of the primary LDAP server has to be approved before you can approve the configuration of the secondary server. See "Approve the Configuration of an LDAP Server Group" on page 232. If two LDAP servers are configured and approved, then when the primary server cannot be connected to or if the connection is lost, a switch from the primary LDAP server to the secondary one occurs.

Procedure

1. From the list of LDAP servers, click the row of the LDAP server that you want to configure.
The **LDAP Server Group Details** window opens.
2. In the **Host Address** field of the **Future Configuration** area, type the hostname or the IP address of the LDAP server.
3. In the **Port Number** field, type the port number to reach the LDAP server. Enter a value between 1 and 65535.
4. Select the **Connection Security** check box if you want to secure the connection to the LDAP server.
If your LDAP server supports anonymous access, then you do not need to provide a DN and password.
5. If you selected **Connection Security**, then in the **Connect DN** field, specify the user DN (250 characters maximum) to connect to the LDAP server.
6. If you select the **Configure Connect Password** check box, then the connect password becomes editable.
7. In the **Connect Password** field, type the password (100 characters maximum) to connect to the LDAP server.
8. Type the password again in the **Confirm Connect Password** field.
9. In the **User DN** field, type the DN of the entry point in the user directory (250 characters maximum).
10. In the **User Object Class**, you can optionally specify the type or class of the user nodes within the directory (32 characters maximum).
11. In the **User Name Attribute** field, type the name of the attribute containing the user name that is used during the logon operation (32 alphanumeric characters maximum).
12. Click **Save**. You can only save your changes if at least the **Host Address**, **Port Number**, **User DN**, **User Object Class**, and **User Name Attribute** fields contain a value.
The **Status** field displays the current status which is **Unapproved**.

A status popup message appears.

13. Click **Close**.

The **LDAP Server Group Details** window closes.

Note If you click **Clear**, the **Future Configuration** fields are reset. If the configuration is approved after the reset, then the server is no more used for authentication.

8.2.5 Approve the Configuration of an LDAP Server Group

Purpose

This procedure enables you to approve the configuration of an LDAP server group.

Users and permissions

To display the list or the details of LDAP servers, your operator profile must have this action:

- **Security Definition / Configure LDAP**

To approve the configuration of an LDAP server, your operator profile must have this action:

- **Security Definition / Approve LDAP**

Security officers can approve the configuration.

Left secrets can be displayed by left security officers or operators with "left" entitlements and permissions. Right secrets can be displayed by right security officers or operators with "right" entitlements and permissions.

For operators, the **Approve Left or Right** part permission for the **Approve LDAP** action must be set to **Left** or **Right**.

Primary and secondary LDAP servers

If you are using a secondary LDAP server, the configuration of the primary LDAP server has to be approved before you can approve the configuration of the secondary server.

Procedure

1. From the list of LDAP servers, click the row of the LDAP server that you want to approve.

The **LDAP Server Details** window opens.

The **Status** field displays the current status which is **Unapproved**.

2. Click **Approve** to approve the changes.

The **Status** field changes to **Waiting LSO Approval** or **Waiting RSO Approval**.

A status popup message appears.

3. Click **Save**.

4. Click **Close**.

The **LDAP Server Group Details** window closes.

The other security officer or operator with the necessary entitlements and permissions must now sign on and approve the changes. When both security officers or operators have approved the

changes, the status changes to Approved and the **Future Configuration** settings become the **Current Configuration** ones.

8.2.6 Disapprove the Configuration of an LDAP Server Group

Purpose

This procedure enables you to disapprove the configuration of an LDAP server group.

Disapproving the future configuration of an LDAP server group enables you to come back to the previously approved configuration.

Users and permissions

To display the list or the details of LDAP servers, your operator profile must have this action:

- **Security Definition / Configure LDAP**

To disapprove the configuration of an LDAP server, your operator profile must have this action:

- **Security Definition / Approve LDAP**

Security officers can disapprove the configuration.

Left secrets can be displayed by left security officers or operators with "left" entitlements and permissions. Right secrets can be displayed by right security officers or operators with "right" entitlements and permissions.

For operators, the **Approve Left or Right part** permission for the **Approve LDAP** action must be set to **Left or Right**.

Procedure

1. From the list of LDAP servers, click the row of the LDAP server for which you want to disapprove the configuration.

The **LDAP Server Group Details** window opens.

The **Status** field displays the current status which is **Waiting LSO Approval** or **Waiting RSO Approval**.

2. Click **Disapprove** to disapprove the configuration and come back to the previously approved configuration.

A status popup message appears.

3. Click **Close**.

The **LDAP Server Group Details** window closes.

The **Status** field changes to **Approved** and the previously approved configuration is restored.

8.2.7 Secure an LDAP Connection

Purpose

You can use SSL to secure the connection to an LDAP authentication server. The LDAP server must have SSL support enabled. The SSL certificate installed on the LDAP server can be either a self-signed certificate or a certificate signed by a Certification Authority.

The keystore that LDAP uses on Alliance Access must trust either the self-signed SSL certificate or the Certification Authority certificate.

Note You must restart the Alliance server after adding the certificate to the keystore.

To add a certificate, perform the applicable procedure that follows.

Procedure on AIX

1. Log on to Alliance Access as Alliance administrator.
2. Launch the **gsk7ikm** graphical application.

Running the **gsk7ikm** graphical application requires the **JAVA_HOME** environment variable to be defined. Set the **JAVA_HOME** environment variable in an Alliance Access **Xterm** window by typing `export JAVA_HOME=<the java path>`. Usually, `<the java path>` looks like `/usr/java14`.

If you use an X-Window-based tool to connect remotely to the Alliance Access server, make sure the **DISPLAY** environment variable is set to the display of your desktop. Also, if there is a firewall in use between Alliance Access and your desktop, make sure that you configure the firewall rules to allow X-Window communication.

3. Create a new keystore in the **\$ALLIANCE/data/ldap** directory.

Select **CMS** for Key database type and enter `key.kdb` in the **File Name** field.

The **Password Prompt** opens.

4. Type a password and a confirmation of the password, and select the **Stash the password to a file** option.
5. Click **OK**.
6. Add either the self-signed SSL certificate or the Certification Authority certificate to the keystore.

Procedure on Linux

1. As the Alliance Access owner, create a file named **Idaprc** in **<ALLIANCE>/data/ldap** directory.
2. Define the SSL/TLS to secure the connection. The following rules apply while creating or updating the file:
 - The file must be owned by and readable by the Alliance Access owner.
 - The file must have the same format as **Idap.conf** (described in the man page).
 - The file must contain only SSL/TLS specific options. Alliance Access will handle the other options (URI, DNs, HOST, PORT...).
 - All paths in the file must be absolute.

Here is an example:

```
TLS_CACERT      /berx012_i1/Alliance/Access/data/ldap/behs0046.crt
TLS_CACERTDIR  /berx012_i1/Alliance/Access/data/ldap
TLS_REQCERT    never
```

Procedure on Solaris

1. Log on to Alliance Access as Alliance administrator.
2. Open a Korn shell.

3. Use the `certutil` command-line application to create a new keystore in the **\$ALLIANCE/data/ldap** directory:
`/usr/sfw/bin/certutil -N -d $ALLIANCE/data/ldap`
4. Add either the self-signed SSL certificate or the Certification Authority certificate to the keystore.
`/usr/sfw/bin/certutil -A -n "<certificate_alias>" -i <certificate_file> -a -t`
Replace `<certificate_alias>` with the name of the certificate.
Replace `<certificate_file>` with the path and filename of the certificate.
 - To list the certificates in the keystore, enter:
`/usr/sfw/bin/certutil -L -d $ALLIANCE/data/ldap`
 - To delete a certificate from the keystore, enter:
`/usr/sfw/bin/certutil -D -n "<certificate_alias>" -d $ALLIANCE/data/ldap`

Procedure on Windows

1. Log on to Alliance Access as Alliance administrator.
2. Open a DOS command prompt.
3. Enter `mmc` to launch the Microsoft Management Console application.
The Microsoft Management Console window opens.
4. Use **File > Open** to open the file `<WINDOWS>/system32/certmgr.msc`, where you replace `<WINDOWS>` with the path to the Windows directory on the Alliance Access server.
The **Certificates** window opens.
5. Select the **Trusted Root Certification Authorities > Certificates** store.
6. Select **Action > All Tasks > Import**.
The **Certificate Import Wizard** opens.
7. Follow the instructions in the **Certificate Import Wizard** to import either the self-signed SSL certificate or the Certification Authority certificate in the **Trusted Root Certification Authorities** certificate store.
A **Security Warning** message opens.
8. Click **Yes**.
A **Certificate Import Wizard** message opens that confirms the successful import of the certificate.
9. Click **OK**.
10. Close the **Certificates** window.
A **Microsoft Management Console** dialog box opens.
11. Click **Yes**.
The **Certificates** window closes.

8.3 Units

8.3.1 Units: Definition

What is a unit?

A unit is a logical grouping to which operators can belong, and to which messages can also be assigned. A unit can correspond to a division, department, office, or some other grouping within an organisation.

If a message is assigned to a unit, then only operators who belong to the same unit can display or modify the message. Units therefore provide a method of controlling which operators can access which messages.

Operators who are allowed to use operator-related functions (such as modifying operator definitions) can be restricted to performing these functions only on operators who belong to certain units.

8.3.2 Definition of Units and Restrict Functions

Definition of units in Alliance Access Configuration

You can use Alliance Access Configuration to add, modify, or remove units. After a new unit has been added, an operator or a security officer must approve the unit before it can be used with operators. The maximum number of units that can be assigned to an operator is 200.

The use of units makes it easy to divide message processing tasks between different groups of operators. Operators can be members of units. Incoming and outgoing messages can be assigned to units.

Note Units are not applicable for CRnet (CREST) message traffic.

Operator Restrict functions

Security officers can use the **Restrict Functions** security parameter (**Operator** class) to specify whether an operator can perform operator-related actions on operators belonging to any unit, or only on operators that belong to a subset of the same units as the operator performing the action. The default is **No**, which means that an operator with the correct entitlements can open, print, add, modify, approve, or remove operators belonging to any unit. If the parameter is set to **Yes**, then an operator can only use these functions on operators that belong to a subset of the same units as the operator performing the action. The setting of this parameter does not affect the left security officer and right security officer, which always have unrestricted access to operator functions.

If the parameter is set to **Yes**, then the following restrictions apply:

- The operator carrying out operator-related functions can only assign a subset of the units assigned to himself, to another operator.
- An operator A can only display information and use operator-related functions on another operator B, if the set of units assigned to operator B is a subset of the units assigned to the operator A.

For example, if operator Marc belongs to units A, B and C, and operator Luc belongs to units C and D, neither Marc or Luc can display each other's operator details. Operator Dirk, who belongs to units A, B, C, and D, can display the operator details for both Marc and Luc and

use operator-related functions on them. However, neither Marc or Luc can display Dirk's operator details.

Note When the security parameter **Restrict Delegation** is set to Yes, any profile assignments made for units take precedence. This does not affect the left security officer and right security officer.

8.3.3 Units Page

Content

The **Units** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Units** page:
 - See "Details" on page 237
 - See "Functions" on page 22
- Details of the available units
 - See "Details" on page 237
- Functions that enable you to manage the units
 - See "Functions" on page 238

Display

Units				Rows in list: 2 , in selection: 1													
Filtering Criteria				Previous	Next												
Name		Status		Submit	Report												
<input type="text"/>		<input type="button"/>		<input type="button"/>	<input type="button"/>												
<table border="1"> <thead> <tr> <th></th> <th>Name</th> <th>Description</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>None</td> <td>System generated unit</td> <td>Approved</td> </tr> <tr> <td><input type="checkbox"/></td> <td>newUnit</td> <td></td> <td>Approved</td> </tr> </tbody> </table>					Name	Description	Status	<input checked="" type="checkbox"/>	None	System generated unit	Approved	<input type="checkbox"/>	newUnit		Approved	<input type="button"/> Previous <input type="button"/> Next	
	Name	Description	Status														
<input checked="" type="checkbox"/>	None	System generated unit	Approved														
<input type="checkbox"/>	newUnit		Approved														

Details

Units		
Field	Description	Filtering criteria
Name	The name of the unit. For filtering, the wildcard characters % and _ enable you to search for a group of units.	✓
Description	The description of the unit	
Status	The status of the unit These are the possible values: <ul style="list-style-type: none"> • Approved: to search only for approved units • Unapproved: to search only for unapproved units 	✓

Functions

Function	Description
Add	Enables you to add a unit Procedure:"Add a Unit" on page 238
Approve	Enables you to approve a unit Procedure:"Approve a Unit" on page 240
Delete	Enables you to delete a unit. Only unapproved units can be deleted. Procedure:"Delete a Unit" on page 239

8.3.4 Units Details Window

Content

The **Units Details** window contains these elements:

- Details of the unit selected
See "Details" on page 238

Display

The screenshot shows a window titled "Unit Details" with a "Help" button in the top right. The main area contains three input fields: "Name" with the value "None", "Description" with the value "System generated unit", and "Status" with the value "Approved". At the bottom are buttons for "Close", "Report", "Previous", and "Next".

Details

Field	Description
Name	The name of the unit
Description	The description of the unit
Status	<p>The status of the unit. These are the possible values:</p> <ul style="list-style-type: none"> • Unapproved • Approved

8.3.5 Add a Unit

Purpose

This procedure enables you to add a unit.

Users and permissions

To display the list or the details of units, or filter the list, your operator profile must have this entity:

- **Security Definition**

To add or modify units, your operator profile must have these actions:

- **Security Definition / Add Unit**
- **Security Definition / Mod Unit**

Security officers can only display the details.

Procedure

1. From the list of units, click **Add**.

You can also add a unit using the characteristics of an existing unit. Select the check box of a unit and click **Add As**.

The **Unit Details** window opens.

2. In the **Name** field, type the name of the unit.
3. In the **Description** field, type a description (24 characters maximum).
4. Click **Save**.

A status popup message appears.

5. Click **Close**.

The **Unit Details** window closes.

The new unit has the status **Unapproved**.

You must approve the unit before it can be assigned to an operator or message instance.

Once created, only the description of a unit can be modified.

8.3.6 Delete a Unit

Purpose

This procedure enables you to delete a unit.

Users and permissions

To display the list or the details of units, or filter the list, your operator profile must have this entity:

- **Security Definition**

To delete units, your operator profile must have this action:

- **Security Definition / Rem Unit**

Overview

Only unapproved units can be deleted.

Procedure

1. From the list of units, select the check box for a unit in the left column.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

8.3.7 Approve a Unit

Purpose

This procedure enables you to approve a unit.

Once a unit has been approved, it cannot be disapproved or deleted.

Users and permissions

To display the list or the details of units, or filter the list, your operator profile must have this entity:

- **Security Definition**

To approve units, your operator profile must have this action:

- **Security Definition / Approve Unit**

Procedure

1. From the list of units, click the row of the unit that you want to approve.

The **Unit Details** window opens.

The **Status** field displays the current status which is **Unapproved**.

2. Click **Approve** to approve the unit.

The **Approve Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

The **Status** changes to **Approved**.

8.4 Operator Profiles

8.4.1 Operator Profiles: Definition

What are operator profiles?

Alliance Access consists of a number of entities. The security officers in your institution are responsible for deciding which entities that you can use. The security officers do this by creating an operator definition for each Alliance Access. As part of this definition, the security officers assign an Alliance Access profile to operators.

An operator profile defines:

- The entities that an operator is allowed to use. When an operator signs on to Alliance Access, only the nodes for entities that the operator can use are displayed in the tree view.
- The entitlements to use actions (functions) within a particular entity.
- The permissions associated with an entitlement. Security officers can use permissions to give greater control over sensitive actions.

8.4.2 Profiles Assignment

Operator profiles

The operator profile assigned to you depends on your job role. Your profile determines the menus, menu options, windows, and available choices which are displayed on the screen when you sign on to Alliance Access.

Any number of operators can be given the same profile, so that the duties which involve Alliance Access can be shared within your institution. If an operator has a combination of responsibilities, then more than one profile can be assigned to the operator, provided there is no conflict between the entitlements and the permissions in one profile and those in another.

Alliance Access is delivered with various default profiles (pre-defined profiles) that security officers can assign to new operators. Each profile corresponds to a specific user role. If none of these profiles provide the required Alliance Access entitlements, then your security officers can define new operator profiles. They can create a completely new profile, or use an existing profile as a template.

An operator profile cannot be modified while it is in use (that is, if any operator who has been assigned that particular profile is currently signed on). Any changes to an operator profile automatically cause the operators that use it to become unapproved. Following such changes, all operators using that profile must be reapproved by both security officers (or by operators with the appropriate entitlement).

Security officers' profiles and security-related entitlements

Security officers (left security officer and right security officer) have a specific set of entitlements assigned to them by Alliance. Both security officers have the same operator profile. This profile cannot be displayed, modified, or removed.

Security officers can assign virtually any entitlement or permission to other operators (including those functions denied to security officers). All security-related functions of the security officers can be assigned to other operators, except for the entitlement to reset the other security officer's password, and the entitlement to modify security parameters. Most of the security parameters relate to password control. These two entitlements are unique to the left security officer and the right security officer, and cannot be assigned to other operators.

8.4.3 Upgrading Alliance Access Profiles

Overview

When upgrading Alliance Access to a new release, all existing profiles are migrated from the upgraded version. In addition, all default profiles for the upgrade are created with a new version prefix. The user may use the new profiles or keep using the migrated ones. Note that the new entities/actions are not added to the migrated profiles.

8.4.4 Operator Profiles Page

Content

The **Operator Profiles** page contains these elements:

- A filtering criterion and filtering functionality that enable you to filter the list entities on the **Operator Profiles** page:
 - See "Details" on page 242
 - See "Functions" on page 22
 - See "Functions" on page 243
- Details of the available operator profiles
See "Details" on page 242
- Functions that enable you to manage the operator profiles
See "Functions" on page 243

Display

The screenshot shows the 'Operator Profiles' page. At the top, there is a 'Filtering Criteria' section with a 'Name' input field, a 'Clear' button, and 'Submit' and 'Report' buttons. Below this is a table titled 'Operator Profiles' with 13 rows selected. The table has columns for 'Name' and other details. The row for 'R7.0_MsgEntry' is highlighted with a gray background and has a checked checkbox in the first column. Other rows include 'NoSDAnoCorr', 'R7.0_Import_Export', 'R7.0_MsgPartner', and 'R7.0_Operator'.

Details

Column	Description	Filtering criterion
Name	The operator profile name The BIC in the operator profile name is the Live BIC.	✓

Functions

Function	Description
Add	Enables you to add an operator profile Procedure: "Add an Operator Profile" on page 244
Delete	Enables you to delete an operator profile Procedure: "Delete an Operator Profile" on page 245

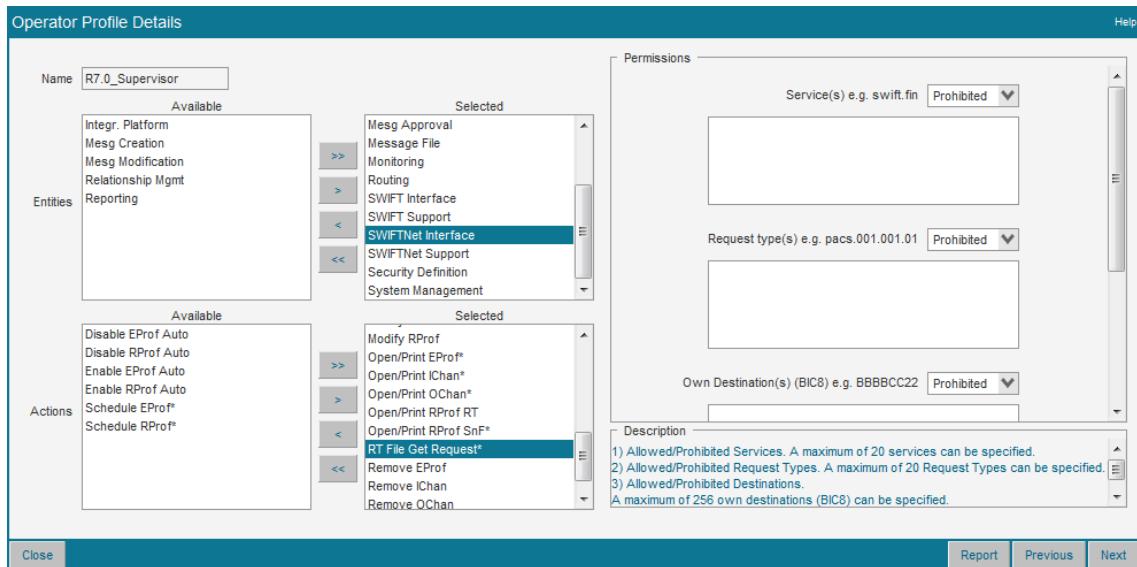
8.4.5 Operator Profile Details Window

Content

The **Operator Profile Details** window contains these elements:

- Details of the operator profile selected
See "Details" on page 243
- Functions that enable you to manage the operator profile
See "Functions" on page 243

Display



Details

Field	Description
Name	The operator profile name
Entities/Available	The entities that can be added to the operator profile
Entities/Selected	The entities selected for the operator profile
Actions/Available	For the entity selected, the actions that can be added to the operator profile
Actions/Selected	For the entity selected, the actions selected for the operator profile
Permissions	The permissions linked to the action selected

8.4.6 Add an Operator Profile

Purpose

This procedure enables you to add an operator profile.

There is no restriction on the number of new profiles that you can add.

Users and permissions

To display the list or the details of operator profiles, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation (Operator** class) security parameter is set to **Yes**, then the list of operator profiles only includes the list of profiles delegated to the operator currently logged in. Security officers can display the full list of profiles.

To add or modify an operator profile, your operator profile must have this action:

- **Security Definition / Add Profile**
- **Security Definition / Mod Profile**

Security officers can add or modify operator profiles.

Procedure

1. From the list of operator profiles, click **Add**.

You can also add an operator profile using the characteristics of an existing profile. Select the check box of an operator profile and click **Add As**.

The **Operator Profile Details** window opens.

2. In the **Name** field, type a name for the operator profile.

This name must be unique and can have up to 20 alphanumeric characters.

3. Select the entities that you want the profile to contain from the **Entities/Available** list.

4. Click an entity in the **Entities/Selected** list to see whether it has related actions.

The actions for the entity are displayed in the **Actions/Available** list.

If an action has an asterisk (*) against it, then it has permissions which you can also change to restrict operators' access to that action.

5. Select the actions that you want the profile to contain from the **Action/Available** list.

6. Click an action with an asterisk (*) in the **Actions/Selected** list.

Permissions are displayed in the **Permissions** area.

Permissions provide a further level of detail about what an operator is entitled to do.

Permissions are usually expressed in one of three ways:

- a **Yes** or **No** flag
- an actual value
- a list of one or more values that are either **Prohibited** or **Allowed**

Prohibited and **Allowed** are used as follows:

If	Then
You select Prohibited	<p>The column to the right of the field can be used to specify a range of values that is prohibited, such as destinations or message types.</p> <p>If you do not enter anything in the column, then nothing is prohibited, that is, everything is allowed.</p> <p>For example, for the Dispose Message action (Mesg Modification entity):</p> <ul style="list-style-type: none"> • If the Bypass Verification CCY/Amount permission is set to Prohibited and the column is empty, this means that the operator can bypass verification for a message of any currency and any amount. • If the permission is set to Prohibited and one or several values are specified in the column, this means that the operator can bypass verification for a message of any currency and any amount, except the ones specified in the column. <p>If the Restrict Delegation security parameter (Operator class) is set to Yes, then new operator profiles must be set up with allowed destinations (BIC8), and existing operator profiles must be changed to include the allowed destinations (BIC8). Prohibited destinations are not supported in this case.</p>
You select Allowed	<p>The column can be used to specify a range of values that is allowed.</p> <p>If you do not enter anything in the column, then nothing is allowed, that is, everything is prohibited.</p> <p>For example, for the Dispose Message action (Mesg Modification entity):</p> <ul style="list-style-type: none"> • If the Bypass Verification CCY/Amount permission is set to Allowed and the column is empty, this means that the operator cannot bypass verification for any message. • If the permission is set to Allowed and one or several values are specified in the column, this means that the operator can bypass verification only for a message of the currency and amount specified in the column.

7. Change the permissions as needed.
 8. Click **Save**.
- A status popup message appears.
9. Click **Close**.

The **Operator Profile Details** window closes.

If you modify a profile that is already assigned to one or more operators, then all operators using that profile become unapproved. The left security officer and right security officer, or operators with the appropriate approval entitlement, must approve the operators again.

8.4.7 Delete an Operator Profile

Purpose

This procedure enables you to delete an operator profile.

Users and permissions

To display the list or the details of operator profiles, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation (Operator class)** security parameter is set to **Yes**, then the list of operator profiles only includes the list of profiles delegated to the operator currently logged in. Security officers can display the full list of profiles.

To delete an operator profile, your operator profile must have this action:

- **Security Definition / Rem Profile**

Security officers can delete operator profiles.

Procedure

1. From the list of operator profiles, select the check box of one or several operator profiles in the left column.
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
A status popup message appears.

8.5 Operators

8.5.1 Operators: Definition

What are operator definitions?

Alliance Access is installed with two predefined operators: the left security officer (LSO) and the right security officer (RSO). The left security officer (LSO) and the right security officer (RSO) are initially used to define other operators. Each operator that you define has a current status which indicates whether the operator can use the system. Until a new operator is approved separately by both security officers, the operator cannot sign on. Before approving a new operator, a security officer must assign profiles to the operator. The name, current status, and assigned profile or profiles that an operator has are called an operator definition.

Alliance Access provides a number of default profiles. When you define a new operator, you can assign one or more of these default operator profiles to the new operator definition. These profiles cannot share the same entities however. If none of the default operator profiles provides the Alliance Access entitlements that you require, then you can either modify an existing profile or create a profile based on an existing one. If you modify an existing operator definition, then the left security officer and the right security officer, or operators with the appropriate approval entitlements, must approve it again before the relevant operator can sign on.

Related information

For examples of default operator profiles, see the Default Printouts on the release media, or on www.swift.com, under Support > [Documentation \(User Handbook\)](#)

8.5.2 Local Security Officers (Service Bureaux)

Setting up local security officers

The service bureau left security officer and right security officer can create "local" security officers for each of the SWIFT user institutions operating through the bureau. To allow this, the security parameter **Restrict Delegation** must be set to Yes. The scope of operator profiles, units, and destinations that a local security officer can assign to other operators can be limited to a subset defined by the left security officer and right security officer. These subsets are designed by the left security officer and right security officer to ensure that operators only have access to their own traffic data, that is by specifying particular profiles, units and destinations. This feature is known as "delegation" and supports the strict segregation of traffic data between institutions using the service bureau.

Note The left security officer and right security officer can create an operator profile which may prohibit or allow access to a selected list of message partners, exit points, routing points, logical terminals, input and output channels, and emission and reception profiles.

This feature is provided by the following actions:

- **Applic. Interface** entity:
 - **Open/Print Partner**
 - **Open/Print Exit Point**
- **Routing** entity: **Open Routing Point**
- **SWIFT Interface** entity: **Own Destination List**
- **SWIFT Support** entity: **Own Destination List**
- **SWIFTNet Interface** entity:
 - **Open/Print EProf**
 - **Open/Print IChan**
 - **Open/Print OChan**
 - **Open/Print RProf SnF**

To activate the delegation feature, the **Restrict Delegation** security parameter must be set to Yes. When this parameter is set to Yes, the **Configure Delegations** button is available to the left security officer and right security officer in the **Operator Details** window.

8.5.3 Operators Page

Content

The **Operators** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Operators** page:
 - See "Operators" on page 248
 - See "Functions" on page 22
- Details of the available operators
See "Operators" on page 248
- Functions that enable you to manage the operators
See "Functions" on page 255

Display

Operators

Filtering Criteria

Name	<input type="text"/>	Profiles	Matching String	<input type="text"/>
Status	<input type="text"/> / <input type="text"/>	Units	Matching String	<input type="text"/>
Authentication Type	<input type="text"/>			

Operators

Rows in list: 20, in selection: 1

<input type="checkbox"/>	Name	Description	Approval Status	Enable Status	Last Login	Authentication
<input type="checkbox"/>	Christine	Christine	Approved	Enabled	09/08/2010 11:10:43	Password
<input checked="" type="checkbox"/>	Diana	Diana	Approved	Enabled	09/08/2010 11:10:43	Password
<input type="checkbox"/>	Francoise	Francoise	Approved	Enabled	09/08/2010 11:10:43	Password
<input type="checkbox"/>	John	John	Approved	Enabled	09/08/2010 11:10:43	Password

Operators

Operators page						
Field	Description					Filtering criteria
Name	The operator's login. For filtering, the wildcard characters % and _ enable you to search for a group of names.					✓

Operators page		
Field	Description	Filtering criteria
Status	<p>You can select one of these values to filter on the approval status of the operator definitions:</p> <ul style="list-style-type: none"> • Approved • Wait RSO Approval • Wait LSO Approval • Unapproved <p>You can also select one of these values to filter on the operator status values:</p> <ul style="list-style-type: none"> • Enabled • Disabled • Time Disabled 	✓
Authentication Type	You can select one of these values to filter on the authentication method:	✓
Profiles	<p>You can filter on the profiles using one of these two options:</p> <ul style="list-style-type: none"> • Matching String: If you select this option, then type an operator profile name in the corresponding field. The wildcard characters % and _ enable you to search for a group of names. • Matching Selection: If you select this option, then select one or several operator profiles in the Available list. 	✓
Units	<p>You can filter on the units using one of these two options:</p> <ul style="list-style-type: none"> • Matching String: If you select this option, then type a unit name in the corresponding field. The wildcard characters % and _ enable you to search for a group of names. • Matching Selection: If you select this option, then select one or several units in the Available list. 	✓
Description	The full name of the operator or other description	

Operators page		
Field	Description	Filtering criteria
Approval Status	<p>The approval status of the operator definition</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Approved Wait RSO Approval Wait LSO Approval Unapproved 	
Enable Status	<p>The operator status</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Enabled Disabled 	
Last Login	The date and time of the last login	
Authentication	<p>The authentication type</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Password One-time Password LDAP 	

8.5.4 Operator Details Window: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details for the configuration of the operator selected
See "Details" on page 251
- Functions that enable you to manage the operator
See "Functions" on page 255

Display

Operator Details - Christine

Configuration **Monitoring**

Name: Christine

Description: Christine DELCUVE

Status: Approved/Enabled

Last Login:

Type: Human

Authentication Type: Password

Authoriser DN for FileAct:

Profiles:

Available: ALL, R7.1_IPLA_Monitor, R7.1_IPLA_Oper, R7.1_Import_Export, R7.1_MsgEntry, R7.1_MsgPartner, R7.1_Operator

Selected: ALLList

Units:

Available: Unit1, Unit2, Unit3, Unit4, Unit5, test

Selected: None

Buttons: Close, Report, Disable, Previous, Next

Details

Field	Description
Name	The operator's login. This name must be unique and can have up to 150 alphanumeric characters. The following characters are allowed: @ . _ - : . The <BIC> in the operator's name is the Live BIC.
Description	The full name of the operator or other description
Status	The approval status of the operator definition and operator status
Last Login	The date and time of the last login
Type	The type of operator that connects to Alliance Access: <ul style="list-style-type: none"> Human user Application user
Authoriser DN for FileAct	With this field, you can force the usage of a specific authoriser DN when the specified operator performs a manual file send operation.

Field	Description
Authentication Type	<p>The method of authenticating the user:</p> <ul style="list-style-type: none"> Password: If this authentication method is selected, then the Generated Password field is displayed. The left or right secrets generated by the system are displayed in this field. If you select the Show Clear Text check box, then the left or right secrets appear in clear. One-time Password: With this authentication type, the password of the user is validated against an authentication server. Before one-time passwords can be used, the authentication server must be set up. LDAP: If this authentication method is selected, then the LDAP User ID field is displayed. The user name of the operator as defined in the LDAP directory should be indicated in this field. You can enter the same LDAP user ID for multiple operators.
LDAP Server Group	<p>If the Authentication Type is LDAP, the one or more LDAP Server Groups that the operator is assigned to, listed in alphabetical order.</p> <p>To view these groups, you need either the Add Operator or Modify Operator permission, but not the Security Definition, Configure LDAP/Approve LDAP permission.</p>
Authentication Server Group	<p>If the Authentication Type is One-Time Password, the one or more Authentication Server Groups that the operator is assigned to, listed in alphabetical order.</p> <p>To view these groups, you need either the Add Operator or Modify Operator permission, but not the Security Definition, Auth Server Config permission.</p>
Profiles/Available	The list of available operator profiles
Profiles/Selected	The list of operator profiles selected for the operator
Units/Available	The list of available units
Units/Selected	The list of units to which the operator belongs

8.5.5 Operator Details Window: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details for the monitoring of the sessions currently open by the operator selected
See "Details" on page 253
- Functions that enable you to manage the operator
See "Functions" on page 255

Display

Operator Details - Diana

Configuration Monitoring

Last Login 2010/08/13 14:53:24

Active Sessions Rows in list: 4, in selection: 1

Change View Refresh Kill Session ◀ Previous Next ▶

	Host Address	Expiration	Session Type
<input checked="" type="checkbox"/>	10.4.160.206	2010/08/13 15:45:04	WebService
<input type="checkbox"/>	10.4.160.206	2010/08/13 15:35:30	WebService
<input type="checkbox"/>	10.4.160.206	2010/08/13 15:45:09	WebService
<input type="checkbox"/>	10.4.160.206	2010/08/13 15:18:36	WebService

◀ ▶

Close Report Disable Previous Next

Details

Field / Column	Description
Last Login	The date and time of the last login
Host Address	The IP address or host name of the Alliance Web Platform host where the operator initiated a session. The address of the browser used to create the session is logged in Alliance Web Platform. For more information, see viewing user session properties in the Web Platform Administration and Operations Guide .
Expiration	For Web services sessions, the time at which the session automatically expires if no action is taken before
Session Type	The type of session: <ul style="list-style-type: none"> WebService: for sessions run through Alliance Web Platform or Web service applications WorkStation: for sessions run through Alliance Workstation

8.5.6 Operator Delegations Window

Content

The **Operator Delegations** window contains these elements:

- Details of the operator profiles, units, and destinations that the local security officer selected is allowed to manage

See "Details" on page 254

Display

The screenshot shows the 'Operator Delegations' window with three main sections: Profiles, Units, and Destinations. Each section has an 'Available' list on the left and a 'Selected' list on the right, with bidirectional selection buttons between them. The 'Profiles' section shows 'R7.0_Operator' in the Selected list. The 'Units' section shows 'None' in the Available list. The 'Destinations' section shows 'SAABBEBO' in the Selected list.

Details

Field	Description
Profiles/Available	The list of available operator profiles
Profiles/Selected	The list of operator profiles that the security officer is allowed to manage
Units/Available	The list of available units
Units/Selected	The list of units that the security officer is allowed to manage
Destinations/Available	The list of available destinations
Destinations/Selected	The list of destinations that the security officer is allowed to manage

8.5.7 Operator Functions

Overview

These functions enable you to manage operators.

Functions

Function	Purpose	Operators page	Operator Details window - Configuration tab	Operator Details window - Monitoring tab
Add / Add As	To add an operator You can also create an operator using the characteristics of an existing operator with the Add As button Procedure: "Add an Operator" on page 256	✓	x	x
Delete	To delete an operator Procedure: "Delete an Operator" on page 258	✓	x	x
Enable	To enable an operator Procedure: "Enable an Operator" on page 260	✓	✓	✓
Disable	To disable an operator Procedure: "Disable an Operator" on page 259	✓	✓	✓
Reset Password / Reset LSO Password or Reset RSO Password	To reset the password of an operator Procedure: "Reset the Password of an Operator" on page 261 If you are logged in as a security officer, then the Reset LSO Password or Reset RSO Password buttons is displayed. Procedure: "Reset the Password of a Security Officer" on page 261	✓	✓	x
Approve	To approve the operators' definitions Procedure: "Approve an Operator" on page 259	✓	✓	x
Configure Delegations	If the Restrict Delegation (Operator class) security parameter is set to Yes , and you are logged on as a left or right security officer, then the Configure Delegations button is available. Allows you to define local security officers. You can define the operator profiles, units, and destinations that a local security officer is allowed to manage. Procedure: "Add an Operator" on page 256	x	✓	x

Function	Purpose	Operators page	Operator Details window - Configuration tab	Operator Details window - Monitoring tab
Kill Session	To kill the operator's session Procedure: "Monitor an Operator Session" on page 262	x	x	✓

8.5.8 Add an Operator

Purpose

This procedure enables you to add an operator.

Users and permissions

To display the list or the details of operators, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation** security parameter (**Operator** class) is set to Yes, then the operator defining operators can only select operator profiles, units and licensed destinations from a restricted subset. This restriction does not apply to security officers.

To add or modify an operator, your operator profile must have these actions:

- **Security Definition / Add Operator**
- **Security Definition / Mod Operator**

If the **Restrict Functions** security parameter (**Operator** class) is set to Yes, then operator-related functions (open, modify, approve, remove, add, print) are restricted to operators belonging to a subset of the units of the operator executing the function. This restriction does not apply to security officers.

Security officers can add operators.

Procedure

1. From the list of operators, click **Add**.

You can also add an operator using the characteristics of an existing operator.

Select the check box of an operator and click **Add As**.

The **Operator Details** window opens.

The status is Unapproved/Disabled.

2. In the **Configuration** tab, type a name for the operator in the **Name** field.

This name must be unique and can have up to 150 alphanumeric characters. The following characters are allowed: @ . _ - : .

SWIFT recommends that you select something simple, such as the operator's first name.

3. In the **Description** field, type the full name of the operator or another description.

4. In the **Type** drop-down list, select one of the following values:

- Application
- Human

5. In the **Authentication Type** drop-down list, select one of the following values:

Parameter	Procedure
Password	<p>With this authentication type, the user name and password are stored in the Alliance Access database.</p> <p>If you select this method, then the left and right secrets are generated by the system.</p> <p>Left secrets can be displayed by left security officers or operators with "left" entitlements and permissions. Right secrets can be displayed by right security officers or operators with "right" entitlements and permissions.</p> <p>If you select the Show Clear Text check box, then the left or right secrets appear in clear.</p>
One-time Password	<p>With this authentication type, the password of the user is validated against an authentication server.</p> <p>Before one-time passwords can be used, the authentication server must be set up.</p>
LDAP	<p>With this authentication type, the user name and password are validated against an LDAP authentication server.</p> <p>If you select LDAP, the LDAP User ID field appears. Type the user name of the operator as defined in the LDAP directory.</p> <p>You can enter the same LDAP user ID for multiple operators.</p> <p>If you leave this field empty, then the local Alliance Access operator name is forwarded to the LDAP server and used for the authentication.</p>

6. For an operator with the LDAP authentication type, select the name of the **LDAP Server Group** that the operator is assigned to.
7. For an operator with the one-time password authentication type, select the name of the **Authentication Server Group** that the operator is assigned to.
8. Assign one or more profiles from the **Profiles/Available** list to the operator definition.
9. Assign one or more units from the **Units/Available** list to the operator.
- During installation, the unit **None** is assigned by default. It can be deselected if needed.
10. If the **Restrict Delegation (Operator** class) security parameter is set to **Yes**, and you are logged on as a left or right security officer, then the **Configure Delegations** button is available.
- This button enables you to define local security officers. You can define the operator profiles, units, and destinations that a local security officer is allowed to manage in the **Operator Delegations** window.
11. Click **Save**.
- A status popup message appears.
12. Click **Close**.
- The **Operator Details** window closes.

If you change the authentication method, the units, or the profiles, then the operator must be re-approved by both security officers or operators with the appropriate approval entitlement.

Effect on passwords when modifying an operator

- If user passwords are used on your system, then the modified operator can continue to sign on with an existing password.
- If you are using one-time passwords:
 - If you change the **Authentication Type** to **One-time Password**, then the operator must sign on using the one-time password generated by the hardware token, even if it is the first sign-on.
 - If **One-time Password** is selected and you select another authentication method, then the operator must use the associated user password. If the new authentication method is **Password**, then the user is prompted to change password.
- If the authentication method is **LDAP**, then the operator must sign on with an LDAP password.

8.5.9 Delete an Operator

Purpose

This procedure enables you to delete an operator.

Users and permissions

To display the list or the details of operators, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation** security parameter (**Operator** class) is set to **Yes**, then the operator defining operators can only select operator profiles, units and licensed destinations from a restricted subset. This restriction does not apply to security officers.

To delete an operator, your operator profile must have this action:

- **Security Definition / Rem Operator**

Security officers can delete operators.

Prerequisites

Operators cannot be removed if they are specified in an alarm distribution list. First remove the operator from the alarm distribution list.

Procedure

1. From the list of operators, select the check box for one or several operators in the left column.
2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

8.5.10 Approve an Operator

Purpose

This procedure enables you to approve an operator.

Users and permissions

To display the list or the details of operators, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation** security parameter (**Operator** class) is set to **Yes**, then the operator defining operators can only select operator profiles, units and licensed destinations from a restricted subset. This restriction does not apply to security officers.

To approve an operator, your operator profile must have this action:

- **Security Definition / Approve Operator**

The **Approve Left or Right** part permission must be set to **Left** or **Right**.

Security officers can left-approve or right-approve operators.

Procedure

1. From the list of operators, select the check box for one or several operators who are in an unapproved state in the left column.
2. Click **Approve**.

A status popup message appears.

Note

The other security officer or operator with the necessary entitlements and permissions must now sign on and approve the operator or operators. When both security officers or operators have approved the changes, the status changes to **Approved** and the operator is automatically enabled.

8.5.11 Disable an Operator

Purpose

This procedure enables you to disable an operator.

The operator definition for an approved and enabled operator can be disabled, so that the operator cannot sign on to Alliance Access. For example, you may decide to disable an operator's definition because the operator has left your institution.

You can disable an operator definition until a specific date and time, or disable it indefinitely. You can also automatically disable an operator who has not signed on for a certain period of time.

Users and permissions

To display the list or the details of operators, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation** security parameter (**Operator** class) is set to **Yes**, then the operator defining operators can only select operator profiles, units and licensed destinations from a restricted subset. This restriction does not apply to security officers.

To disable an operator, your operator profile must have this action:

- **Security Definition / Disable Operator**

Security officers can disable operators without any restrictions.

Procedure

1. From the list of operators, select the check box for one or several operators who are in an enabled state in the left column.

2. Click **Disable**.

The **Disable Operator** window opens.

3. In the **Next Sign On Allowed** drop-down list, select one of the following options:

- **By Enable Command:** To disable the operator definition until you enable the definition again with the **Enable** button.
- **On the Following Date:** To disable the operator definition until the date, and time that you specify, or until you enable the definition again with the **Enable** button.

4. Click **Disable**.

A status popup message appears.

8.5.12 Enable an Operator

Purpose

This procedure enables you to enable an operator.

Users and permissions

To display the list or the details of operators, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation** security parameter (**Operator** class) is set to **Yes**, then the operator who defines operators can only select operator profiles, units and licensed destinations from a restricted subset. This restriction does not apply to security officers.

To enable an operator, your operator profile must have this action:

- **Security Definition / Enable Operator**

Security officers can enable operators without any restrictions.

Procedure

1. From the list of operators, select the check box for one or several operators who are in a disabled state in the left column.
 2. Click **Enable**.
- A status popup message appears.

8.5.13 Reset the Password of an Operator

Purpose

This procedure enables you to reset the password of an operator.

If an operator forgets their user password, then the security officers, or operators with the appropriate **Approve Operator** entitlement, can reset the password.

Users and permissions

To display the list or the details of operators, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation** security parameter (**Operator** class) is set to **Yes**, then the operator defining operators can only select operator profiles, units and licensed destinations from a restricted subset. This restriction does not apply to security officers.

To reset the password of an operator, your operator profile must have this action:

- **Security Definition / Approve Operator**

Security officers can reset the passwords of operators.

Procedure

1. From the list of operators, select the check box for one or several operators in the left column.
 2. Click **Reset Password**.
- A status popup message appears.
- The operator's user password is reset to its default value.
3. Open the operator's details and select the **Show Clear Text** check box.
- The right or left half of the password is displayed. Take note of the password and pass it secretly to the operator. The other security officer has to take note of the other half of the password and pass it to the operator.
- The operator must then sign on using the two halves of the password.

8.5.14 Reset the Password of a Security Officer

Purpose

This procedure enables you to reset the password of a security officer.

If a security officer (left security officer or right security officer) forgets their password, then the password can only be reset by the other security officer.

Users and permissions

Security officers are the only ones who can reset the password of their peer.

The **Reset Peer Officer Password (Password class)** security parameter must be set to **Yes**.

By default, the **Reset Peer Officer Password (Password class)** security parameter is set to **No**, which means that the security officers cannot reset each other's password. If the parameter is set to **No**, and a security officer forgets a password, then contact Support for further instructions.

Procedure

1. Sign on as right security officer or left security officer.
2. From the list of operators, click **Reset LSO Password** or **Reset RSO Password**.
A status popup message appears.

The left or right security officer's password is reset to the eight hexadecimal-character master password that SWIFT dispatched. Your organisation must have retained the original master password provided by SWIFT and stored it in a secure place.

8.5.15 Monitor an Operator Session

Purpose

This procedure enables you to monitor an operator session.

Users and permissions

To display the list or the details of operators, or filter the list, your operator profile must have this entity:

- **Security Definition**

If the **Restrict Delegation** security parameter (**Operator** class) is set to **Yes**, then the operator defining operators can only select operator profiles, units and licensed destinations from a restricted subset. This restriction does not apply to security officers.

To monitor an operator session, your operator profile must have this entity:

- **Monitoring**

You can kill an operator's session if the profile that has been assigned to you includes the **Stop Process** action for the **Monitoring** entity.

Procedure

1. From the list of operators, click the row of the operator which you want to monitor.
The **Operator Details** window opens.
2. Click the **Monitoring** tab.
3. You can click **Refresh** to refresh the list.
The **Kill Session** button enables you to kill the operator's session.
4. Click **Close**.
The **Operator Details** window closes.

9 Reference Data

9.1 BIC Directory

9.1.1 Alliance Bank Files

Alliance Bank Files

The Alliance Bank File contains the BIC information of all the institutions that currently use the SWIFT network either directly or through another party. The file contents are like the printed version of the BIC Directory except that the data is provided in a different layout and in different character sets.

Note The Alliance Bank File is sometimes referred to as the **BIC** file.

When installing a bank file on an Alliance Access server (running either UNIX or Windows) or on Web Platform, you no longer need to unzip the bank file in advance. You need to unzip the file only if you use the **Load BIC Files** command from Alliance Workstation started from an Alliance Access server on Windows. The use of this command is not recommended, because it requires the additional step of unzipping the bank file.

Updates to an Alliance Bank File

The Alliance Bank File which contains information for all institutions is a *Full Bank File*.

Between each distribution of a Full Bank File, SWIFT also distributes a delta file. This delta file contains only the changes since the last Full Bank File was issued. It only contains entries that have been added, modified, or deleted. In this document, this file is called a *Bank Update File*.

9.1.2 What Happens During Bank File Installation

Update on BIC Load

The Correspondent Information File (CIF) contains correspondent, country, and currency records, plus details of the aliases (alternative names) for correspondents. Each correspondent, country, and currency record has an **Update on BIC Load** field, which can be set to **Yes** or **No**.

When you install a Bank File (Full or Update file)

1. **New record**

Alliance Access adds new records in the Bank File to the CIF automatically.

2. **Update of a record**

If an existing correspondent record in the CIF has the **Update on BIC Load** field set to **Yes**, and some information has changed (for example, a correspondent has a new address), then the correspondent record is updated with the changes.

3. Deletion of a record

If the Bank File shows that a correspondent record must be deleted or if the correspondent does not appear in the Bank File, then Alliance Access checks the record and the following occurs:

- If at least one defined application is selected, then the correspondent record is not deleted. An event is recorded in a journal explaining why the correspondent was not deleted.
- If no defined application is selected, then Alliance Access checks the preferred network applications used within the correspondent:
 - If SWIFT (that is, SWIFTNet) is the only Preferred Network, then the correspondent record is deleted, and details of the correspondent are removed from any alias record automatically.
 - If SWIFT (that is, SWIFTNet) is not the only Preferred Network, then the record is not deleted. Alliance Access removes SWIFT (that is, SWIFTNet) from the list of Preferred Networks for the correspondent and creates an entry in the Event Log. This entry informs you that it was not possible to remove the correspondent automatically, and lists the Preferred Networks for the correspondent.

Note Even if an existing correspondent record in the CIF has the **Update on BIC Load** field set to **No**, SWIFT (that is, SWIFTNet) is removed from the list of Preferred Networks.

Note The **Status** of existing correspondent records remains unchanged when you install a new Bank File, whether the **Update on BIC Load** field is set to **Yes** or **No**. Therefore, if a record was made Inactive, it will still be Inactive after installing the new Bank File.

9.1.3 Options for Installing an Alliance Bank File

Overview

Periodically, SWIFT distributes a new Alliance Bank File at www.swiftrefdata.com. SWIFT recommends that you install the Alliance Bank File on a regular basis, to keep your Correspondent Information File (CIF) synchronised with the latest publication.

This section outlines the options available for installing a Full Bank File or Bank Update File:

- "Install manually"
- "Install automatically"
- "Schedule the installation of a Bank Update File"

Important After the installation of Alliance Access, you must install a Full Bank File.

Download the Alliance Bank File

To download the Alliance Bank File, perform the following steps:

1. Go to www.swiftrefdata.com.
2. Click **Login Here** on the **Your SWIFTRef access point** page.

- You are redirected to the SWIFT customer login page.
3. Type your e-mail address and your swift.com password, then click **Login**.
 4. The swiftrefdata.com home page is displayed, where you can access the Alliance Bank File. You may have to click **SWIFT Alliance** or **More** for the download option to become available.
 5. Locate the desired Alliance Bank File in the list, then click **Download** next to it. Refer to the following sections for details on the options for installing the file.
 6. If the Alliance Bank File is not in the list of documents that you can download, then order your download permission. Go to www.swift.com/ordering > Order products and services > Reference Data Directories > BIC Directory (file).
 7. Click **Order**. The **Order Downloadable Directories** page is displayed.

Install manually

Installing a Bank Update File manually involves the following tasks:

1. Download the Bank Update File to the **UpdateBIC** file directory.
For more information, see "Download an Alliance Bank File" on page 267.
2. Install the Bank File while the server is running in operational mode.

Important The manual installation of a Full Bank File is not possible from Alliance Access Configuration.

Install automatically

Installing a Full Bank File automatically involves the following tasks:

1. Download the Full Bank File to the **BIC** file directory.
For more information, see "Download an Alliance Bank File" on page 267.
2. Unzip the Bank File and remove the checksum file (**md5sum.txt** for ABE or **MD5.sum** for TXT format) from the directory.
3. The bank file installs automatically at the next restart of the Alliance Access server.

Each time the Alliance Access servers are stopped, the system checks whether a Full Bank File is present in the **BIC** file directory. If a file is present, then Alliance Access installs it after the servers have been stopped and before the next restart.

After successful activation of the Bank File in the Alliance Access database, the file is deleted from the **BIC** file directory. After this activation, or in case of a failure, an event is recorded in the event log the next time that the Alliance Access starts.

Schedule the installation of a Bank Update File

Scheduling the installation of a Bank Update File involves the following tasks:

1. Create a schedule for the installation of the Bank Update File.
2. The installation of the Bank File will take place when the scheduled action is executed.

If an update file is available in the **UpdateBIC** directory, then the file is installed at the scheduled time. You do not have to restart the servers after the file is installed.

After successful activation of the Alliance Bank File in the Alliance Access database, the file is deleted from the **UpdateBIC** file directory. After this activation, or in case of a failure, an event is recorded in the event log.

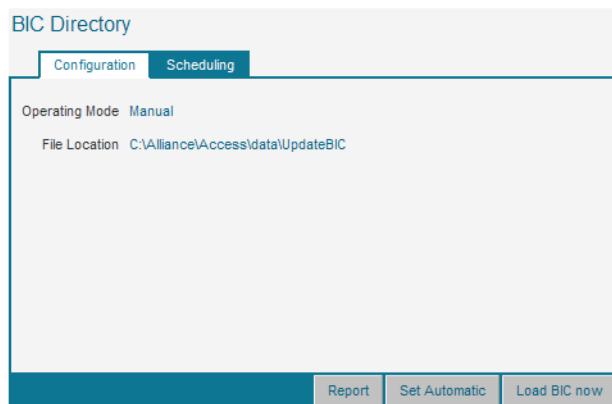
9.1.4 BIC Directory: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details that relate to the configuration of the Alliance Bank File installation
See "Details" on page 266
- Functions that enable you to manage the Alliance Bank File installation
See "Functions" on page 267

Display



Details

Field	Description
Operating Mode	These are the possible values: <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
File Location	The location of the UpdateBIC directory for manual and scheduled installations of Bank Update Files. The default location is: <software dir>\data\UpdateBIC where <software dir> is the directory in which Alliance Access is installed.

9.1.5 BIC Directory: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Tabs with Scheduled Actions Lists" on page 28.

9.1.6 BIC Directory Functions

Overview

These functions enable you to manage the Alliance Bank Files.

Functions

Function	Description
Set Automatic / Set Manual	Enables you to set the operation mode to <code>Automatic</code> or to <code>Manual</code> Procedure: "Change the Operation Mode" on page 268
Load BIC now	Loads the Bank Update File Procedure: "Configure and Launch a Manual Installation of a Bank Update File" on page 268

9.1.7 Download an Alliance Bank File

Purpose

You can download the Alliance Bank File from www.swiftrefdata.com.

To download a Bank File on UNIX or Linux:

1. Log on as an Alliance Administrator (`all_adm`).

The System Administration window appears.

2. Open an X-term from the **OS Configuration** menu in the System Administration window.
3. Create a temporary directory on the Alliance Access server, to which the `all_adm` user has access. For example, `/tmp`.
4. Download the Bank File from www.swiftrefdata.com. The file is packaged in **.ZIP** format.
5. Change to the installation directory for the Full Bank File or Bank Update File, as follows:
 - For a Full Bank File:
`cd $ALLIANCE/data/BIC`
 - For a Bank Update File:
`cd $ALLIANCE/data/UpdateBIC`
 - Copy the bank file to the relevant directory above.

Where **\$ALLIANCE** is the installation directory of Alliance Access. Installing Alliance Access creates these directories automatically.

To download a Bank File on Windows:

1. Create a temporary directory on the Alliance Access server, to which the Alliance Administrator user has access. For example, `\temp`.
2. Download the Bank File from www.swiftrefdata.com. The file is packaged in **.ZIP** format.

3. Change to the installation directory for the Full Bank File or Bank Update File, as follows:
 - For a Full Bank File:
cd %ALLIANCE%\data\BIC
 - For a Bank Update File:
cd %ALLIANCE%\data\UpdateBIC
 - Copy the bank file to the relevant directory above.

Where **%ALLIANCE%** is the installation directory of Alliance Access. Installing Alliance Access creates these directories automatically.

Note

You need to unzip the file only if you use the **Load BIC Files** command from Alliance Workstation started from an Alliance Access server on Windows. The use of this command is not recommended, because it requires the additional step of unzipping the bank file.

9.1.8 Configure and Launch a Manual Installation of a Bank Update File

Purpose

This procedure enables you to install a Bank Update File manually. The manual installation of a Full Bank File is not possible from Alliance Access Configuration.

Users and permissions

To display the configuration details and launch an installation manually, your operator profile must have this action:

- **Correspondent Info / Install Bankfile**

Prerequisites

A Bank Update File must be available in the **UpdateBIC** file directory. For more information, see "Download an Alliance Bank File" on page 267.

The servers must be running in operational mode.

Procedure

1. From the **Configuration** tab, check the configuration.
2. Click **Load BIC now**.

A status popup message appears.

Important Do not stop the servers until the installation is completed.

When the installation is completed, an event is recorded in the event log.

9.1.9 Change the Operation Mode

Purpose

This procedure enables you to change the operation mode.

Users and permissions

To change the operation mode, your operator profile must have this action:

- **Correspondent Info / Install Bankfile**

The **Modify operating mode** permission must be set to Yes.

Procedure

- From the **Configuration** tab or the **Scheduling** tab, given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

A status popup message appears.

9.2 BICs and Other Codes

9.2.1 BICs and Other Codes

Introduction

In Alliance Access, a correspondent can be an institution, a department or an individual which Alliance Access can communicate with through a network.

You can create and maintain the details of correspondents or groups of related correspondents. For example, if a department is at the same address as the institution to which it belongs, you can specify that the department correspondent inherits its address details from the existing institution correspondent. If the institution and department move to a new address, you only have to change the address of the institution correspondent. The department correspondent inherits the changed address automatically.

9.2.2 BICs and Other Codes Page

Content

The **BICs and Other Codes** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **BICs and Other Codes** page:
 - See "Correspondents" on page 270
 - See "Functions" on page 22
- Details of the available correspondents
 - See "Correspondents" on page 270
- Functions that enable you to view the correspondents
 - See "Functions" on page 276

Display

BICs and Other Codes

Filtering Criteria

Type	Definition	Status
BIC	Institution Name	Modified Since
Department	Branch	Update on BIC Load
Last Name	City Name	Application
First Name	Country Code	

BICs and Other Codes

	Change	View	Add	Delete	Activates	Inactivates	Report	Department	Last Name	First Name	Status	Type	City Name	Institution Name	Country	Branch Info
<input type="checkbox"/>	BIC										Active	Institution	BEograd	KBC BANKA AD	RS	
<input type="checkbox"/>	AAAARSBGXXX										Active	Institution	KUWAIT	ALMUZAINI EXCHANGE COMPANY KW		
<input type="checkbox"/>	AAACKWKWXXXX										Active	Institution	PARIS	ASSET ALLOCATION ADVISORS S FR		
<input type="checkbox"/>	AAADFRP1XXX										Active	Institution	PARIS	ASSOCIATION ADMINISTRATIVE A FR		
<input type="checkbox"/>	AAAGFRP1XXXX										Active	Institution	ALKHOBAR	SAUDI HOLLANDI BANK	SA	(EASTERN AREA ALKHOBAR)
<input type="checkbox"/>	AAALSARIALK										Active	Institution	RIYADH	SAUDI HOLLANDI BANK	SA	(CENTRAL TREASURY DEPT)
<input type="checkbox"/>	AAALSARICTD										Active	Institution	JEDDAH	SAUDI HOLLANDI BANK	SA	(WESTERN AREA JEDDAH)
<input type="checkbox"/>	AAALSARIED										Active	Institution	RIYADH	SAUDI HOLLANDI BANK	SA	(CENTRAL AREA RIYADH)
<input type="checkbox"/>	AAALSARYD										Active	Institution	RIYADH	SAUDI HOLLANDI BANK	SA	
<input type="checkbox"/>	AAALSARXXX										Active	Institution	RIYADH	SAUDI HOLLANDI BANK	SA	

Correspondents

Correspondents		Filtering criteria
Field	Description	
Type	<p>The correspondent type. This can be either an institution, a department, or an individual.</p> <p>These are the possible filtering criteria:</p> <ul style="list-style-type: none"> Institution: to search only for correspondents that are institutions Department: to search only for correspondents that are departments Individual: to search only for correspondents that are individuals 	✓
BIC	<p>The BIC-11 address of the institution. The BIC-8 destination address is followed by either a specific three-character branch code or by a default branch code of xxx.</p> <p>For filtering, the wildcard characters % and _ can also be used.</p>	✓
Department	<p>If the correspondent is a department or individual, this is the name of the department within the institution. Otherwise, it is blank.</p> <p>For filtering, if the Type drop-down list is empty or set to Department or Individual, then in the Department field, you can enter the name of the department within the institution that you are searching for. The wildcard characters % and _ can be used.</p>	✓
Last Name	<p>If the correspondent is an individual, this is the last name of the individual. Otherwise, it is blank.</p> <p>For filtering, if the Type drop-down list is empty or set to Individual, then in the Last Name field, you can enter the last name of the individual who you are searching for. The wildcard characters % and _ can be used.</p>	✓
First Name	<p>If the correspondent is an individual, this is the first name of the individual. Otherwise, it is blank.</p> <p>For filtering, if the Type drop-down list is empty or set to Individual, then in the First Name field, you can enter the first name of the individual who you are searching for. The wildcard characters % and _ can be used.</p>	✓

Correspondents		
Field	Description	Filtering criteria
Definition	<p>These are the possible values:</p> <ul style="list-style-type: none"> Internal: to search only for internal correspondents. These are correspondents owned by the institution. External: to search only for external correspondents. These are correspondents not owned by the institution. 	✓
Institution Name	<p>The name of the institution.</p> <p>For filtering, the BIC-11 address of the institution. The BIC-8 destination address is followed by either a specific three-character branch code or by a default branch code of xxx</p> <p>The full name of the institution. The wildcard characters % and _ can be used.</p>	✓
Branch (Info)	<p>The name of the branch.</p> <p>For filtering, the full name of the branch. The wildcard characters % and _ can be used.</p>	✓
City Name	<p>The full name of the city in which the correspondent is located.</p> <p>For filtering, the wildcard characters % and _ can be used.</p>	✓
Country (Code)	<p>The two-character ISO standard code for the country in which the correspondent is based - the same as characters 5 and 6 of the BIC-11 address in the Institution field.</p> <p>For filtering, the wildcard characters % and _ can be used.</p>	✓
Status	<p>The status of the correspondent. This can be Active or Inactive. You cannot send a message to an inactive correspondent.</p> <p>For filtering, these are the possible values:</p> <ul style="list-style-type: none"> Active: to search only for correspondents with an Active status. Inactive: to search only for correspondents with an Inactive status. You cannot send a message to an inactive correspondent. 	✓
Modified Since	Enter a date using the date picker. Only correspondent records which have been modified since this date are included in the search.	✓
Update on BIC Load	Select this check box to filter on any unpublished BICs that you have defined on your correspondents.	✓
Application	<p>These are the possible values:</p> <ul style="list-style-type: none"> APPLI: to search only for correspondents that have APPLI as one of their defined applications. APPLI is the Alliance application interface to external message partners (such as back-office banking systems). <p>If you select APPLI, then the Exit Point drop-down list appears. Select the exit point to which any messages for the correspondent are routed.</p>	✓

9.2.3 BICs and Other Codes Details Window: Profile Tab

Content

The **Profile** tab contains these elements:

- Details of the correspondents
See "Details" on page 272
- Functions that enable you to view the correspondents
See "Functions" on page 276

Display

Details

Field	Description
Status	The status of the correspondent. This can be Active or Inactive . You cannot send a message to an inactive correspondent.

Field	Description
Definition	<p>These are the possible values:</p> <ul style="list-style-type: none"> Internal: to create an internal correspondent. An internal correspondent is owned by the institution. External: to create an external correspondent. An external correspondent is not owned by the institution.
Header	<p>Select a correspondent type in the Type drop-down list.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Institution: to create a correspondent that is an institution Department: to create a correspondent that is a department Individual: to create a correspondent that is an individual <p>Then, you can complete the following fields:</p> <ul style="list-style-type: none"> BICs and Other Codes: The BIC-11 address of the institution. The BIC-8 destination address is followed by either a specific three-character branch code or by a default branch code of xxx. Special characters are not allowed. Department: If the Type field is set to Department or Individual, then in the Department field, you can enter the name of the department. Special characters are not allowed. Last Name: If the Type field is set to Individual, then in the Last Name field, you can enter the last name of an individual. Special characters are not allowed. First Name: If the Type field is set to Individual, then in the First Name field, you can enter the first name of an individual. Special characters are not allowed. <p> Optionally, you can enter a more specific description of the correspondent type in the Sub Type field. Special characters are not allowed.</p>

Field	Description
Details	<p>In the Profile drop-down list, specify the following:</p> <ul style="list-style-type: none"> • Specific: The correspondent profile is specific to this correspondent and is not inherited from a parent correspondent. • Same as Institution: The correspondent is a department and inherits its profile from the institution to which it is associated. • Same as Department: The correspondent is an individual and inherits its profile from the department to which it is associated. <p>The available choices depend on the correspondent type selected in the Type drop-down list.</p> <p>If you selected Specific, you have to complete the following fields:</p> <ul style="list-style-type: none"> • Institution Name: the full name of the institution • Branch: the full name of the branch • City: the name of the city in which the correspondent is located. <p>The Country field shows the ISO standard country code for the country in which the correspondent is based. This is character 5 and 6 of the BIC-11 address in the Institution field.</p> <ul style="list-style-type: none"> • Address: the address of the correspondent • Location: the location of the correspondent • POB Number: the post office box of the correspondent • POB Location: the location of the post office box
Preferred Language	<p>The preferred language that Alliance Access must use when expanding messages sent to the correspondent</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • English • Francais • Deutsch • Italiano • Espanol
Comments	Any general comment about the correspondent
Update on BIC Load	<p>Select this check box if you want the correspondent record to be updated when an Alliance Bank File is loaded. This means that the record may be changed or even deleted as a result of the update.</p> <p>Clear the check box if you do not want the correspondent record to be updated when an Alliance Bank File is loaded.</p> <p>This means that if the Alliance Bank File shows that the correspondent must be modified, the record is not modified. If the Alliance Bank File shows that the correspondent must be deleted, then the record is not deleted, but SWIFT is removed from the list of Preferred Networks for the correspondent.</p>
Last Modification	This field shows the date on which the correspondent record was last modified.

9.2.4 BICs and Other Codes Details Window: Preferred Networks Tab

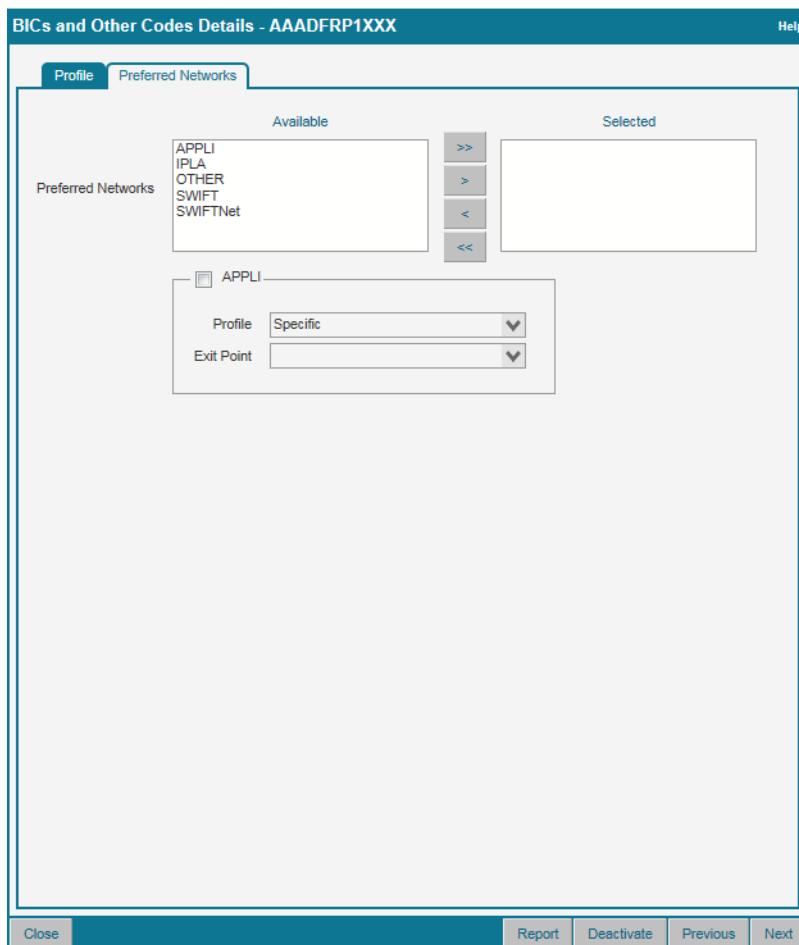
Content

The **Preferred Networks** tab displays the network applications that Alliance Access can use to send messages to the correspondent.

The **Preferred Networks** tab contains these elements:

- Details of the correspondents
See "Details" on page 272
- Functions that enable you to view the correspondents
See "Functions" on page 276

Display



Details

Field	Description
Preferred Networks	<p>All the defined applications for the correspondent that are also network applications.</p> <p>By default, Alliance Access sends any message to the correspondent using the first network application in the Selected list that can handle the message format, unless you specify a different network application during message creation or modification. Your correspondent may prefer you to use the applications in a specific order.</p> <p>The OTHER network is available from the list of preferred networks if the Application Development Toolkit Runtime is licensed.</p>
APPLI	<p>In the Profile drop-down list, specify the following:</p> <ul style="list-style-type: none"> Specific: The APPLI profile is specific to this correspondent and is not inherited from a parent correspondent. Same as Institution: The correspondent is a department and inherits its APPLI profile from the institution to which it is associated. Same as Department: The correspondent is an individual and inherits its APPLI profile from the department to which it is associated. <p>Then in the Exit Point drop-down list, select the name of the Alliance exit point to which any messages for the correspondent are to be routed. This is useful primarily for messages received for internal correspondents.</p> <p>Another use is when you cannot send a message directly to an external correspondent. You can define an exit point for messages to that correspondent. Alliance routes any message to the correspondent to the exit point automatically. You can then transmit the message to the correspondent by some other communication method.</p>

9.2.5 Correspondent Functions

Overview

These functions enable you to view correspondents.

Functions

Function	Description	Correspondents page	Correspondent Details window
Add	Enables you to add a correspondent Procedure: "Add a Correspondent" on page 277	✓	✗
Delete	Enables you to delete a correspondent Procedure: "Delete a Correspondent" on page 280	✓	✗
Activate	Enables you to activate a correspondent Procedure: "Activate or Deactivate a Correspondent" on page 280	✓	✓
Deactivate	Enables you to deactivate a correspondent Procedure: "Activate or Deactivate a Correspondent" on page 280	✓	✓

9.2.6 Add a Correspondent

Purpose

This procedure enables you to add a correspondent.

Users and permissions

To display the list or the details of correspondents, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Corr Dets** (to display the details)

To add or modify a correspondent, your operator profile must have the following additional actions:

- **Correspondent Info / Add Correspondent**
- **Correspondent Info / Modify Corr Dets**

Procedure

1. From the list of correspondents, click **Add**.

You can also create a correspondent using the characteristics of an existing correspondent. Select the check box of a correspondent and click **Add As**.

The **Correspondent Details** window opens.

2. Click the **Profile** tab.
3. In the **Definition** drop-down list, select one of the following values:
 - Internal
 - External
4. Select a correspondent type in the **Type** drop-down list and complete the related fields.

Correspondent type	Related fields
Institution	<p>Institution: Enter the BIC-11 address of the institution. The BIC-8 destination address is followed by either a specific three-character branch code or by a default branch code of xxx. Special characters are not allowed.</p>
Department	<ul style="list-style-type: none"> • Institution: see above • Department: Enter the name of the department. Special characters are not allowed.
Individual	<ul style="list-style-type: none"> • Institution: see above • Department: see above • Last Name: Enter the last name of an individual. Special characters are not allowed. • First Name: Enter the first name of an individual. Special characters are not allowed.

5. Optionally, you can enter a more specific description of the correspondent type in the **Sub Type** field. Special characters are not allowed.
 6. In the **Profile** drop-down list, specify whether the correspondent profile is specific to this correspondent or is inherited from an existing correspondent. The available choices depend on the correspondent type
 - Specific
 - Same as Institution
 - Same as Department
 7. If you selected **Specific**, complete the following fields:
 - **Institution Name**: the full name of the institution
 - **Branch**: the full name of the branch
 - **City**: the name of the city in which the correspondent is located.

The **Country** field shows the ISO standard country code for the country in which the correspondent is based. This is character 5 and 6 of the BIC-11 address in the **Institution** field.

 - **Address**: the address of the correspondent
 - **Location**: the location of the correspondent
 - **POB Number**: the post office box of the correspondent
 - **POB Location**: the location of the post office box
 8. In the **Preferred Language** drop-down list, select the preferred language that Alliance Access must use when expanding messages sent to the correspondent.

These are the possible values:

 - English
 - Francais
 - Deutsch
 - Italiano
 - Espanol
 9. In the **Comments** field, you can add a general comment about the correspondent.
 10. If you want the correspondent record to be updated when an Alliance Bank File is loaded, select the **Update on BIC Load** check box.

This means that the record may be changed or even deleted as a result of the update.
11. Click **Save**.
- A status popup message appears.
12. Click **Close**.
- The **Correspondent Details** window closes.

The correspondent is added to the list. By default, new correspondents are created in active state.

9.2.7 Select a Preferred Network Application

Purpose

This procedure enables you to select the preferred network application that Alliance Access must use when sending messages to the correspondent.

Users and permissions

To display the list or the details of correspondents, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Corr Dets** (to display the details)

To select a preferred network, your operator profile must have the following additional action:

- **Correspondent Info / Modify Corr Dets**

Procedure

1. From the list of correspondents, click the row of the correspondent for which you want to select a preferred network application.

The **Correspondent Details** window opens.

2. Click the **Preferred Networks** tab.
3. Select the preferred network application or applications from the **Preferred Networks/ Available** list.

By default, Alliance Access sends any message to the correspondent using the first network application in this list that can handle the message format, unless you specify a different network application during message creation or modification. Your correspondent may prefer you to use the applications in a specific order.

Note The OTHER network is available from the list of preferred networks if the Application Development Toolkit Runtime is licensed.

4. If you need to use the APPLI application, select the **APPLI** check box.
5. In the **Profile** drop-down list, specify whether the application interface profile is specific to this correspondent or is inherited from an existing correspondent.

The available choices depend on the correspondent type:

- Specific
- Same as Institution
- Same as Department

6. If you selected **Specific**, in the **Exit Point** drop-down list select the name of the Alliance exit point to which any messages for the correspondent are to be routed. This is useful primarily for messages received for internal correspondents.

Another use is when you cannot send a message directly to an external correspondent. You can define an exit point for messages to that correspondent. Alliance routes any message to the correspondent to the exit point automatically. You can then transmit the message to the correspondent by some other communication method.

7. Click **Save**.

A status popup message appears.

8. Click **Close**.

The **Correspondent Details** window closes.

The correspondent details are updated.

9.2.8 Activate or Deactivate a Correspondent

Purpose

This procedure enables you to activate or deactivate a correspondent.

You cannot activate or deactivate a correspondent when the servers are running in housekeeping mode.

Users and permissions

To display the list or the details of correspondents, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Corr Dets** (to display the details)

To activate or deactivate a correspondent, your operator profile must have the following additional action:

- **Correspondent Info / Modify Corr Dets**

Procedure

1. From the list of correspondents, select the check box for one or several correspondents in the left column.
2. Click **Activate** or **Deactivate**.

A status popup message appears.

The status of the correspondent or correspondents selected changes to **Active** or **Inactive**.

9.2.9 Delete a Correspondent

Purpose

This procedure enables you to delete a correspondent.

You can only delete a parent correspondent if you first either delete all its child correspondents, or you modify the child correspondents so that they no longer inherit the parent's profiles.

If you delete a correspondent and this correspondent is referenced by an alias or a distribution list, the correspondent is also deleted from the list of correspondents of the alias or distribution list.

Users and permissions

To display the list or the details of correspondents, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Corr Dets** (to display the details)

To delete a correspondent, your operator profile must have the following additional action:

- **Correspondent Info / Remove Correspondent**

Procedure

1. From the list of correspondents, select the check box for one or several correspondents in the left column.
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
A status popup message appears.

The correspondent or correspondents selected are deleted.

9.3 Aliases

9.3.1 Aliases

Introduction

When creating a message, it is possible to specify that the message is sent to an alias instead of an actual BIC-11 address. An alias is an alternative name for a correspondent or group of correspondents. If the alias is for a single correspondent, then you can use it to send any message type. If the alias is for a group of correspondents, then you can send only non-financial messages (MT 999s). The message is broadcast to the group of correspondents which means that a single message is created and sent to them all.

A correspondent or group of correspondents can have more than one alias.

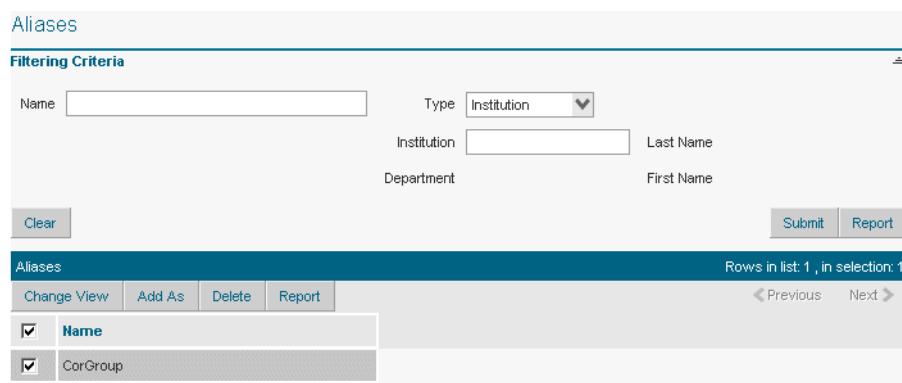
9.3.2 Aliases Page

Content

The **Aliases** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Aliases** page:
 - See "Aliases" on page 282
 - See "Functions" on page 22
- Details of the available aliases
 - See "Aliases" on page 282
- Functions that enable you to manage the aliases
 - See "Functions" on page 283

Display



The screenshot shows the 'Aliases' page interface. At the top, there is a 'Filtering Criteria' section with fields for 'Name' (text input), 'Type' (dropdown menu set to 'Institution'), 'Institution' (text input), 'Last Name' (text input), 'Department' (text input), and 'First Name' (text input). Below this is a 'Clear' button and a 'Submit' button. The main area is titled 'Aliases' and shows a list of items. The first item is 'Name' with a checked checkbox, and the second item is 'CorGroup' with a checked checkbox. At the bottom of the list are buttons for 'Change View', 'Add As', 'Delete', and 'Report'. Navigation buttons 'Previous' and 'Next' are also present.

Aliases

Aliases		
Field	Description	Filtering criteria
Name	The name of the alias. For filtering, the wildcard characters % and _ enable you to search for a group of aliases.	✓
Type	The correspondent type These are the possible values: <ul style="list-style-type: none"> • Institution: to search only for correspondents that are institutions • Department: to search only for correspondents that are departments • Individual: to search only for correspondents that are individuals 	✓
Institution	The BIC-11 address of the institution to search for. The wildcard characters % and _ can be used.	✓

Aliases		
Field	Description	Filtering criteria
Department	If the Type drop-down list is empty or set to Department or Individual , then in the Department field, you can enter the name of the department within the institution that you are searching for. The wildcard characters % and _ can be used.	✓
Last Name	If the Type drop-down list is empty or set to Individual , then in the Last Name field, you can enter the last name of the individual who you are searching for. The wildcard characters % and _ can be used.	✓
First Name	If the Type drop-down list is empty or set to Individual , then in the First Name field, you can enter the first name of the individual who you are searching for. The wildcard characters % and _ can be used.	✓

Functions

Function	Description
 Add	Enables you to add an alias Procedure: "Add an Alias" on page 284
 Delete	Enables you to delete an alias Procedure: "Delete an Alias" on page 285

9.3.3 Alias Details Window

Content

The **Alias Details** window contains these elements:

- Details of the aliases
See "Details" on page 284
- Functions that enable you to manage the aliases
See "Functions" on page 284

Display

Alias Details

Correspondents				Rows in list: 4 , in selection: 1	
<input type="button" value="Add"/>	<input type="button" value="Delete"/>	Institution	Department	Last Name	First Name
<input type="checkbox"/>		AAFAFRP1XXX			
<input checked="" type="checkbox"/>		AAFMGB21XXX			
<input type="checkbox"/>		AAFNFRP1XXX			
<input type="checkbox"/>		AAGOCHZ1XXX			

Details

Field / Column	Description
Name	The name of the alias
Institution	The BIC-11 address of the institution
Department	The name of the department (optional)
Last Name	The last name of an individual (optional)
First Name	The first name of an individual (optional)

Functions

Function	Description
<input type="button" value="Add"/>	Enables you to add one or several correspondents using the BIC picker Procedure: "Add an Alias" on page 284
<input type="button" value="Delete"/>	Enables you to delete one or several correspondents Procedure: "Delete an Alias" on page 285

9.3.4 Add an Alias

Purpose

This procedure enables you to add an alias.

Users and permissions

To display the list or the details of aliases, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Alias** (to display the details)

To add or modify an alias, your operator profile must have the following additional actions:

- **Correspondent Info / Add Alias**
- **Correspondent Info / Modify Alias**

Procedure

1. From the list of aliases, click **Add**.

You can also create an alias using the characteristics of an existing alias. Select the check box of an alias and click **Add As**.

The **Alias Details** window opens.

2. In the **Name** field, type the name of the alias (31 characters maximum).

3. Click **Add**.

The **BIC Picker** window opens.

4. Select one or more correspondents using the BIC picker.

For more information about the BIC picker, see "BIC Picker" on page 41.

5. Click **Save**.

A status popup message appears.

6. Click **Close**.

The **Alias Details** window closes.

The alias is added to the list.

9.3.5 Delete an Alias

Purpose

This procedure enables you to delete one or several aliases.

If you delete an alias, then it cannot be recovered.

Users and permissions

To display the list or the details of aliases, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Alias** (to display the details)

To delete an alias, your operator profile must have the following additional action:

- **Correspondent Info / Remove Alias**

Procedure

1. From the list of aliases, select the check boxes for one or several aliases in the left column. You can select all the aliases by selecting the check box in the column heading line.
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
A status popup message appears.

The alias or aliases are deleted.

9.4 Countries

9.4.1 Countries

Introduction

You can create and maintain the country records in the Correspondent Information File. Most of the details in the Correspondent Information File are imported from the Alliance Bank File. Each country record in the Correspondent Information File includes a field that defines whether the record must be updated automatically when an Alliance Bank File is loaded into Alliance. If you do not want to wait for the next update of the Alliance Bank File, then you can modify existing country records and add new country records manually.

9.4.2 Countries Page

Content

The **Countries** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Countries** page:
 - See "Countries" on page 287
 - See "Functions" on page 22
- Details of the available countries
See "Countries" on page 287
- Functions that enable you to view the countries
See "Functions" on page 287

Display

Countries

Filtering Criteria

Code	<input type="text"/>	Name	<input type="text"/>
<input type="button" value="Clear"/>		<input type="button" value="Submit"/>	<input type="button" value="Report"/>

Countries Rows in list: 20 , in selection: 1

	Code	Name
<input type="checkbox"/>	AQ	ANTARCTICA
<input type="checkbox"/>	AR	ARGENTINA
<input checked="" type="checkbox"/>	AS	AMERICAN SAMOA
<input type="checkbox"/>	AT	AUSTRIA
<input type="checkbox"/>	AU	AUSTRALIA

Countries

Countries		
Field	Description	Filtering criteria
Code	The unique two-character ISO standard country code. For filtering, the wildcard characters % and _ enable you to search for a group of codes.	✓
Name	The country name. For filtering, the wildcard characters % and _ enable you to search for a group of names.	✓

Functions

Function	Description
<input type="button" value="Add"/>	Enables you to add a country Procedure: "Add a Country" on page 288
<input type="button" value="Delete"/>	Enables you to delete a country Procedure: "Delete a Country" on page 289

9.4.3 Country Details Window

Content

The **Country Details** window contains these elements:

- Details of the countries

See "Details" on page 288

Display

The screenshot shows a 'Country Details' window with the following fields and settings:

- Code:** AS
- Name:** AMERICAN SAMOA
- Update on BIC Load:**

At the bottom of the window are buttons for Close, Report, Previous, and Next.

Details

Field	Description
Code	The unique two-character ISO standard country code
Name	The name of country
Update on BIC Load	Select this check box if you want the country record to be updated when an Alliance Bank File is loaded. This means that the record may be changed or even deleted as a result of the update. Clear the check box if you do not want the country record to be updated when an Alliance Bank File is loaded.

9.4.4 Add a Country

Purpose

This procedure enables you to add a country.

Users and permissions

To display the list or the details of countries, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Country** (to display the details)

To add or modify a country, your operator profile must have the following additional actions:

- **Correspondent Info / Add Country**
- **Correspondent Info / Modify Country**

Prerequisites

You cannot add countries when the servers are running in housekeeping mode.

Procedure

1. From the list of countries, click **Add**.

You can also create a country using the characteristics of an existing country. Select the check box of a country and click **Add As**.

The **Country Details** window opens.

2. In the **Code** field, type the country code.

3. In the **Name** field, type the name of the country.
4. If you want the country record to be updated when an Alliance Bank File is loaded, select the **Update on BIC Load** check box.

This means that the record may be changed or even deleted as a result of the update.

5. Click **Save**.

A status popup message appears.

6. Click **Close**.

The **Country Details** window closes.

The country is added to the list.

9.4.5 Delete a Country

Purpose

This procedure enables you to delete one or several countries.

If you delete a country record, then it cannot be recovered.

Users and permissions

To display the list or the details of countries, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Country** (to display the details)

To delete a country, your operator profile must have the following additional action:

- **Correspondent Info / Remove Country**

Prerequisites

You cannot delete countries when the servers are running in housekeeping mode.

Procedure

1. From the list of countries, select the check boxes for one or several countries in the left column. You can select all countries by selecting the check box in the column heading line.
2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

The country or countries are deleted.

9.5 Currencies

9.5.1 Currencies

Introduction

You can create and maintain the currency records in the Correspondent Information File. Most of the details in the Correspondent Information File are imported from the Alliance Bank File. Each currency record in the Correspondent Information File includes a field that defines whether the record must be updated automatically when an Alliance Bank File is loaded into Alliance. If you do not want to wait for the next update of the Alliance Bank File, then you can modify existing currency records and add new currency records manually.

9.5.2 Currencies Page

Content

The **Currencies** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Currencies** page:
 - See "Currencies" on page 291
 - See "Functions" on page 22
- Details of the available currencies
 - See "Currencies" on page 291
- Functions that enable you to view the currencies
 - See "Functions" on page 291

Display

Currencies

Filtering Criteria

Code Name

Currencies Rows in list: 20 , in selection: 1

<input type="checkbox"/>	Code	Name	Digits
<input type="checkbox"/>	AOA	KWANZIA	2
<input checked="" type="checkbox"/>	ARS	ARGENTINE PESO	2
<input type="checkbox"/>	AUD	AUSTRALIAN DOLLAR	2
<input type="checkbox"/>	AWG	ARUBAN GUILDER	2

Currencies

Currencies		
Field	Description	Filtering criteria
Code	The unique three-character ISO standard currency code. For filtering, the wildcard characters % and _ enable you to search for a group of codes.	✓
Name	The currency name. For filtering, the wildcard characters % and _ enable you to search for a group of names.	✓
Digits	The maximum number of digits needed to correctly display fractional amounts of the currency. This can be any number between 0 and 6.	

Functions

Function	Description
Add	Enables you to add a currency Procedure: "Add a Currency" on page 292
Delete	Enables you to delete a currency Procedure: "Delete a Currency" on page 293

9.5.3 Currency Details Window

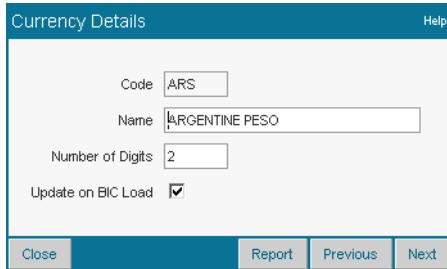
Content

The **Currency Details** window contains these elements:

- Details of the currencies

See "Details" on page 291

Display



Details

Field	Description
Code	The unique three-character ISO standard currency code
Name	The name of the currency
Number of Digits	The maximum number of digits needed to correctly display fractional amounts of the currency. This can be any number between 0 and 6.

Field	Description
Update on BIC Load	Select this check box if you want the currency record to be updated when an Alliance Bank File is loaded. This means that the record may be changed or even deleted as a result of the update. Clear the check box if you do not want the currency record to be updated when an Alliance Bank File is loaded.

9.5.4 Add a Currency

Purpose

This procedure enables you to add a currency.

Users and permissions

To display the list or the details of currencies, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
- **Correspondent Info / Open/Print Currency** (to display the details)

To add or modify a currency, your operator profile must have the following additional actions:

- **Correspondent Info / Add Currency**
- **Correspondent Info / Modify Currency**

Prerequisites

You cannot add currencies when the servers are running in housekeeping mode.

Procedure

1. From the list of currencies, click **Add**.

You can also create a currency using the characteristics of an existing currency. Select the check box of a currency and click **Add As**.

The **Currency Details** window opens.

2. In the **Code** field, type the currency code.
3. In the **Name** field, type the name of the currency.
4. If you want the currency record to be updated when an Alliance Bank File is loaded, select the **Update on BIC Load** check box.

This means that the record may be changed or even deleted as a result of the update.

5. Click **Save**.

A status popup message appears.

6. Click **Close**.

The **Currency Details** window closes.

The currency is added to the list.

9.5.5 Delete a Currency

Purpose

This procedure enables you to delete one or several currencies.

If you delete a currency record, then it cannot be recovered.

Users and permissions

To display the list or the details of currencies, or filter the list, your operator profile must have these actions:

- **Correspondent Info** (to display the list)
 - **Correspondent Info / Open/Print Currency** (to display the details)
- To delete a currency, your operator profile must have the following additional action:
- **Correspondent Info / Remove Currency**

Prerequisites

You cannot delete currencies when the servers are running in housekeeping mode.

Procedure

1. From the list of currencies, select the check boxes for one or several currencies in the left column. You can select all the currencies by selecting the check box in the column heading line.
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
A status popup message appears.

The currency or currencies are deleted.

10 Application Interface

10.1 Application Interface

Description

The Application Interface controls the transfer of messages and files between Alliance Access Configuration and back-office applications, printers, or any other system that communicates with Alliance Access Configuration. Suitable messages for transferring include SWIFT FIN, MX, FileAct, and system messages. Suitable files include payload files, or files that contain several messages (such as for Bulk Payments).

Within the Application Interface, a **message partner** represents the external application or product that communicates with Alliance Access Configuration. A message partner profile specifies how each message partner communicates with Alliance Access Configuration, and allows you to control and monitor the communication sessions.

Alliance Access Configuration provides default message partner profiles and default exit points. For more information, see the Default Printouts on the release media, or on www.swift.com, under Support > [Documentation \(User Handbook\)](#).

Alliance Access Configuration transfers a message to a message partner through an **exit point**, which holds the message in a queue before transferring it to the message partner. Each exit point is associated with a particular message partner.

The Application Interface allows you to:

- create, modify, or remove exit points and message partner profiles
- assign an exit point to a message partner
- control and monitor communication sessions between Alliance Access Configuration and a message partner.

10.2 Message Partners

10.2.1 Message Partners and Message Partner Profiles

Message partner

A message partner is an external application, such as, a back-office application, a printer, or a mainframe connection.

The Application Interface manages the transfer of files and messages between Alliance Access and a message partner using the profile that is defined for that message partner.

Profile of a message partner

A message partner profile specifies the parameters necessary to transfer message and files between Alliance Access and a message partner. The most important of these parameters is the connection method, which defines the type of connection protocol and the data format to be used for the transfer.

Every application that communicates with Alliance Access must have a message partner profile defined in the Application Interface.

Managing communication sessions

Once a message partner profile is configured, an operator with the appropriate permissions can view details about the current ongoing communication session or about the last communication session.

Also, operators with the appropriate permissions, can perform the following tasks:

- "Start a Session" on page 326
- "Run a Session" on page 328
- "Stop a Session" on page 329
- "Abort a Session" on page 330

Name of a message partner profile

The message partner profiles are defined automatically during the configuration process.

All CRnet message partner names have the following format:

CR<F|P><direction><application name>

where:

- **F**, indicates a CRFI application and **P** indicates a CRPI application
- **direction** is :
 - "to", for a message partner profile that manages the transfer of files and messages from Alliance Access to the message partner.
 - "fr", for a message partner profile that manages the transfer of files and messages from the message partner to Alliance Access.

For more information, see the [System Management Guide](#).

10.2.2 Message Flow in the Application Interface

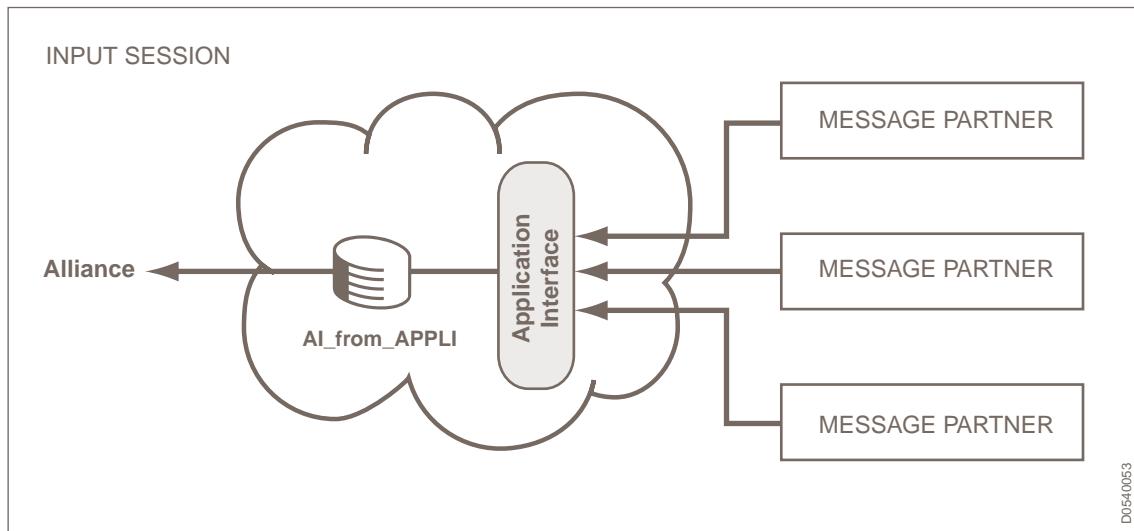
Message Processing Function

Message processing functions (MPFs) control the exchange of messages between the Application Interface (AI) and the message partners. The Application Interface Services (MXS) component manages the details of all message partner profiles and exit points.

Messages are handled differently depending on the direction of the message flow:

- "Input message flow" on page 296
- "Output message flow" on page 296

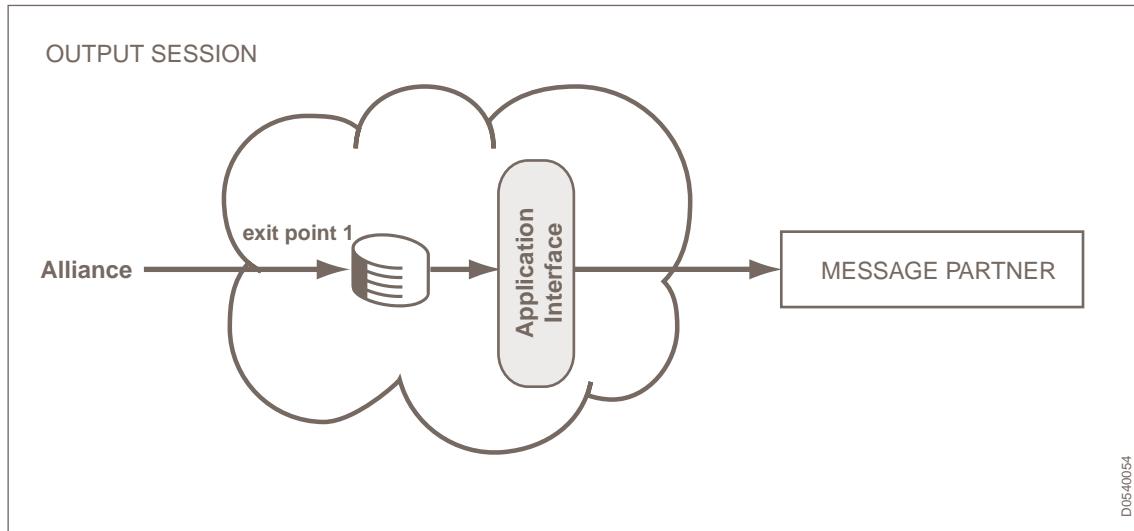
Input message flow



Incoming messages from a message partner are placed in a common **AI_from_APPLI** queue until they are processed by a message processing function. This queue is referred to as the *"Application Interface (AI) inbound"* queue.

This queue is used to route all incoming messages from all message partners using the connection methods, Direct FileAct, File Transfer, Interactive, WebSphere MQ, or SOAP.

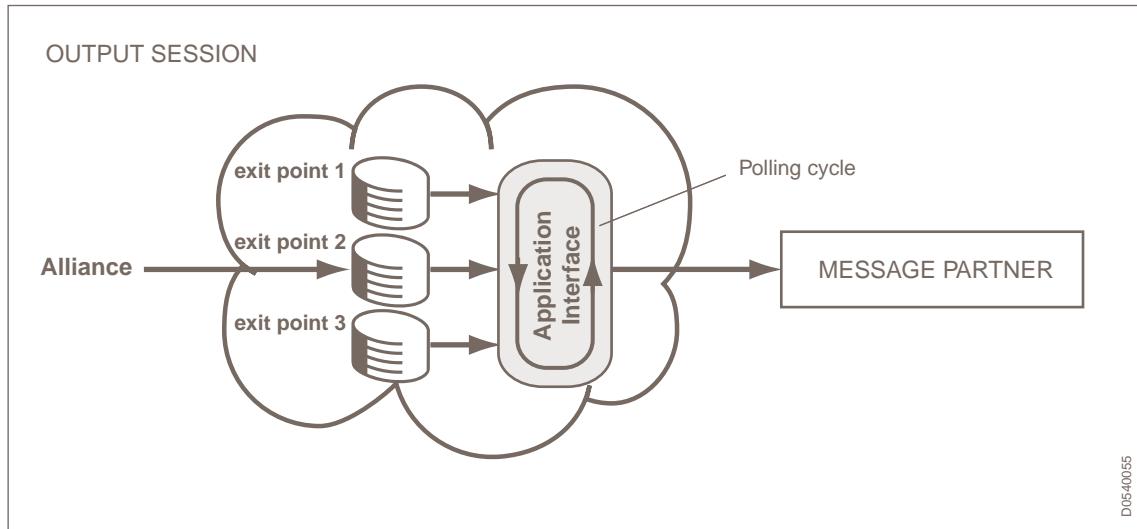
Output message flow



Outgoing messages to a message partner are placed in the exit point queue that is assigned to that message partner. The messages remain in the exit point until they are processed by a message processing function. When more than one exit point is assigned to a message partner during an output session, then a polling mechanism services each exit point queue in turn.

An operator can create or remove exit points, or assign an exit point to a message partner.

Output session with multiple exit points



10.2.3 Connection Methods

Connection method description

A connection method is part of a message partner profile. It specifies the type of communication protocol and the data format that is used to transfer messages between Alliance Access and a back-office application or external product. The location of the message or parameter files for transmission are specified as a connection point, which is associated with a connection method.

The Application Interface application supports several connection methods. This section provides basic descriptions of these connection methods.

Note All sessions that use the Interactive, WebSphere MQ, and SOAP connection methods are run on the server.

Bidirectional message exchange

Bidirectional message exchange during the same session (to and from Alliance Access a message partner) is possible with the following connection methods:

- Interactive
- File Transfer
- SOAP

Bidirectional message exchange is not available for the Direct FileAct, Print, or Websphere MQ connection methods.

FileAct message exchange

To exchange FileAct messages between Alliance Access and a message partner, the following connection methods are available:

- Direct FileAct
- File Transfer
- SOAP

- WebSphere MQ

Direct FileAct

The Direct FileAct connection method enables the transfer of a payload file between Alliance Access and a back-office application. A payload file contains the data that is to be transferred. The FileAct transmission parameters are deduced from the message partner profile. You do not need to send an XML version 2 message or a file that contains the FileAct transmission parameters when you send each payload file. Dedicated Direct FileAct input and output file directories are accessible to both Alliance Access and the back-office application or operator. The back-office application or an operator put the payload files in these directories to send the files over SWIFTNet, or they get the payload files received from SWIFTNet from these directories.

Direct FileAct also enables back-office applications to benefit from simplified reporting of network acknowledgements and of reconciled delivery notifications.

A message partner profile with the Direct FileAct connection method must exist for each correspondent that will use Direct FileAct to transmit files between each other.

The Direct FileAct connection method requires the licence package **22: DIRECT FILEACT**.

The file-transfer session can be started automatically or manually. For example, if a back-office application stores a payload file in a pre-configured input directory, then the presence of the file in the directory can automatically start a file-transfer session.

File Transfer

The File Transfer method enables the transfer of batch files containing multiple FIN, FileAct, or InterAct messages between Alliance Access and a back-office application. For FileAct messages, in addition to transferring a payload file, Alliance Access or a back-office application also transfers an XML version 2 message containing the FileAct settings which control the file transfer, and an optional parameter file. The file-transfer session can be started automatically or manually.

Note For FileAct messages, the body of the XML version 2 message does not contain the payload of the message to be transmitted. Instead, the body of the message points to the location of the payload file.

To exchange FileAct messages, XML version 2 with revision 2 or 3 is required.

For each message format, Alliance Access can read or write a batch message file on the server or on the User Space.

The File Transfer connection method supports the following message file data formats:

Data format	Purpose
Common Application Server (CAS)	CAS standards 1 and 2 which support the sub-formats ASN.1 or text encoding (only CAS version 2) Used for Network Dependent Format (NDF) or Network Independent Format (NIF). Messages transferred using the CAS 2 protocol are accepted only when Input File Format Recognition is set to Forced.
DOS-PCC	Used for batch input and output of messages, which enables you to read or write an ST200 DOS message file. Messages transferred using the DOS-PCC or RJE formats with HMAC-256 authentication are accepted only when Input File Format Recognition is set to Forced.

Data format	Purpose
MERVA/2	Used for batch transfer (to and from Mainframes) in IBM MERVA/2 format.
Remote Job Entry (RJE)	Used for batch input and output of messages in ST200 RJE format.
XML	Used for batch input and output of MX or FileAct messages, or for FpML documents..

You can find examples of the data formats that you can use with the File Transfer method in the following directory, which is beneath your installation directory:

Windows: **<Alliance installation directory>\mxs\batch_examples**

UNIX or Linux: **\$ALLIANCE/MXS/batch_examples**

Interactive

The Interactive method supports bidirectional message transfer with back-office applications according to the Common Application Server (CAS) standards 1 and 2 that support sub-formats ASN.1 or text encoding (only CAS version 2) for Network Dependent Format (NDF) or Network Independent Format (NIF).

Print

The Print method enables you to specify how to print messages in batch from Alliance Access to either a printer or a file in a user-specified directory.

Output messages can also be printed in ST200-like format, which can also include warning indications, or eye-catchers, in the header of the output.

SOAP

The SOAP connection method enables the exchange of MT, XML-based messages, and FileAct messages between Alliance Access and back-office applications. The SOAP connection method requires the licence package **14:SOAP ADAPTER** and supports only the XMLv2 data format.

The parameters that control the file transfer include a pointer to the payload file, service, receiver of the file, header information, and notification options. These file-transmission parameters are carried in an XMLv2 message.

The SOAP Host Adapter supports the exchange of FileAct messages over HTTPS in two modes:

- Full FileAct mode, where file transmission parameters and the FileAct payload are transferred in XMLv2 format and the data exchange uses Web services over HTTPS.
- Mixed FileAct mode, where the file transmission parameters are carried in an XML version 2 message that is transferred using Web services over HTTPS, whereas the FileAct payload is transferred over the local file system

WebSphere MQ

The WebSphere MQ connection method enables FIN, XML-based, or FileAct messages to be exchanged between Alliance Access and back-office applications through IBM WebSphere MQ. This connection method requires the licence package **13:MQ HOST ADAPTER**.

The WebSphere MQ method supports the following data formats:

- MQ-MT
- XML version 2, with revision Original, 1, 2, 3, or 4.

The exchange of FileAct messages over WebSphere MQ requires XML version 2, revision 2 or 3.

The WebSphere Host Adapter supports the exchange of FileAct messages over WebSphere MQ in two modes:

- Full FileAct mode - where both the XML version 2 message and the FileAct payload are transferred over WebSphere MQ.
- Mixed FileAct mode - where the XML version 2 message is transferred over WebSphere MQ, whereas the FileAct payload is transferred over the local file system.

10.2.4 Preparing the Application Interface for a Transfer Session

Purpose

Before working with the Application Interface for the first time, you must define a number of key objects.

Warning During day-to-day operations, do not open the message partner profiles or exit point profiles unless you need to modify them or add new profiles.

Automatic message partner sessions

All sessions using automatic message partners are run on the server.

All message files or parameter files that are referenced in an automatic message partner profile must be local to the server.

The operator profile of the operator who loads or moves files to the server must have the **Access Control / Files On Server** action assigned.

Preparing the Application Interface

1. Ensure that you have correctly configured and enabled message partner profiles, to control the flow of messages and files.
2. Ensure that the routing is defined and active. For example, to route messages and files to an exit point associated with a message partner profile, you must have routing rules defined to do this.
3. To change the existing default exit point profiles, you can create an exit point which stores files or message before they are transferred to a message partner.
4. Start a message partner session to transfer files or messages between Alliance Access and the message partner.

10.2.5 Status of Message Partner Sessions

Description

You can monitor message partners that have a certain communication status, such as when they are aborting or recovering. You can monitor any or all of the following session statuses:

Status	Description
Aborting	<p>The session is closing down as a result of an Abort command being issued or a serious failure, such as an authentication error. Interactive sessions may also be aborted by the message partner.</p> <p>You can use the Event log to examine the details of all abort events. Such events are classified as <code>System</code>, and are described with an abort reason and an abort text. For sessions involving the CAS protocol, the description of an event may include the expected session or sequence number.</p>
Closed	No transfer of messages is currently taking place with the message partner.
Closing	<p>The session is closing down for one of the following reasons:</p> <ul style="list-style-type: none"> An end-of-file (EOF) was reached during a batch input session All the messages queued at the exit points when the Run Session command was issued have been transferred in this batch output session A Stop Session command was issued. Note that interactive sessions may also be stopped by the message partner.
Interrupted	<p>The message partner has lost the connection to WebSphere MQ.</p> <p>Only applicable to WebSphere MQ message partners.</p>
Open	The session is active and messages are being transferred.
Opening	<p>The session is started but is not yet open.</p> <p>The Start Session command was issued and the session is initialising.</p> <p>Some sessions may be started directly by the message partner.</p> <p>This is optional for an interactive session.</p>
Recovering	The session is recovering from a session failure, such as an abort request or a system restart.

10.2.6 Message Partners Page

Content

The **Message Partners** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list of entries on the **Message Partners** page:
 - See "Message Partners" on page 302
 - See "Functions" on page 22
- Details of the message partners defined for the current Alliance Access instance
 - See "Details" on page 304
- Functions that enable you to manage the message partners
 - See "Functions" on page 322

Display

Message Partners								
Filtering Criteria								
Message Partners								
Change View	Add As	Delete	Enable	Disable	Start Session	Run Session	Stop Session	Abort Session
Name	Partner Id	Direction	Connection Method	Description	Status	Session	Session Status	
<input type="checkbox"/> FileAndOut	7	To & From Message Partner	File Transfer	File Transfer Test To and From	Enabled	0	Closed	
<input type="checkbox"/> FileInput	1	From Message Partner	File Transfer		Disabled	0	Closed	
<input type="checkbox"/> FileOutput	2	To Message Partner	File Transfer		Disabled	0	Closed	
<input type="checkbox"/> FrontCAS	14	From Message Partner	Interactive	Interactive Test From MP	Enabled	0	Closed	
<input type="checkbox"/> FrontDFA	11	From Message Partner	Direct FileAct	DirectFileAct Test From MP	Enabled	0	Closed	
<input type="checkbox"/> MVRFileInput	4	From Message Partner	File Transfer		Disabled	0	Closed	
<input type="checkbox"/> MVRFileOutput	6	To Message Partner	File Transfer		Disabled	0	Closed	

Message Partners

Message Partners		
Field	Description	Filtering criteria
Name	Specifies the Name of the message partner profile ⁽¹⁾ value to use for filtering	✓
Partner Id	Specifies the Partner Id that was automatically assigned to the message partner upon creation.	
Direction	<p>Specifies the Direction ⁽¹⁾ value to use for filtering The field determines the session direction</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • To Message Partner: output messages from Alliance Access • From Message Partner: input messages to Alliance Access This option is not available for the Print connection method. • To & From Message Partner: input and output messages This option is not available for the Direct FileAct, Print, or Websphere MQ connection methods. 	✓

Message Partners		
Field	Description	Filtering criteria
Connection Method	<p>Specifies the Connection Method ⁽¹⁾ value to use for filtering. The field determines the connection method.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • File Transfer: transfers batch files between message partners • Interactive: supports bi-directional message transfer with message partners • Direct FileAct: enables the transfer of a payload file between Alliance Access and a back-office application • Print: enables Alliance Access to print messages to a file or to a printer that is specified in the message partner profile • Websphere MQ: enables messages to be exchanged between Alliance Access and back-office applications through IBM WebSphere MQ • SOAP: enables the exchange of MT or XML-based messages between Alliance Access and back-office applications through the SOAP protocol 	✓
Status	<p>Indicates the status of the message partner profile.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Enabled: profile is approved for use • Disabled: profile is not authorised and cannot be used in a session • Disabling: a session is in progress, and will not become disabled until an operator clicks Stop Session. <p>To modify the settings of a message partner, the status must be set to Disabled and then set to Enabled for the changes to take effect.</p> <p>An Interactive Message Partner that is in the state Disabling becomes disabled only after clicking Stop Session.</p>	
Session Status	Indicates the status of the communication session for the current message partner. See "Status of Message Partner Sessions" on page 301.	
Description	The description of the message partner profile. Maximum 50 characters long	
Session (Session Identifier)	Indicates the number of the session that is still open, or of the latest session that was open with the message partner. The identifier increments by one for each consecutive session.	

(1) See "Details" on page 304

Details

Column	Description
Name	The name of the message partner profile
Direction (Allowed Direction)	<p>Determines the session direction</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • To Message Partner: output messages from Alliance Access • From Message Partner: input messages to Alliance Access <p>This option is not available for the <code>Print</code> connection method.</p> <ul style="list-style-type: none"> • To & From Message Partner: input and output messages <p>This option is not available for the <code>Direct FileAct</code>, <code>Print</code>, or <code>Websphere MQ</code> connection methods.</p>
Connection Method	<p>Determines the connection method</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • <code>File Transfer</code>: transfers batch files between message partners • <code>Interactive</code>: supports bi-directional message transfer with message partners • <code>Direct FileAct</code>: enables the transfer of a payload file between Alliance Access and a back-office application • <code>Print</code>: enables Alliance Access to print messages to a file or to a printer that is specified in the message partner profile • <code>Websphere MQ</code>: enables messages to be exchanged between Alliance Access and back-office applications through IBM WebSphere MQ • <code>SOAP</code>: enables the exchange of MT or XML-based messages between Alliance Access and back-office applications through the SOAP protocol
Description	<p>The description of the message partner profile</p> <p>Maximum 50 characters long</p>
Status	<p>Indicates the status of the message partner profile</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • <code>Enabled</code>: profile is approved for use • <code>Disabled</code>: profile is not authorised and cannot be used in a session • <code>Disabling</code>: a session is in progress, and will not become disabled until an operator clicks <code>Stop Session</code>. <p>To modify the settings of a message partner, the status must be set to <code>Disabled</code> and then set to <code>Enabled</code> for the changes to take effect.</p>
Session (Session Identifier)	<p>Indicates the number of the session that is still open, or of the latest session that was open with the message partner</p> <p>The identifier increments by one for each consecutive session.</p>

Column	Description
Session Status	Indicates the status of the communication session for the current message partner. See "Status of Message Partner Sessions" on page 301.

10.2.7 Message Partner Details Window: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details that relate to the configuration of the message partners
See "Details" on page 306
- Functions that enable you to manage the message partners
See "Functions" on page 322

Display

Message Partner Details - FileInAndOut

Configuration **Monitoring** **Help**

Name	FileInAndOut
Description	File Transfer Test To and From MP
Status	Enabled
Partner Id	7
Allowed Direction	To & From Message Partner
Connection Method	File Transfer
File Transfer	
Data Format	XML Version 2 Revision 2
Use Binary Prefix	<input checked="" type="checkbox"/>
Session Initiation	Manual
Parameter File	Not Required
File On	Server
Profile Name	R7.1_MsgPartner
Local Authentication	
Reception	
Input Filename Pattern	C:\Alliance\Access\usrdata\userspace\tes
Input Attachment Path	C:\Alliance\Access\usrdata\userspace\tes
FileAct Payload Timeout (seconds)	0
Generate Report File	No
Validation level	Maximum
Message modification	Allowed
Unit to be assigned	None
Emission expiry	Days
Batch File Validation	Continue on Rejection
Build unique file transfer reference	

Close **Refresh** **Report** **Disable** **Start Session** **Run Session** **Previous** **Next**

Details

- Generic details for message partners: see "Details" on page 304
- **Connection Method** details:
 - **File Transfer**: see "File Transfer" on page 306
 - **Interactive**: see "Interactive" on page 307
 - **Direct FileAct**: see "Direct FileAct" on page 308
 - **Print**: see "Print" on page 308
 - **WebSphere MQ**: see "WebSphere MQ" on page 309
 - **SOAP**: see "SOAP" on page 311
- **Local Authentication** details: see "Local Authentication" on page 311
- **Reception** details: see "Reception" on page 313
- **Emission** details: see "Emission" on page 317

File Transfer

Field	Description
Data Format	Determines the message transport format that the session uses
Data Format for outgoing message partners	Present when Allowed Direction is To & From Message Partner and Data Format is Automatic
Use Binary Prefix	<p>Determines if the message partner uses an XMLv2 binary prefix for local authentication (LAU). If not, and if you are using XMLv2 revision 2.0.6, you can alternatively use the XMLv2 <code>LAU</code> field tag to store binary prefix information.</p> <p>See the section on changes in revision 2.0.6 in the Configuration Guide for more information on this tag.</p> <p>For output message partners, Alliance Access adds the binary prefix (if the message partner is configured to do so), and calculates and adds the LAU. For input message partners, Alliance Access detects whether a binary prefix is present and checks the LAU data in both the binary prefix and the LAU tag, if one or both are present.</p>
Session Initiation	<p>Determines how sessions start</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Manual: operators start sessions with the message partner manually • Automatic: sessions with the message partner start automatically
Parameter File	<p>Determines whether the session uses parameter files</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Required • Not Required

Field	Description
File On	<p>Identifies the location of the file</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Server • Userspace <p>The value <code>Workstation</code> is also available for backwards compatibility only. This field is available only for <code>To</code>, <code>From</code>, and <code>To & From</code> message partners using the File Transfer connection in Manual mode.</p>
Profile Name	<p>Specifies the security definition profile that the session uses</p> <p>The entitlements and permissions of this profile allow the message partner profile to create and route input messages within Alliance Access.</p>

Interactive

Field	Description
Data Format	Determines the message transport format that the session uses
Can be started by	<p>Determines the party that starts a session</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • <code>Operator</code>: Only an Alliance Access operator can start a session • <code>Message Partner</code>: Only a message partner can start a session • <code>Operator and Message Partner</code>: Either party can start a session <p>The value selected determines which party is assigned to listen for an open session request.</p> <p>For example, if <code>Message Partner</code> is selected, then Alliance Access must constantly listen for an incoming request from the message partner.</p>
Connection Id	<p>Identifies the message partner</p> <p>Must be unique in the system</p>
Host Address	<p>Identifies the host address of the message partner</p> <p>Maximum 31 characters</p>
Window Size	<p>Determines how many messages are transmitted before a logical reply is required</p> <p>Present only when Data Format is set to a <code>CAS Version 2</code> format</p> <p>Maximum window size: 16</p>
Priority	<p>Determines the level of priority</p> <p>The system uses the value to specify the order in which the messages in concurrent output sessions are taken from the relevant exit queues and transmitted to the message partner</p> <p>Valid only when more than one output session is active and when the window size is greater than 1</p> <p>Allowed values: 0 (highest priority) to 9 (lowest priority)</p>
Session Authentication Required	<p>Determines whether to use session authentication between the Application Interface and the message partner</p> <p>See "Local Authentication" on page 311</p>

Field	Description
Profile Name	Specifies the security definition profile that the session uses The entitlements and permissions of this profile allow the message partner profile to create and route input messages within Alliance Access.

Direct FileAct

Field	Description
Session Initiation	Determines how sessions start These are the possible values: <ul style="list-style-type: none">• Manual: operators start sessions with the message partner manually• Automatic: sessions with the message partner start automatically
Profile Name	Specifies the security definition profile that the session uses The entitlements and permissions of this profile allow the message partner profile to create and route input messages within Alliance Access.

Print

Field	Description
Session Initiation	Determines how sessions start These are the possible values: <ul style="list-style-type: none">• Manual: operators start sessions with the message partner manually• Automatic: sessions with the message partner start automatically
Print To	Determines where to send the data These are the possible values: <ul style="list-style-type: none">• File• Printer
File On	Identifies the location of the file These are the possible values: <ul style="list-style-type: none">• Server• Userspace The value Workstation is also available for backwards compatibility only. Present only when Print To is set to File
Expansion language	For To message partners, specifies the language used for the field expansions of messages sent to those message partners. As well as the supported languages, the Server default value is displayed. If this value is selected, the language defined in the Expansion language global configuration parameter will be used.
Printer Location	Identifies the location of the printer: Server Present only when Print To is set to Printer

Field	Description
Printer Name	The name of the printer Present only when Print To is set to Printer

WebSphere MQ

Field	Description
Data Format	Determines the message transport format that the session uses
FileAct Mode	<p>Specifies which FileAct mode to use</p> <p>Present when Allowed Direction is From Message Partner and Data Format is set to an XML Version 2 format or if Allowed Direction is To Message Partner and Data Format is set to XML Version 2 Revision 2 or XML Version 2 Revision 3.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • FULL (Default): both the XML version 2 message and the FileAct payload are transferred between the back-office application and Alliance Access over WebSphere MQ • MIXED: the XML version 2 message is transferred between the back-office application and Alliance Access over WebSphere MQ, and the FileAct payload is transferred over the local file system
Chunk Size	<p>Specifies the maximum size of a WebSphere MQ message (in bytes) that Alliance Access can send a back-office application</p> <p>To set this value, see the System Management Guide or refer to the guidelines provided in the IBM WebSphere MQ documentation. Default value: 32768 bytes.</p> <p>Present when Allowed Direction is To Message Partner, Data Format is set to XML Version 2 Revision 2 or XML Version 2 Revision 3, and FileAct Mode is set to FULL</p>
No Segmentation	<p>If you selected FULL FileAct mode, and the payload of the file is greater than the Chunk Size, then clear the check box to ensure that the payload file is segmented before it is sent to the back-office application.</p> <p>If you select the check box, then MQ grouping is used and MQ segmentation is not used. For more information about the WebSphere MQ segmentation, see the WebSphere MQ documentation.</p> <p>Present when Allowed Direction is To Message Partner, Data Format is set to XML Version 2 Revision 2 or XML Version 2 Revision 3, and FileAct Mode is set to FULL</p>
Queue Manager Name	<p>Identifies the name of the WebSphere MQ queue manager where the WebSphere MQ queue is defined</p> <p>Maximum length: 48 characters</p>
Queue Name	<p>Identifies the name of the WebSphere MQ queue</p> <p>Maximum length: 48 characters</p>
Error Queue Name	<p>Identifies the name of the MQ Error queue</p> <p>Maximum length: 48 characters</p> <p>If you leave this field empty, then the default error queue is used.</p>

Field	Description
Transfer Access Information	<p>Determines whether the session transfers information about the Alliance Access instance which has processed the message with the message</p> <p>This is the information included:</p> <ul style="list-style-type: none"> • the name of the Alliance Access instance • the exit point the message was taken from (for emission profiles) • the routing point where the message ended (for reception profiles) • the owner of the Alliance Access instance • the unit to which the message belongs
Use MQ Descriptor	<p>Determines how the session sends the Alliance Access information to the message partner:</p> <ul style="list-style-type: none"> • If you select the check box, then the MQ Message Descriptor part carries the Alliance Access information. • If you clear the check box, then the MQ Message Data part carries the Alliance Access information. <p>Present only when Transfer Access Information is selected</p>
Use Binary Prefix	<p>Determines if the message partner uses an XMLv2 binary prefix for local authentication (LAU). If not, and if you are using XMLv2 revision 2.0.6, you can alternatively use the XMLv2 <code>LAU</code> field tag to store binary prefix information.</p> <p>See the section on changes in revision 2.0.6 in the Configuration Guide for more information on this tag.</p> <p>In the From SWIFT direction, Alliance Access adds the binary prefix (if the message partner is configured to do so) and checks the LAU data from either the prefix (which can be of any XMLv2 revision) or the LAU tag (if XMLv2 revision 2.0.6 is used), or both. If both are used, both are checked.</p> <p>In the To SWIFT direction, Alliance Access detects whether a binary prefix is present and checks the LAU data in both the binary prefix and the LAU tag, if one or both are present.</p>
Session Initiation	<p>Determines how sessions start</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Manual: operators start sessions with the message partner manually • Automatic: sessions with the message partner start automatically
Keep Session Open	<p>Determines whether Alliance Access automatically recovers a failed connection with WebSphere MQ. In addition, if selected, then an output WebSphere MQ message partner can be scheduled to start the session automatically based on the time defined in Run Output Session Triggers.</p>
Generate unique MQ Message ID	<p>If this check box is selected, Alliance Access generates a unique MQ message ID by appending the message instance number to the SUMID. If it is not selected, the message instance number is not appended to the SUMID.</p>

Field	Description
Expansion language	<p>For To message partners, specifies the language used for the field expansions of messages sent to those message partners.</p> <p>This field is displayed only if the Data Format field (in the Emission block) is set to MQ-MT. It is available only when the Message emission format field or the Original message format field is set to Expanded.</p> <p>As well as the supported languages, the Server default value is displayed. If this value is selected, the language defined in the Expansion language global configuration parameter will be used.</p>
Profile Name	<p>Specifies the security definition profile that the session uses</p> <p>The entitlements and permissions of this profile allow the message partner profile to create and route input messages within Alliance Access.</p>

SOAP

Field	Description
Data Format	<p>Determines the message transport format that the session uses:</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • XML Version 2 Revision 2 • XML Version 2 Revision 3
FileAct Mode	<p>Specifies the mode in which to transfer FileAct messages</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Full (Default) - to transfer both the XMLv2 message that contains the file-transmission parameters and the FileAct payload over SOAP • Mixed - to transfer the XMLv2 message that contains the file-transmission parameters over SOAP and to transfer the FileAct payload over the local file system.
Window Size	Determines how many messages are transmitted before a logical reply is required
Profile Name	<p>Specifies the security definition profile that the session uses</p> <p>The entitlements and permissions of this profile allow the message partner profile to create and route input messages within Alliance Access.</p>

Local Authentication

Field	Description
Local Authentication	Determines whether the session uses local authentication between the Application Interface and the message partner

Field	Description
Authentication Method	<p>Specifies which authentication method to use for the communication session:</p> <ul style="list-style-type: none"> • HMAC-SHA256 • SA2 <p>Present only when:</p> <ul style="list-style-type: none"> • The connection method is File Transfer, and the data format is either DOS-PCC or RJE. Ensure that the Data Format is set to DOS-PCC or RJE, (not "Automatic"). • The connection method is WebsSphere MQ, and the data format is either MQMT.
Key Type	<p>Determines whether session authentication uses unidirectional or bidirectional keys</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Unidirectional: uses two different keys, one to authenticate the output sessions and another to authenticate the input sessions • Bidirectional: uses the same key to authenticate the output and the input sessions <p>Present when Allowed Direction is To & From Message Partner</p>
Send Key First Part / Send Key Second Part	<p>The first / second 16 characters of the key to authenticate the output sessions</p> <p>The two parts together form a 32 character hexadecimal string.</p> <p>Present only when Allowed Direction is To Message Partner or To & From Message Partner and Key Type is set to Unidirectional</p>
Receive Key First Part / Receive Key Second Part	<p>The first / second 16 characters of the key to authenticate the input sessions</p> <p>The two parts together form a 32-character hexadecimal string.</p> <p>Present only when Allowed Direction is From Message Partner or To & From Message Partner and Key Type is set to Unidirectional</p>
Key First Part / Key Second Part	<p>The first / second 16 characters of the key to authenticate the output and the input sessions</p> <p>The two parts form a 32-character hexadecimal string.</p> <p>Present only when Allowed Direction is To & From Message Partner and Key Type is set to Bidirectional</p>
Show Clear Text	<p>Determines whether the system displays the authentication keys</p> <p>By default, the system does not display the authentication keys. This is to help prevent unauthorised users reading the authentication key information "from over your shoulder".</p>

Reception

Field	Description	Applicability				
		File Transfer	Interactive	Direct FileAct	WebSphere MQ	SOAP
Requestor DN	The requestor DN	x	x	✓	x	x
Responder DN	The responder DN	x	x	✓	x	x
Service	The SWIFTNet service name	x	x	✓	x	x
Request Type	The request type	x	x	✓	x	x
Input Filename Pattern	Specifies the location from which the system transfers the input files If File On is set to <code>Userspace</code> , then you can use [? ...] to select the path that you require (see "Choose Directory" on page 25).	✓	x	x	x	x
Input Attachment Path	Specifies the location from which the system reads the payload files If File On is set to <code>Userspace</code> , then you can use [? ...] to select the path that you require (see "Choose Directory" on page 25).	✓ ⁽¹⁾	x	✓	✓ ⁽¹⁾	✓
FileAct payload timeout (seconds)	Alliance Access accepts a delay equivalent to this timeout between the reception of the XMLv2 message and the availability of the file payload itself before considering that it is missing. The minimum value is 0 and the maximum value is 900. By default, the value is set to 0 when creating a new message partner.	✓	x	x	✓	✓
Generate Report File	Determines whether the system generates a report on the processing of the input file These are the possible values: <ul style="list-style-type: none">• <code>No</code>: does not generate a report• <code>Failure</code>: generates a report only if an error occurs• <code>Failure or Success</code>: always generates a report	✓ ⁽¹⁾	x	x	x	x
FIFO	Determines whether the system adds the messages received from the back-office application in FIFO (First In First Out) order	x	x	x	x	✓

Field	Description	Applicability				
		File Transfer	Interactive	Direct FileAct	WebSphere MQ	SOAP
Validation level	<p>Determines the level of validation the session performs on the text block of each input message.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Maximum: performs the same validation as Medium Provided as a possible future level of message validation • Medium: performs syntactical validation at the field level Checks for the presence of mandatory fields, keyword validation, limits, ranges of values, and so on If validation fails, then the system generates a negative reply and sends it to the message partner • Minimum: performs validation and extraction of some keywords (for example: currency, amount, value date) • No Validation: performs no validation <p>For more information about the impact of a specific level, see "Levels of Validation" on page 759.</p>	✓	✓	✓	✓	✓
Extended error text	<p>When this check box is selected, Alliance Access returns an extended error text in the MQ response, in the case of a message validation error. This text contains the same 'reason' text as in the logged event.</p> <p>When creating a new message partner, it is not selected by default.</p>	x	x	x	✓	x
Message modification	<p>Determines whether operators can modify the text of input messages</p> <ul style="list-style-type: none"> • Allowed: operators can modify messages that have failed validation • Prohibited: operators cannot modify messages 	✓	✓	x	✓	✓
Unit to be assigned	Specifies the unit to which the session assigns all incoming messages	✓	✓	✓	✓	✓
UUMID included in Original Message	Determines whether the session includes a UUMID in the messages	x	x	x	✓ (2)	x
Create Repair Message	<p>Determines whether the session creates a repair message upon reception of a transmission notification</p> <p>Present only when Connection Method is WebSphere MQ and licence option 07:STANDALONE REC is installed</p>	x	x	x	✓	x

Field	Description	Applicability				
		File Transfer	Interactive	Direct FileAct	WebSphere MQ	SOAP
Emission Expiry	<p>For From and From & To message partners, a time interval field that enables you to request Alliance Access to send all FileAct and InterAct messages received from the back office by means of that message partner before an absolute date and time, which is calculated as follows: date/time of the message creation in the database plus the value of this field (a relative value in days, hours and/or minutes expressed as d, h, m). This applies only to messages sent to real-time InterAct and FileAct services. Alliance Access stops emission attempts after that absolute date/time, in the event that emissions repeatedly fail.</p> <p>This field is optional and has a maximum value of 30 days. If present, this field cannot be set to 0.</p>	✓	✓	✓	✓	✓
Batch File Validation	<p>Determines whether transfers continue if validation errors occur during input</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Abort on Rejection: the session aborts if an error occurs Continue on Rejection: the session continues if an error occurs 	✓	x	x	x	x
Build unique file transfer reference	<p>Determines whether to attach a unique reference to the ACKs and NAKs that are received back from SWIFT in response to the input messages</p> <p>The references enable the back-office application to reconcile the messages that it has sent to SWIFT with the acknowledgements that it receives from Alliance Access.</p> <p>The reference is included as part of the S block of the ACK or NAK, and contains the following:</p> <ul style="list-style-type: none"> input file name sequence number of the message number of messages in the input file <p>The unique message reference is constructed as follows: <Input batch filename>/<sequence number of the message>/<number of messages in the batch file></p> <p>The maximum permitted length of the generated reference is 46 characters. Therefore, when configuring the message partner with this reference, in order to avoid the session aborting with the error "File name too long", limit the length of the file name to 32 characters, as described in the Daily Operations Guide.</p> <p>When the message partner is not configured with this reference, limit the length of the file name to 89 characters.</p>	✓	x	x	x	x

Field	Description	Applicability				
		File Transfer	Interactive	Direct FileAct	WebSphere MQ	SOAP
Priority	<p>These are the possible values:</p> <ul style="list-style-type: none"> Normal Urgent 	x	x	✓	x	x
Routing	<p>Determines how the system routes messages that do not contain disposition information</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Route: routes the messages according to the routing rules that the Application Interface Inbound queue specifies Dispose: disposes the messages to the corresponding message preparation queue according to the value set in message in <p>For more information about setting these values, see "Message Validation and Disposition Overview" on page 758.</p>	✓	✓	✓	✓	✓
message in	<p>Specifies the default queue to which the system disposes messages that do not contain disposition information</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Modification Verification Authorisation Ready To Send <p>Present only when Routing is set to Dispose</p>	✓	✓	✓	✓	✓
Report Content	<ul style="list-style-type: none"> Transfer UUMID Original Message Validation Error Code <p>Present only when Connection Method is WebSphere MQ and if Data Format is MQ-MT</p>	x	x	x	✓	x
File Info	Provides information about the payload file. Routing rules can be defined to route messages based on the content of this field.	x	x	✓	x	x
File Description	Provides information about the content of the payload file. Routing rules can be defined to route messages based on the content of this field. It is a free-text field.	x	x	✓	x	x
Transfer Info	Provide information about a file transfer. Routing rules can be defined to route messages based on the content of this field.	x	x	✓	x	x

Field	Description	Applicability				
		File Transfer	Interactive	Direct FileAct	WebSphere MQ	SOAP
Transfer Description	Provide information about a file transfer. Routing rules can be defined to route messages based on the content of this field.	x	x	✓	x	x
Header Info		x	x	✓	x	x

(1) Present only when **Data Format** is set to an XML Version 2 format or Automatic

(2) Present only when **Data Format** is set to MQ-MT, see "WebSphere MQ" on page 309

Emission

Field	Description	Applicability					
		File Transfer	Interactive	Direct FileAct	Print	WebSphere MQ	SOAP
Exit Points	<p>Specifies the exit points to use:</p> <ul style="list-style-type: none"> • Available contains the list of exit points available • Selected contains the exit points that you assign to the message partner 	✓	✓	✓	✓	✓	✓
Filename Pattern	Present only when Connection Method is Print	x	x	x	✓	x	x
Output Filename Pattern	<p>Specifies the location to which the system writes the output files</p> <p>If File On is set to <code>Userspace</code>, then you can use Choose Directory to select the path that you require (see "Choose Directory" on page 25).</p>	✓	x	x	x	x	x
Maximum number of messages per session	<p>Specifies the maximum number of messages that Alliance Access can put in a file that is sent to the back office or printed to a printer or file. This value applies regardless of whether the session is manual (run session only) or automatic. The minimum value is 0, and there is no maximum value. This field is optional (except in the case of defining an LTA command for Direct FileAct, when it must be set to 1).</p> <p>If a non-zero value is specified, Alliance Access groups messages into batches of no more than the number defined in this field. If 0 is specified, the feature is disabled and Alliance Access groups messages into batches in the same way as before Alliance Access 7.0.60.</p>	✓	x	✓	✓	x	x

Field	Description	Applicability					
		File Transfer	Interactive	Direct FileAct	Print	WebSphere MQ	SOAP
Output Attachment Path	<p>Specifies the location to which the system writes the payload files</p> <p>If File On is set to <code>Userspace</code>, then you can use Choose Directory to select the path that you require (see "Choose Directory" on page 25).</p>	✓ (1)	x	✓	x	✓ (1)	✓
Output Attachment Extension	Specifies the optional extension of the payload file. The extension has 20 characters maximum.	✓ (1)	x	✓	x	✓ (1)	✓
Local transfer command	Specifies the user-defined executable that handles the message files once they reach the back-office application	✓	x	✓	✓	x	x
Command Parameters	Specifies the parameters for the Local transfer command executable	✓	x	✓	✓	x	x
Always transfer MAC/PAC	<p>Determines whether Alliance Access adds dummy MAC/PAC trailer value (00000000) to a message if it does not contain a MAC/PAC trailer.</p> <p>This option is available to support back-office applications that require MAC/PAC trailers.</p>	✓ (2)	✓ (3)	x	x	✓	x
Transfer PKI Signature	<p>Determines whether the system transfers PKI signatures when sending FIN messages to the message partner</p> <p>The PKI signature is always transferred for messages in XML version 2 format.</p> <p>If a back-office application is ready to receive PKI signatures, then you must select the Transfer PKI Signature option.</p>	✓ (4)	✓ (3)	x	x	✓ (5)	x
Remove S-Block	Removes the S-Block from the MQ Message Data part of the message, which is transferred over FileAct to the message partner. The S-block is also removed from the original message if it is transferred.	x	x	x	x	✓ (5)	x
Transfer UUMID	Determines whether the system transfers the UUMID with the message to the message partner	x	x	x	x	✓ (5)	x
Increment Sequence Number across Sessions	Determines whether the system uses continuous sequence numbers	✓	✓ (6)	x	✓	✓ (6)	✓ (6)
Routing Code Transmitted	Determines whether the session transmits the routing code to the message partner	✓ (10)	x	x	✓	✓ (5)	x

Field	Description	Applicability					
		File Transfer	Interactive	Direct FileAct	Print	WebSphere MQ	SOAP
Message Emission Format	<p>Determines which message layout format the system uses</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Complete Text: outputs the headers and the message text in non-expanded layout • Expanded: outputs the headers and the message text in expanded layout 	✓ (7)	✓ (8)	x	x	✓ (5)	x
Transfer Original Message with Notification	<p>Determines whether the system appends the original message to the notification</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Created by another Message Partner: appends the original message when a message partner that did not create the original message requires a notification • Message Modified: appends the original message if it is subsequently modified • Always: appends the original message for all notifications • Never: does not append the original message for any notification 	✓	✓	✓ (6)	✓	✓	✓
Maximum number of messages per session	<p>Specifies the maximum number of messages that Alliance Access can put in a file that is sent to the back office or printed to a printer or file. This value applies regardless of whether the session is manual or automatic. The minimum value is 0, and there is no maximum value. This field is optional.</p> <p>If a non-zero value is specified, Alliance Access groups messages into batches of no more than the number defined in this field. If 0 is specified, the feature is disabled and Alliance Access groups messages into batches in the same way as before Alliance Access 7.0.60.</p>	✓	x	x	✓	x	x

Field	Description	Applicability					
		File Transfer	Interactive	Direct FileAct	Print	WebSphere MQ	SOAP
Original Message Format	<p>Determines how much of the original message content the system includes in the notification</p> <p>These are the possible values (depending on the connection method and data format, some options are not available):</p> <ul style="list-style-type: none"> • Minimum Info: includes the minimum information needed for traffic reconciliation with the message partner • Headers Only: includes only the headers • Complete Text: includes the headers and the message text in non-expanded layout 	✓ (7)	✓ (8)	x	x	✓	✓
Include all FIN Blocks	<p>Determines the content of the Body element for MT messages</p> <p>If the check box is selected, then the Body element contains all the FIN blocks (1, 2, 3, 4, 5) of the MT message.</p> <p>If the check box is not selected, the Body element contains the block 4 of the MT message.</p>	✓ (9)	x	x	x	✓ (9)	✓ (9)
Run Output Session Triggers:	<p>Determines how the sessions start</p> <p>Present only when Session Initiation is set to Automatic</p> <ul style="list-style-type: none"> • Number of messages • Or at (hh:mm) <p>The number of queued messages that triggers a session to start. If you specify 0, the feature is disabled.</p> <p>The time at which the session starts</p> <p>You can add several times.</p> <p>Use Add and Remove to add or remove values</p>	✓	x	x	✓	✓	x

- (1) Present only when **Data Format** is set to XML Version 2 Revision 2 or XML Version 2 Revision 3
- (2) Not present when **Data Format** is set to a CAS Version 1 format, XML Version 1, or Automatic
- (3) Present only when **Data Format** is set to a CAS Version 2 format
- (4) Not present when **Data Format** is set to a CAS Version 1 format, an XML format, or Automatic
- (5) Present only when **Data Format** is set to MQ-MT
- (6) Read only
- (7) Present only when **Data Format** is set to a CAS Version <n> Network Independent format, XML Version 2, or Automatic
- (8) Present only when **Data Format** is set to a CAS Version <n> Network Independent format
- (9) Present only when **Data Format** is set to XML Version 2 Revision 3
- (10) Present only when **Data Format** is set to DOS PCC, MERVA/2, RJE, or XML Version 1

10.2.8 Message Partner Details Window: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details that relate to the monitoring of the message partners

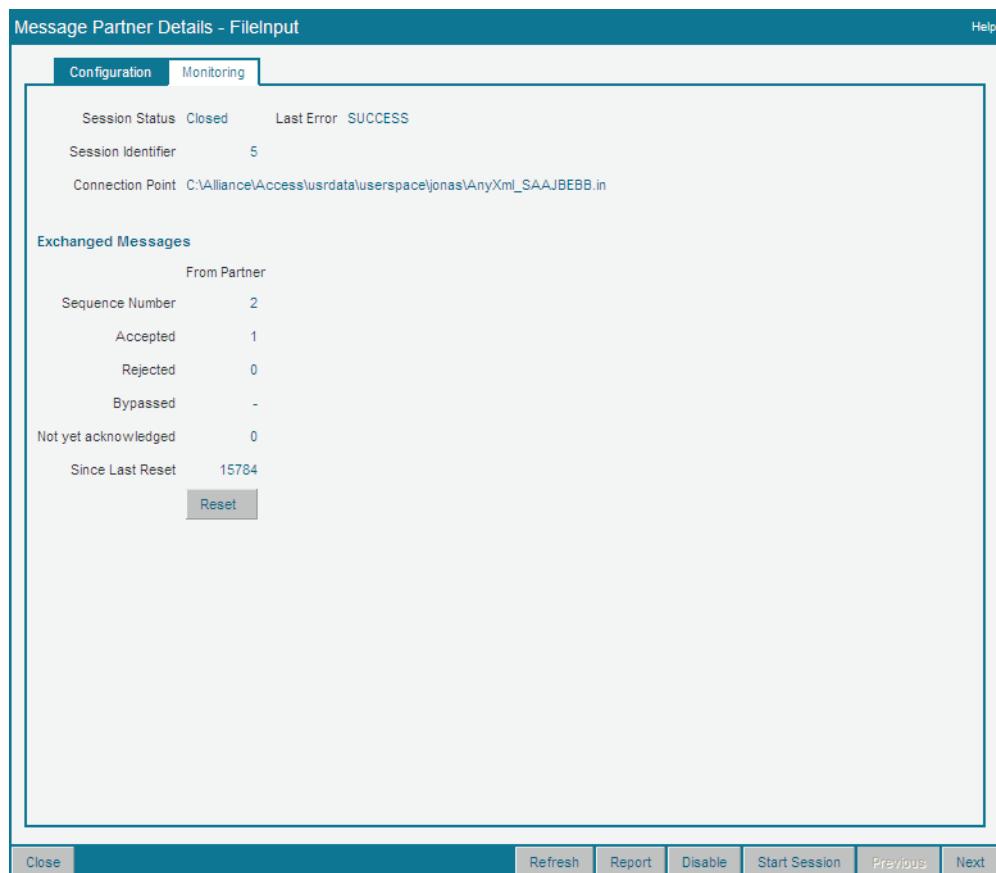
See "Details" on page 321

The details available on the **Monitoring** tab of the **Message Partner Details** window are all read only.

- Functions that enable you to manage the message partners

See "Functions" on page 322

Display



Details

Generic Details for Monitoring

Field	Description
Session Status	See Session Status in "Details" on page 304
Session Identifier	See Session Identifier in "Details" on page 304
Connection Point	Indicates the location of the message file or parameter file

Field	Description
Last Error	Shows the last error that occurred during the last session

Exchanged Messages

Field	Description
Sequence Number	Shows the sequence number of the next message expected to be processed during this session for both Input (from MP) and Output (to MP) sessions
Accepted	Shows the number of messages that have been accepted for both Input (from MP) and Output (to MP) sessions During file transfer, the entire file must be read in and processed before a number appears here. The messages are routed only when the entire file is read in.
Rejected	Shows how many messages have been rejected so far in the current session for both Input (from MP) and Output (to MP) sessions Rejection can occur for a number of reasons, for example, message syntax errors. The reason for the rejection of a message is logged in the event log.
Bypassed	Shows the number of output messages that were bypassed (and completed) in a "To Message Partner" session Messages are bypassed when the output data format selected for the exchange is one that does not support certain types of message, for example, RJE does not support notifications. When an unsupported type of message appears at the exit point it is moved to the text modification queue and completed. Each message bypass is recorded as an event in the event log.
Not yet acknowledged	Shows the number of processed messages that are waiting to be "Accepted" for both Input (from MP) and Output (to MP) sessions Acceptance only occurs when the entire file has been processed.
Since Last Reset	Shows the number of messages processed since the last reset of the counters

10.2.9 Message Partner Functions

Overview

These functions enable you to manage message partners.

Functions

Function	Description	Message Partners page	Message Partner Details window
Add / Add As	<p>Enables you to add a new message partner entity</p> <p>When no entity is selected:</p> <ul style="list-style-type: none"> Add: Opens a Message Partner Details window with all the values set to default <p>When an entity is selected:</p> <ul style="list-style-type: none"> Add As: Opens a Message Partner Details window and populates the fields with the values from the selected message partner entity <p>Procedure: "Add Entities" on page 26</p>	✓	x

Function	Description	Message Partners page	Message Partner Details window
Delete	Deletes the disabled message partner or message partners selected	✓	x
Enable	Enables the message partner or message partners selected	✓	✓
Disable	Disables the message partner or message partners selected	✓	✓
Start Session	Enables you to start a message partner session Procedure: "Start a Session" on page 326	✓	✓
Run Session	Enables you to run a message partner session Procedure: "Run a Session" on page 328	✓	✓
Stop Session	Enables you to stop a message partner session Procedure: "Stop a Session" on page 329	✓	✓
Abort Session	Enables you to abort a message partner session Procedure: "Abort a Session" on page 330	✓	✓
Reset	Resets the message counters	x	✓

10.2.10 Start Session / Run Session Window

Content

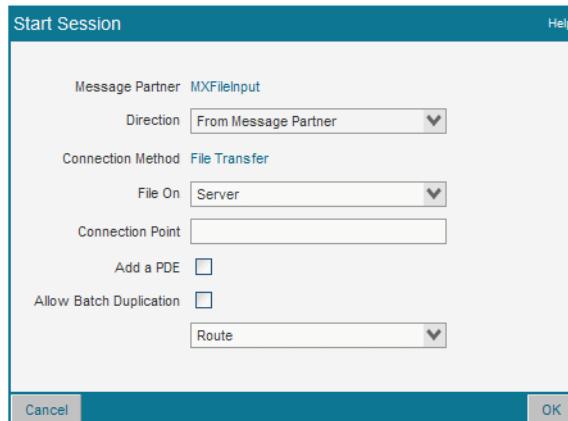
The **Start Session** and **Run Session** windows contain these elements:

- Details of the message partner session

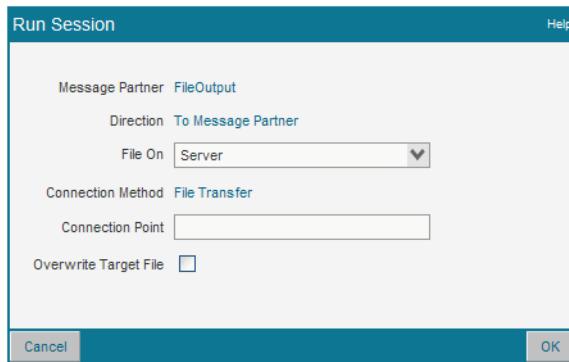
See "Details" on page 324

Display

Start Session window



Run Session window



Details

Field	Description
Message Partner	Read-only. The name of the message partner profile.
Direction	Read-only. Determines the session direction.
Connection Method	Read-only. Determines the connection method as set in the message partner profile.
File On	<p>Identifies the location of the file</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Server • Userspace <p>The value <code>workstation</code> is also available for backwards compatibility only.</p>
Connection Point	Indicates the location of the message file or parameter file
Add PDE	For input sessions, used to force a Possible Duplicate Emission trailer to each of the messages
Allow Batch Duplication	For input sessions, used to allow file duplication for batch input sessions using a parameter file
Overwrite Target File	For output sessions, used to overwrite a duplicate file
Route / Dispose	<p>Present for input sessions</p> <p>If you select <code>Dispose</code>, then the following values are available:</p> <ul style="list-style-type: none"> • Modification • Verification • Authorisation • Ready To Send

10.2.11 Add a Message Partner

Purpose

This procedure enables you to add a message partner profile for a specific connection method.

Users and permissions

To display the list or the details of message partners, or filter the list, your operator profile must have this action:

- **Applic. Interface / Open/Print Partner**

To add a message partner, your operator profile must have the following additional actions:

- **Applic. Interface / Add Partner**
- **Access Control / Files on User Space**
- **Access Control / Files on Server**

Procedure

1. From the list of message partners, click **Add**.

You can also add a message partner using the characteristics of an existing message partner. Select the check box of a message partner, and click **Add As**.

The **Message Partner Details** window opens.

2. In the **Name** field, type the name of the message partner.

Once created, you cannot change the name of the message partner.

3. In the **Description** field, type a description.

4. Specify the connection method in the **Connection Method** drop-down list.

5. Specify the direction of the message flow for the connection method in the **Allowed Direction** drop-down list.

6. Fill in the following:
 - connection method details
 - local authentication details
 - – reception details, when **Allowed Direction** is **From** message partner
 - emission details, when **Allowed Direction** is **To** message partner

See "Details" on page 306 for more information.

7. Click **Save**.

A status popup message appears. The message partner is created with the status **Disabled**.

8. Click **Close**.

9. Next, enable the message partner, to allow it to be used in a communication session.

10.2.12 Enable or Disable a Message Partner

Purpose

This procedure describes how to enable or disable a message partner.

You must enable a message partner to allow it to be used in a communication session.

You must disable a message partner before you can change its details.

Users and permissions

To display the list or the details of message partners, or filter the list, your operator profile must have this action:

- **Applic. Interface / Open/Print Partner**

To enable or disable a message partner, your operator profile must have the following additional actions:

- **Applic. Interface / Enable Mess. Partner**
- **Applic. Interface / Open/Print Partner**

To enable a message partner

1. From the list of message partners, select the check box of one or several message partners in the left column.
2. Click **Enable**.

When an operator tries to enable a message partner, then an error message appears if the message partner is configured incorrectly.

To disable a message partner

1. From the list of message partners, select the check box of one or several message partners in the left column.
 2. Click **Disable**.
- If the selected message partner has a session enabled which was started by clicking **Start Session**, then the session stays in a **Disabling** status until an operator clicks **Stop Session**.

10.2.13 Start a Session

Purpose

This procedure starts an input session or an output session manually with a message partner.

Tip If the session does not use the File Transfer connection method, then the session stays open until an operator stops it explicitly. To start a session that stops automatically, use **Run Session** instead. For more information, see "Run a Session" on page 328.

After an operator starts a session, Alliance Access transfers all the messages that are queued for exchange with the message partner. If new messages arrive at the inbound queue or outbound queue while the session is still open, then Alliance Access also transfers those messages.

The session stops in the following circumstances:

- An operator stops the session.
- An error occurs from which the session cannot recover.
- If the connection method is File Transfer with the data formats, File, RJE, MERVA/2, or CAS, then the session stops automatically after the file input is complete.

Tip	This command is not available for SOAP sessions. It is always the back-office application that starts a SOAP session with Alliance Access.
------------	--

Starting output sessions

If the output session is a Print session that was started by clicking **Start Session**, then an operator must stop the session before the print job is spooled to the printer.

When the connection method is File Transfer, Alliance Access does not transfer the notification of output messages or copies of input messages. An operator can only print these notifications or copies.

Add a Possible Duplicate Emission flag

Sometimes with input sessions, it may be necessary to retransmit a batch file. In such cases, it is essential that a Possible Duplicate Emission trailer is added to each of the messages. By default, no Possible Duplicate Emission trailer is added.

SWIFT recommends that you avoid situations where the messages in one batch are identical with those of another batch.

Note	Automatic input sessions reject all input files with CRC matches. These files are moved into the Automatic Input Error Directory. For more information about the error directory, see "Recovery of Batch Sessions" on page 562.
-------------	---

Users and permissions

To display the list or the details of message partners, or filter the list, your operator profile must have this action:

- **Applic. Interface / Open/Print Partner**

To start sessions, your operator profile must have the following additional actions:

- **Applic. Interface / Start Session**
- **Access Control / Files on User Space**

Also, the list of allowed message partners for the operator must contain the selected message partner.

Procedure

1. Select the check box of the message partner for which you want to start a session.
 2. Click **Start Session**.
- The **Start Session** window opens.
3. Select the value for **File On**, as necessary.
 4. Specify the value for **Connection Point**, as necessary.
 5. Select **Add a PDE**, as necessary.
 6. Select **Allow Batch Duplication**, as necessary.
 7. Select **Route** or **Dispose** from the drop-down list, as necessary.
 8. If you set to **Dispose**, then select the value for **To**, as necessary.

9. Click **OK**.

A status popup message appears.

The **Start Session** window closes.

The system transfers all messages that are ready to be sent for the direction **From MP**.

Depending on the direction and connection method, the session remains open so that all new messages that appear are also transferred.

10.2.14 Run a Session

Purpose

This procedure starts an output session manually with the message partner, automatically closes after a certain number of messages are transferred.

Tip To start an input session manually, follow the procedure, "Start a Session" on page 326.

After an operator runs a session, Alliance Access records the number of messages that are waiting in an output queue to be sent to a message partner. Then, Alliance Access transfers those messages.

The session stops in the following circumstances:

- Alliance Access automatically stops the session after it has sent the pre-recorded number of messages (even if new messages have been queued since the session was started).
- An operator stops the session.
- An error occurs from which the session cannot recover.

Any new messages which are queued during the session are held there until a session is run again for that message partner.

When the connection method is File Transfer, Alliance Access does not transfer the notification of output messages or copies of input messages. An operator can only print these notifications or copies.

Applicability

This command is not available for SOAP sessions. It is always the back-office application that starts a SOAP session with Alliance Access.

This procedure is only applicable for output sessions that use the connection methods **File Transfer, Direct FileAct, or Print**.

WebSphere MQ message partners exhibit the following behaviour:

- If the **Keep session open** option is selected, then the session will be started automatically but will remain open, even though the start was triggered by **Run Session**.
- If the **Keep session open** option is not selected, then the session will be started automatically and will be closed as soon as all messages are processed.

In addition, if the message partner is configured to run an output session based on triggers (number of messages or at a specific time) and there are no messages to process:

- If the **Keep session open** option is selected, then the session will be started automatically and the session will remain open.
- If the **Keep session open** is not selected, then the session will not be started automatically.

Users and permissions

To display the list or the details of message partners, or filter the list, your operator profile must have this action:

- **Applic. Interface / Open/Print Partner**

To run message partner sessions, your operator profile must have the following additional actions:

- **Applic. Interface / Run Session**
- **Access Control / Files on User Space**

Also, the list of allowed message partners for the operator must contain the selected message partner.

Procedure

1. Select the check box of the message partner for which you want to run a session.
 2. Click **Run Session**.
- The **Run Session** window opens.
3. Select the value for **File On**, as necessary.
 4. If the **Connection Method** is one of the following:
 - **File Transfer**, then type the location of the message file or parameter file in the **Connection Point** field.
 - **Print** (for print-to-file), then verify the target directory or file for printed reports is correctly specified in the **Connection Point** field.

Tip Do not type *, because it is not a valid file name.

5. Select **Overwrite Target File**, as necessary.
6. Click **OK**.

A status popup message appears.

The system first counts the number of messages that are waiting at assigned exit point and then transfers those messages. It then stops the session when this pre-recorded number of messages has been processed. Any new messages which are queued during the session are held there until the next time a session is started.

10.2.15 Stop a Session

Purpose

This procedure enables you to stop message partner sessions.

Users and permissions

To display the list or the details of message partners, or filter the list, your operator profile must have this action:

- **Applic. Interface / Open/Print Partner**

To stop message partner sessions, your operator profile must have the following additional action:

- **Applic. Interface / Stop Session**

Also, the list of allowed message partners for the operator must contain the selected message partner.

Procedure

1. Select the check box of the message partner for which you want to stop a session.

2. Click **Stop Session**.

The **Stop Session** window opens.

3. Click **OK**.

A status popup message appears.

The **Stop Session** window closes.

After the completion of any active message or message file transfer, the current active session is closed.

If **Allowed Direction** is set to **From Message Partner** and **Session Initiation** is set to **Automatic**, then the communication session re-opens automatically. To prevent this, you must disable the message partner.

10.2.16 Abort a Session

Purpose

This procedure enables you to stop message partner sessions immediately.

It is not possible to stop sessions for these message partners:

- Message partners that use the **SOAP** connection method
- Message partners that use the **Interactive** connection method

Users and permissions

To display the list or the details of message partners, or filter the list, your operator profile must have this action:

- **Applic. Interface / Open/Print Partner**

To abort message partner sessions, your operator profile must have the following additional action:

- **Applic. Interface / Abort Session**

Also, the list of allowed message partners for the operator must contain the selected message partner.

Procedure

1. Select the check box of the message partner for which you want to abort a session.

2. Click **Abort Session**.

The **Confirm Abort** window opens.

3. Click **OK**.

A status popup message appears.

The **Confirm Abort** window closes.

Any messages that have already been exchanged are removed and a recovery of the session takes place automatically.

10.2.17 Delete a Message Partner

Purpose

This procedure describes how to delete a message partner.

Warning Since the name of the message partner is used for recovery purposes during Alliance Access startup, a message partner may not be deleted and re-created with the same name until all messages sent or received by the initial message partner have been archived.

Users and permissions

To display the list or the details of message partners, or filter the list, your operator profile must have this action:

- **Applic. Interface / Open/Print Partner**

To delete a message partner, your operator profile must have the following additional action:

- **Applic. Interface / Rem Partner**

Prerequisites

Before you delete a message partner profile, you must take the following actions:

- ensure that the message partner is not assigned to an exit point
- disable the message partner, if it is not already disabled
- check that no routing rule includes the message partner (keyword **Src_entity**) in its conditional trigger criteria.

Procedure

1. From the list of message partners, select the check box of the message partner that you want to delete in the left column.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

The **Delete Confirmation** window closes.

A status popup message appears.

11 SWIFTNet Interface

11.1 FIN Delivery Subsets

11.1.1 Delivery Subsets: Definition

What are delivery subsets?

FIN delivery subsets enable you to control the order in which you receive output messages from the SWIFT network. A receiving user can define delivery subsets specifying how messages are to be delivered to that destination. The messages addressed to that destination are then queued by the system in the defined delivery subsets. The delivery criteria that can be specified include message priority, message category, message type (and service code for FINCopy), branch code, and the presence of field 13C. You may also choose to receive certain queued messages in value date order.

Alliance Access provides you with the possibility of specifying user-defined delivery subsets for a destination.

In the absence of user-defined delivery subsets, messages are queued in three default subsets:

- System
- Urgent
- Normal

11.1.2 FIN Delivery Subsets Page

Content

The **FIN Delivery Subsets** page contains these elements:

- A filtering criterion and filtering functionality that enable you to filter the list entities on the **FIN Delivery Subsets** page:
 - See "Details" on page 334
 - See "Functions" on page 22
- Details of the available delivery subsets
 - See "Details" on page 334
- Functions that enable you to manage the delivery subsets
 - See "Functions" on page 334

Display

FIN Delivery Subsets

Filtering Criteria

Destination:

Clear Submit Report

FIN Delivery Subsets Rows in list: 20 , in selection: 1

Change View Redefine Report Previous Next

<input type="checkbox"/>	Destination	Current Subsets	Future Subsets	Status
<input type="checkbox"/>	SAAABEBO	SYSTEM, URGENT, NORMAL	SYSTEM, URGENT, NORMAL	Wait MT 047 resp
<input checked="" type="checkbox"/>	SAAABEBB	SYSTEM, URGENT, NORMAL	SYSTEM, URGENT, NORMAL	No change
<input type="checkbox"/>	SAABBEBO	SYSTEM, URGENT, NORMAL	SYSTEM, URGENT, NORMAL	No change
<input type="checkbox"/>	SAABEBBB	SYSTEM, URGENT, NORMAL	SYSTEM, URGENT, NORMAL	No change

Details

Column	Description	Filtering criteria
Destination	The destination BIC-8 for which the delivery subsets are defined	✓
Current Subsets	The current delivery subsets defined for the destination	
Future Subsets	The future delivery subsets. If you did not create any new subset, the list is the same as the Current Subsets list.	
Status	<p>The status of the delivery subsets defined for the destination.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • No change: No change since the last MT 047 message was sent. • Wait MT 047 resp: Waiting for a response to the MT 047 message (Delivery Instructions Redefinition Request) generated by Alliance and sent to the network to request the replacement of the currently used delivery subset by those in the Future Subsets list. • Modified: A modification to the future subsets has occurred since the last MT 047 message was sent. • Invalid: A delayed NAK (MT 015) to the MT 047 request was sent by FIN to inform you that the request was cancelled. Refer to the FIN System Messages guide for more details. 	

Functions

Function	Description
Redefine	Enables you to redefine the delivery subsets for a destination Procedure: "Redefine a Delivery Subset" on page 342

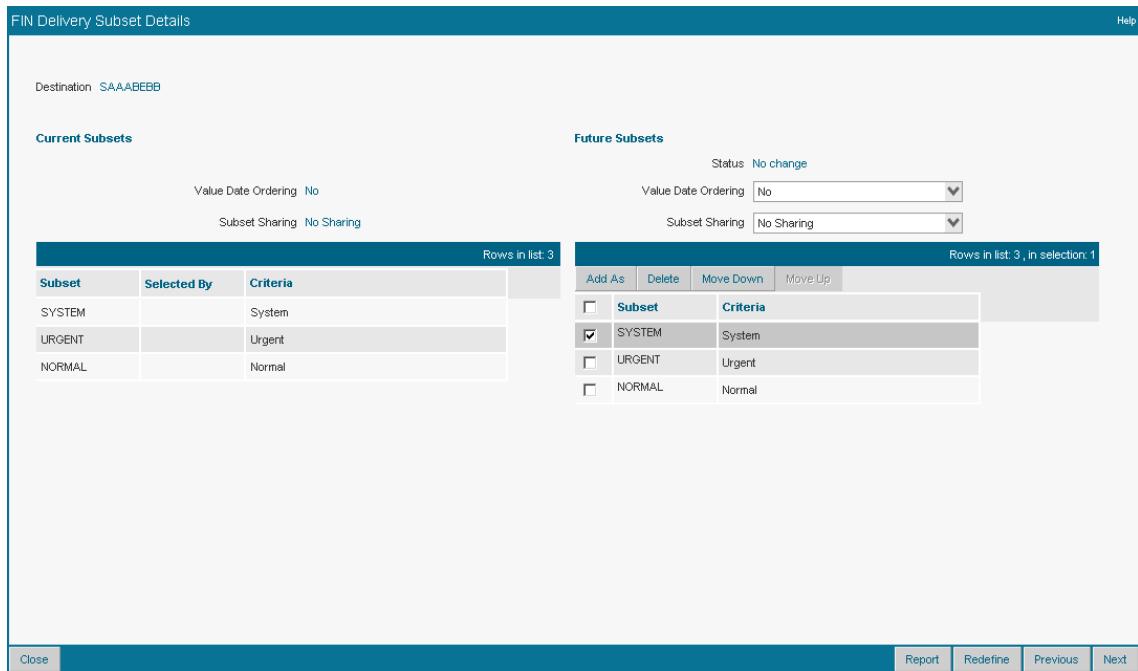
11.1.3 FIN Delivery Subset Details Window

Content

The **FIN Delivery Subset Details** window contains these elements:

- Details of the delivery subset selected
See "Details" on page 335
- Functions that enable you to manage the delivery subset
See "Functions" on page 337

Display



The screenshot shows the 'FIN Delivery Subset Details' window. At the top, it displays the destination BIC-8: SAAABEBB. The window is divided into two main sections: 'Current Subsets' and 'Future Subsets'.

Current Subsets: This section contains a table with three rows:

Subset	Selected By	Criteria
SYSTEM		System
URGENT		Urgent
NORMAL		Normal

Below the table, there are two dropdown menus: 'Value Date Ordering' (set to 'No') and 'Subset Sharing' (set to 'No Sharing').

Future Subsets: This section also contains a table with three rows, but the 'Subset' column is empty. It includes a 'Status' dropdown set to 'No change'.

Add As	Subset	Criteria
<input type="checkbox"/>	SYSTEM	System
<input type="checkbox"/>	URGENT	Urgent
<input type="checkbox"/>	NORMAL	Normal

Below the table, there are two dropdown menus: 'Value Date Ordering' (set to 'No') and 'Subset Sharing' (set to 'No Sharing').

At the bottom of the window, there are buttons for 'Close', 'Report', 'Redefine', 'Previous', and 'Next'.

Details

Field	Description
Destination	The destination BIC-8 for which the delivery subsets are defined

Field	Description
Current Subsets	<p>The current delivery subsets defined for the destination.</p> <p>The details displayed are the following:</p> <ul style="list-style-type: none"> • Value Date Ordering: Indicates if value date ordering is activated. <p>If value date ordering is activated, then the messages are delivered in value date order within each subset.</p> <p>The order of delivery is:</p> <ul style="list-style-type: none"> – value-date-sensitive messages with the earliest value date are delivered first – if a message contains more than one value date field, then the field with the earliest value date is considered for value date ordering – if there are several messages queued with the same value date, then delivery is according to priority and time of queuing. <ul style="list-style-type: none"> • Subset Sharing: Indicates if more than one logical terminal of the same destination can select the same delivery subsets • Subset: Name of the current delivery subsets • Selected By: Logical terminal codes • Criteria: Delivery subsets' criteria
Future Subsets	<p>The future delivery subsets.</p> <p>The details displayed are the following:</p> <ul style="list-style-type: none"> • Status: Status of the delivery subsets defined for the destination. <p>These are the possible statuses:</p> <ul style="list-style-type: none"> – No change: No change since the last MT 047 message was sent. – Wait MT 047 resp: Waiting for a response to the MT 047 message (Delivery Instructions Redefinition Request) generated by Alliance and sent to the network to request the replacement of the currently used delivery subset by those in the Future Subsets list. – Modified: A modification to the future subsets has occurred since the last MT 047 message was sent. – Invalid: A delayed NAK (MT 015) to the MT 047 request was sent by FIN to inform you that the request was cancelled. Refer to the FIN System Messages guide for more details. <ul style="list-style-type: none"> • Value Date Ordering: If you select Yes in the Value Date Ordering drop-down list, then the messages are delivered in value date order within each subset (see Current Subsets). • Subset Sharing: Indicates if more than one logical terminal of the same destination can select the same delivery subsets • Subset: Name of the future delivery subsets • Criteria: Delivery subsets' criteria

Functions

Function	Description
Redefine	Redefines the delivery subsets for a destination Procedure: "Redefine a Delivery Subset" on page 342
Future Subsets	<ul style="list-style-type: none"> Add: Enables you to add a delivery subset You can also add a delivery subset using the characteristics of an existing subset (Add As). Procedure: "Add a Delivery Subset" on page 339 Delete: Enables you to delete a delivery subset Move Down: Enables you to move the selected delivery subset down Move Up: Enables you to move the selected delivery subset up

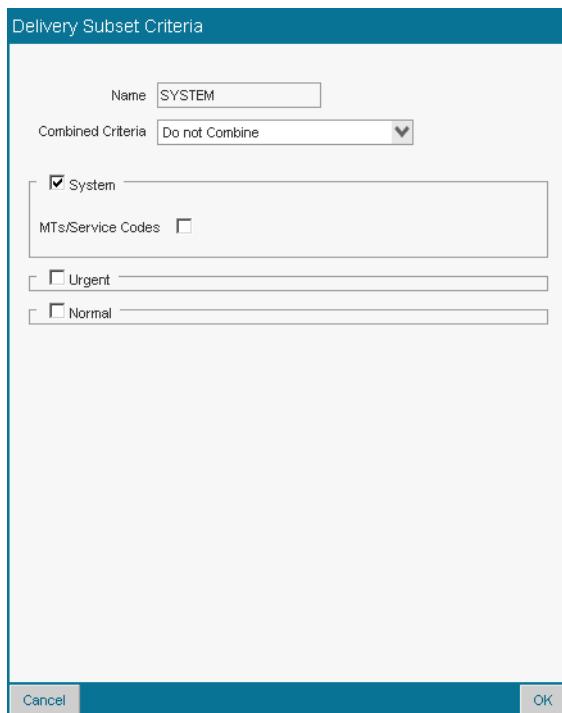
11.1.4 Delivery Subset Criteria Window

Content

The **Delivery Subset Criteria** window contains these elements:

- Details of the future delivery subset criteria
- See "Details" on page 338

Display



Details

Field	Description
Name	The user-defined name of the future subset. The name must contain six characters.
Combined Criteria	These are the possible values: <ul style="list-style-type: none"> • Combine: combine the criteria defined in the Delivery Subset Criteria window. The criteria have an AND relationship. • Do not Combine: do not combine the criteria have an OR relationship.
System	MTs/Service Codes : This field enables you to specify a maximum of 10 message types (or FIN copy services), to be contained in the delivery subset. Type in the message type or service code (three alphanumeric characters). If an entry is made in this field, then the message category to which this message type belongs may not be specified in the Categories field. Note that no check is performed on the validity of the message type entered in this field.
Urgent	<ul style="list-style-type: none"> • Categories: This field enables you to select the message category (or categories) to be contained in the delivery subset. You can indicate up to 9 categories. Message types belonging to the message category selected here may not be entered in the MTs/Service Codes field. • MTs/Service Codes: see System. • Branch Codes: This field enables you to specify a maximum of 9 message branch codes, for the selected destination, to be contained in the delivery subset. Type in the branch code (three alphanumeric characters). Note that branch codes are optional. "XXX" should not be entered as a branch code. Also, branch codes must be valid for the destination (this is not validated by Alliance). • Field 13C: This field enables you to restrict the delivery subset to FIN messages that contain field 13C. Select the Field 13C check box to enable this option.
Normal	As for the Urgent category, you can define options for the following: <ul style="list-style-type: none"> • Categories • MTs/Service Codes • Branch Codes • Field 13C

11.1.5 Request a Report of Current Delivery Subsets

Purpose

Before making any changes to the delivery subsets, or if you have just installed Alliance for the first time and you want to replace the system defaults with FIN subsets defined at SWIFT for your previous CBT, it is recommended to send a Delivery Instructions Request (MT 035) to FIN. A Delivery Instructions Report (MT 055) is sent in response, listing the delivery subsets currently held for the destination, and is sent to the requesting logical terminal. It also indicates whether value date ordering is active for that destination.

If you have just installed Alliance Access, then Alliance Access processes the MT 055 message and replaces its current default set with the definitions contained in the MT 055.

The MT 035 is generated using Alliance Message Management. For information about how to create and send system messages, see the [Message Management Guide](#).

Procedure

1. Create an MT 035 and route it to the **_SI_to_SWIFT** queue.
2. Do a Login/Select (Input & Output mode, without delivery subsets selected) with the logical terminal used to send the MT 035.
3. Wait for an MT 055 response. Subsets are updated.
4. Do a Quit with the logical terminal.

11.1.6 Add a Delivery Subset

Purpose

To change delivery subsets, you have to add future subsets and then redefine the subsets ([Redefine](#)). The Redefine option sends an MT 047 (Delivery Instructions Redefinition Request), containing the details of the change. Before attempting to redefine a delivery subset, you must know that Alliance does not validate the content of an individual subset, and it does not ensure that all subset definitions for a destination are complete. If the definitions are incorrect then SWIFT replies with an MT 015 Delayed NAK. If the MT 047 is valid, then the corresponding subset change is made in FIN at midnight local time, and you are informed by an MT 067 (Delivery Instructions Redefinition Report) to indicate that the change was made successfully.

Users and permissions

To display the list or the details of delivery subsets, or filter the list, your operator profile must have this action:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

To add a delivery subset, your operator profile must have the following additional action:

- **SWIFT Interface / Modify Subsets**

Procedure

1. From the list of delivery subsets, click a row to display the details of the delivery subsets defined for a destination.

The **FIN Delivery Subset Details** window opens.

2. In the **Future Subsets** list, click [Add](#).

You can also add a delivery subset using the characteristics of an existing subset. Select the check box of a delivery subset and click [Add As](#).

The **Delivery Subset Criteria** window opens.

3. Type a delivery subset name in the **Name** field.

The name must contain six characters.

4. Select any or all of the following check boxes: **System**, **Urgent**, or **Normal**, then define options as explained below.

If	Then
You selected System	<p>You can define options for the message types or service codes.</p> <p>Select the MTs/Service codes check box. In the field that appears, type one or several message types (for example, 025) or service codes for FINCopy (for example, SRY) separated by commas.</p> <p>For example, if you type 025, only the MT 025 messages will be queued in the delivery subset.</p>
You selected Urgent	<p>You can define options for the following:</p> <ul style="list-style-type: none"> message categories <p>Select the Categories check box. In the field that appears, type one or several categories (from 1 to 9) separated by commas.</p> <p>For example, if you type 1, only the category 1 messages will be queued in the delivery subset.</p> <ul style="list-style-type: none"> message types or service codes <p>Select the MTs/Service codes check box. In the field that appears, type one or several message types (for example, 025) or service codes for FINCopy (for example, SRY) separated by commas.</p> <p>For example, if you type 025, only the MT 025 messages will be queued in the delivery subset.</p> <ul style="list-style-type: none"> branch codes <p>Select the Branch Codes check box. In the field that appears, type a branch code (for example, WAJ).</p> <p>For example, if you type WAJ, only the messages sent to destinations containing this branch code will be queued in the delivery subset.</p> <ul style="list-style-type: none"> messages that contain the field 13C <p>Messages containing the field 13C will be queued in the delivery subset.</p>
You selected Normal	<p>As for the Urgent category, you can define options for the following:</p> <ul style="list-style-type: none"> message categories message types or service codes branch codes messages that contain the field 13C

5. If you want to combine the criteria defined in the **Delivery Subset Criteria** window, select **Combined** in the **Combined Criteria** drop-down list. The criteria have an AND relationship.

If you select **Do not Combine**, the criteria have an OR relationship.

6. Click **OK**.

The delivery subset is added to the **Future Subsets** list.

Note You can sort the delivery subsets in priority order.

Select the check box of a delivery subset and click **Move Down** or **Move Up**.

7. If you require date ordering, then select **Yes** in the **Value Date Ordering** drop-down list.
8. If you want to have more than one logical terminal of the same destination select the same delivery subsets, select either the **Share With Overflow** or **Share With Load Balancing** option in the **Subset Sharing** drop-down list.

The same message is not delivered to all the logical terminals that have selected the same delivery subset. Instead, messages are delivered round robin to all logical terminals having selected the same delivery subset.

Note	To select the same delivery subset with different logical terminals from the same destination, the selection mode for these logical terminals has to be modified from exclusive mode to shared mode. See "Add and Configure a Logical Terminal" on page 356 to modify the selection mode.
-------------	---

9. Click **Save**.
A status popup message appears.
10. Click **Close**.
The **FIN Delivery Subset Details** window closes.

After creating future delivery subsets, use the **Redefine** option to redefine the subsets. An MT 047 (Delivery Instructions Redefinition Request) is sent and the delivery subsets are updated. See "Redefine a Delivery Subset" on page 342.

11.1.7 Example of Delivery Subset Creation

Overview

If, for example, you want to create a special subset that includes only messages relating to Traveller's cheques, then you would probably want to queue category 8 messages separately for Urgent and Normal. Currently, normal priority category 8 messages are placed in the **NORMAL** subset and urgent priority are placed in the **URGENT** subset.

Procedure

1. In the **Future Subsets** list of the **FIN Delivery Subset Details** window, select the check box of the **URGENT** subset and click **Add As**.
The **Delivery Subset Criteria** window opens.
2. Type a delivery subset name in the **Name** field.
The name must contain six characters.
3. Select the **Urgent** check box.
4. Select the **Categories** check box, then in the field that appears, type 8.
5. Repeat the previous step with the **Normal** priority.
6. Click **OK**.
The **Delivery Subset Criteria** window closes.
7. Click **Save**.
The delivery subset is added to the **Future Subsets** list in the **FIN Delivery Subset Details** window.

- A status popup message appears.
8. Click **Close**.
- The **FIN Delivery Subset Details** window closes.

11.1.8 Delete a Delivery Subset

Purpose

This procedure enables you to delete a delivery subset.

Users and permissions

To display the list or the details of delivery subsets, or filter the list, your operator profile must have this action:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

To delete a delivery subset, your operator profile must have the following additional action:

- **SWIFT Interface / Modify Subsets**

Procedure

1. From the list of delivery subsets, click a row to display the details of the delivery subsets defined for a destination.

The **FIN Delivery Subset Details** window opens.
2. Select the check box of a delivery subset and click **Delete**.

The **Delete Confirmation** window opens.
3. Click **OK**.

The **Delete Confirmation** window closes.
4. Click **Save**.

A status popup message appears.
5. Click **Close**.

The **FIN Delivery Subset Details** window closes.

After deleting delivery subsets, use the Redefine option to redefine the subsets. An MT 047 (Delivery Instructions Redefinition Request) is sent and the delivery subsets are updated. See "Redefine a Delivery Subset" on page 342.

11.1.9 Redefine a Delivery Subset

Purpose

This procedure enables you to redefine a delivery subset.

Users and permissions

To display the list or the details of delivery subsets, or filter the list, your operator profile must have this action:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

To redefine a delivery subset, your operator profile must have the following additional action:

- **SWIFT Interface / Redefine Delivery**

Procedure

1. From the list of delivery subsets, select the check box of a destination in the left column.
2. Click **Redefine**.

The **Redefine** window opens.

3. In the **MT047 Sender Logical Terminal** drop-down list, select a logical terminal belonging to the destination.
4. In the **MT047 Sender Branch Code** field, you can specify a branch code. Otherwise the default value is **XXX**.
5. Click **Redefine**.

A status popup message appears.

The **Redefine** window closes.

Note Because SWIFT cannot run an MT 047 while there are FIN sessions open for that destination, it sends a System Request to Quit message (MT 008) to all the destination's logical terminals indicating the time at which the MT 047 is processed. FIN sessions that remain open at that time are aborted.

6. After redefining delivery subsets for a destination, do a Login/Select (Input & Output mode) with the logical terminal which will receive the output messages. This is especially important if the names of the delivery subsets have changed.

11.2 FIN Logical Terminals

11.2.1 Logical Terminals: Definition

What is a logical terminal?

A logical terminal is a logical entity through which users send and receive FIN messages. Each logical terminal is identified by a unique 8-character BIC (that is a destination), plus a 1-character terminal code.

You can work with live or FIN Test and Training logical terminals.

During the installation of Alliance Access, the Alliance Administrator specifies the destinations that your institution is licensed to use.

After the installation of Alliance Access or when you purchase additional destinations, you must configure the logical terminals using Alliance Access Configuration. Operators can then manage

the connection of logical terminals to the SWIFT network from Alliance Access Configuration and from Alliance Access Monitoring.

To deal with traffic volumes of between 10,000 and 20,000 messages per day, it is recommended to have two logical terminals on two different destinations. Both logical terminals must be configured for Login and Select in input/output mode.

For information about the automatic allocation of logical terminals, see "Load Balancing FIN Messages over Logical Terminals" on page 346.

11.2.2 Logical Terminals: Main Tasks

Configuration of logical terminals in Alliance Access Configuration

You can configure the following:

- BIC and signing BIC for Test and Training (**Master BIC for T&T**)
- message syntax table
- window size
- selection mode for delivery subsets
- Alliance Gateway connection and authoriser distinguished name

Connection or disconnection

Before sending and receiving FIN messages, you must connect logical terminals to SWIFTNet.

An auto-reconnect option is also available. With this option, if the session of a logical terminal with the SWIFT network is interrupted, then Alliance Access attempts to reconnect automatically the logical terminal.

Operation mode and scheduling

You can configure the operation mode of logical terminals and work with scheduled operations.

Automatic logical terminal allocation

Alliance Access provides ways to balance the FIN traffic over several logical terminals.

Monitoring

You can monitor logical terminals and their statuses.

11.2.3 Configuration of Logical Terminals

Configuration tasks

You have to configure several elements:

Task	Description
Select a BIC	You have to select a BIC as a destination to be able to send or receive messages.
Select a signing BIC for Test and Training (Master BIC for T&T)	If you are working in a Test and Training environment, you have to select a live BIC to sign the messages sent or received.

Task	Description
Select a message syntax table	A logical terminal must have a message syntax table assigned to it, so that it can validate the messages it sends and receives. A message syntax table contains descriptions of all message types that can be sent and received for the SWIFT FIN application. Alliance Access can store more than one message syntax table. A logical terminal can use either a current release of the message standards, or a Test and Training version of the message syntax table.
Define a window size	The window size determines how many messages can be sent to the network without having to wait for an acknowledgement from FIN. This value is used when a FIN session is opened.
Select a selection mode (Exclusive or Shared)	The selection mode determines how the delivery subsets are selected by logical terminals.
Define an Alliance Gateway connection	Each logical terminal must have an Alliance Gateway connection and authoriser distinguished name (and certificate) assigned to it.

11.2.4 Connection To / Disconnection From the SWIFT Network

Connection

Before sending and receiving FIN messages, you must establish a communication session with the SWIFT network. This involves:

- Logging on to Application Control (APC). This is the SWIFT application that establishes and controls communication between a logical terminal and SWIFT. APC also controls the initiation and termination of FIN sessions.
- Selecting FIN and its facilities. FIN is the SWIFT application through which all messages between institutions are input and output. Certain messages between institutions and SWIFT can also be sent and received through FIN.

For more information, see "Connect to the SWIFT Network" on page 357.

Disconnection

To terminate a SWIFT session, you must disconnect the logical terminal from FIN and then log off from APC.

For more information, see "Disconnect from the SWIFT Network" on page 359.

11.2.5 Auto Reconnect Option

Description

Sometimes the session of a logical terminal with the SWIFT network can be interrupted while you are logged on. If you have enabled the auto reconnect feature, then Alliance Access attempts to reconnect automatically the logical terminal to the same SWIFT session. System parameters can be configured in Alliance Access Configuration that determine the number of times, how often and for how long auto reconnect is attempted (**Usersync - Max Retries**, **Usersync - Max Time**, and **Usersync - Retry Timer** parameters).

11.2.6 Operation Mode and Scheduling

Description

In Alliance Access, there are two modes in which a logical terminal can operate: Manual and Automatic. The Automatic mode enables you to schedule operations. When a logical terminal is operating in Manual mode, none of the scheduled operations are activated.

You can change the operation mode of a logical terminal at any time, even if it is currently logged into Application Control (APC) or FIN.

Change of operation mode

If the logical terminal is operating in manual mode, and if one or more of the following conditions are true, then Alliance Access does not change the operational mode of the logical terminal to automatic:

- The logical terminal has no connection assigned to it currently
- Alliance Access has no calendar defined for the current year
- No scheduled actions are defined for the logical terminal
- No scheduled action is defined to occur at 00:01 am for each type of day for which at least one action has been defined

Note

The scheduled action at 00:01 am is mandatory for recovery reasons (for logical terminals only, not emission or reception profiles). You can either define a real action for that time or use the same action as the last action of the previous day.

When you schedule Specific Days, make sure that an entry exists for 00:01 for every day that you want the Logical Terminal to be Selected.

- The logical terminal is in a session and the connection that the logical terminal is using is currently suspended.

11.2.7 Load Balancing FIN Messages over Logical Terminals

Description

Load balancing is the method of distributing the load of queued FIN messages for a given destination across available logical terminals, rather than using a specific sender logical terminal normally defined in each message.

Load balancing is achieved using these methods:

- automatic allocation of logical terminals
- use of the code "*LT X*"

Important Use only one method of load balancing.

Using either method of load balancing, the acknowledgement message which is returned to the message partner application may also not match that of the sender logical terminal.

Users that already have a back-office application that implements load balancing may experience a negative impact on performance and must ensure that the **LT load balancing** parameter is set to **No**.

Automatic allocation of logical terminals

Automatic logical terminal allocation balances the load of queued messages for a given destination across the available logical terminals, rather than using a specific sender logical terminal normally defined in each message.

A system parameter can be configured to enable the automatic allocation. For more information, see the **LT load balancing** parameter in "Message" on page 118 (**System** node > **Parameters** > **Message**)

When this parameter is set to **Yes**, then Alliance Access allocates automatically a logical terminal to FIN messages independently from the original logical terminal sender. therefore, Alliance Access may transmit a message from a back-office application through a logical terminal other than the one specified in the message.

The following limitations apply when using automatic logical terminal allocation:

- Automatic logical terminal allocation is disabled for any destination that has at least one logical terminal without a designated connection.
- The logical terminals that are used for automatic logical terminal allocation must use the same message syntax table. This limitation is verified each time the SWIFT Interface Services (SIS) component is started.
- All logical terminals of a given destination must have the same protocol version. This is assumed, it is not validated by the software.
- During an interrupt, the messages handled by a logical terminal that have not received an acknowledgement from the network are reserved until the logical terminal is reconnected.

Reserved messages can be released using the Abort command on the logical terminal. The messages are returned to the message pool and transmitted by the next logical terminal allocated by the system.

Do not use automatic logical terminal allocation in the following situations:

- When the message partner uses the sender logical terminal for message reconciliation rather than the destination.
- When you want to load balance system messages.

Use of the code LT X

When back-office applications send to Alliance Access FIN messages with the code "X" as the sender logical terminal, Alliance Access validates the messages with the message syntax table set as default Live or default Test & Training. Then, Alliance Access distributes these messages over the logical terminals that are available for input.

Messages with "LT X", including urgent messages, have a lower priority than messages with a specific LT assigned. This means that normal messages with "LT A" are sent first followed by urgent messages with "LT X". If you want to include system messages in load balancing, then use the code "LT X".

The logical terminal that was used to send the messages is logged within the emission appendix of these messages.

11.2.8 SWIFT Sessions Monitoring

Overview

Details of your connection to SWIFT can be monitored.

This includes monitoring the following:

- FIN session status (FIN state)
- communication status of a logical terminal (LT state)
- messages that are queued for the logical terminal to send, or exchanged messages

11.2.9 FIN Logical Terminals Page

Content

The **FIN Logical Terminals** page contains these elements:

- A filtering criterion and filtering functionality that enable you to filter the list entities on the **FIN Logical Terminals** page:
 - See "FIN Logical Terminals " on page 348
 - See "Functions" on page 22
- Details of the available logical terminals
 - See "FIN Logical Terminals " on page 348
- Functions that enable you to manage the logical terminals
 - See "Functions" on page 355

Display

FIN Logical Terminals											
Filtering Criteria											
Destinations											
Destination	Code	Connection Name	Syntax Version	LT Status	LT State	FIN State	Auto Re-connect	Operation Mode	Selection Mode		
SAAABEBO	A	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared	Search	Report
SAAABEBB	A	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared		
SAAABEBB	B	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared		
SAAABEBB	C	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared		
SAAABEBB	D	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared		
SAAABEBB	E	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared		
SAAABEBB	F	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared		
SAAABEBB	G	sms1d	1405	Enabled	Logged out	Not Selected	Disabled	Manual	Shared		

FIN Logical Terminals

FIN Logical Terminals		
Field	Description	Filtering criteria
Destination	The destination BIC-8 defined for the logical terminal. The destination BIC can be a live BIC or a Test and Training BIC.	✓
Code	The terminal code. Letter between A and Z.	
Connection Name	The Alliance Gateway connection	
Syntax Version	The message syntax table version	
LT Status	The possible values are either Enabled or Disabled.	

FIN Logical Terminals		
Field	Description	Filtering criteria
LT State	<p>During a communication session, a logical terminal has an "LT state" (or "APC state").</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Aborting: The logical terminal has been requested to abort by the user or the network and is waiting for an acknowledgement to the Abort request from APC. Interrupted: The session has failed. An automatic reconnection will be attempted shortly, if the option was enabled before log on (See "Enable the Auto Reconnect Option" on page 361). Logged In: APC system message transfer is possible over the APC session. Logged Out: No session exists for the logical terminal. Login Ack Wait: Waiting for an acknowledgement to the Login request. Logout Ack Wait: Waiting for an acknowledgement to the Logout request. Reconnecting: The automatic reconnect is currently attempting to reconnect a failed session. This can only occur if the auto reconnect feature is enabled before login (See "Enable the Auto Reconnect Option" on page 361). 	

FIN Logical Terminals		
Field	Description	Filtering criteria
FIN State	<p>A logical terminal also has a "FIN state" which represents the state of communication between the logical terminal and FIN.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Aborting: The logical terminal has been requested (by the user or the network) to abort. Awaiting the acknowledgement to the Abort request from FIN. Interrupted: The FIN session has failed. If auto reconnect is enabled, then the logical terminal automatically attempts to re-select after the Application Control (APC) has been established. Not Selected: No FIN session exists for the logical terminal. Quit Ack Wait: Waiting for an acknowledgement to the Quit request. Re-selecting: This indicates that the logical terminal is attempting to re-select a failed FIN session. This FIN state can only occur if the auto reconnect feature is enabled. Select Ack Wait: Waiting for an acknowledgement to the Select request. This state is transient. Selected for Input: Selected for input only. You have selected the logical terminal for sending messages to FIN, but not for receiving any messages from FIN. Selected for Output: Selected for output only. You have selected the logical terminal for receiving messages from FIN, but not for sending any messages to FIN. Selected I/O: Selected for input and output. You have selected the logical terminal for sending and receiving messages from FIN. 	
Auto Re-connect	Indicates if the auto reconnect feature has been enabled. If it is enabled, then Alliance Access attempts to reconnect automatically the logical terminal to the same SWIFT session. Parameters can be configured that determine the number of times, how often and for how long auto reconnect is attempted.	
Operation Mode	Indicates the mode in which the logical terminal is operating. There are two modes in which the logical terminal can operate. The two modes of operation are Manual and Automatic . The automatic mode enables you to schedule operations. When the logical terminal is operating in manual mode, none of the scheduled operations are activated.	
Selection Mode	<p>The selection mode of the delivery subsets.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Exclusive Shared 	

11.2.10 FIN Logical Terminal Details Window: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details for the configuration of the logical terminal selected
See "Details" on page 351
- Functions that enable you to manage the logical terminal
See "Functions" on page 355
- Details of the connections to Alliance Gateway
See "Connections to Alliance Gateway" on page 354

Display

Details

Field	Description
Destination	The destination BIC-8
Master BIC for T&T	The signing BIC for Test and Training. Live BIC used to sign the messages sent or received.
Code	The terminal code. Letter between A and Z.
Status	The LT state and FIN state combined

Field	Description
Operation Mode	There are two modes in which a logical terminal can operate: <ul style="list-style-type: none"> • Manual: manual mode, no scheduled operations activated • Automatic: enables you to schedule operations
Syntax Version	The message syntax table version
Requested Window Size	The number of messages that can be sent to the network without having to wait for an acknowledgement from FIN. This value is used when a FIN session is opened. The range is 0 through 99. The default value is 10.
Selection Mode	Determines how the delivery subsets are selected by logical terminals: <ul style="list-style-type: none"> • Exclusive: When a logical terminal is in exclusive mode, the application permits only the selection of delivery subsets not yet selected. • Shared: When a logical terminal is in shared mode, the application allows selection of both: <ul style="list-style-type: none"> – delivery subsets not yet selected – delivery subsets already selected by logical terminals that are also defined as shared. Exclusive delivery subsets already selected by logical terminals cannot be selected.
Auto Re-Connect	Indicates if the auto reconnect feature has been enabled. If it is enabled, then Alliance Access attempts to reconnect automatically the logical terminal to the same SWIFT session. Parameters can be configured that determine the number of times, how often and for how long auto reconnect is attempted.
Connections to Alliance Gateway	<ul style="list-style-type: none"> • Sequence: ID automatically assigned to the connection. You can have four connections maximum. • Connection Name: Alliance Gateway connection assigned to the logical terminal. The Alliance Gateway connections are defined in the Gateway Connectivity node (System node). • Authoriser DN: Authoriser distinguished name assigned to the logical terminal. • CID Signing DN: Central Institution Destination (CID) signing distinguished name (for FINCopy).

11.2.11 FIN Logical Terminal Details Window: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details for the monitoring of the logical terminal selected
See "Details" on page 353
- Functions that enable you to manage the logical terminal
See "Functions" on page 355

Display

Pending Messages		
	FIN	APC
System	0	0
Urgent	0	-
Normal	0	-

Session Details		
	FIN	APC
Actual Window Size	N/A	-
Messages Waiting ACK	N/A	-
Session number	N/A	N/A
Output Sequence Number	N/A	N/A
Input Sequence Number	N/A	N/A

Exchanged Messages		
	Sent	Received
During This Session	0	0
Since Last Reset	22532	46576

Details

The following fields are available:

Field	Description
Status	The communication status of the logical terminal (LT state or FIN state).
Selected Delivery Subset	The delivery subset selected.
Directed Queue	Specifies whether the logical terminal receives system messages addressed to it from the SWIFT network.
Pending Messages FIN / APC	<ul style="list-style-type: none"> System: Specifies the number of FIN or APC messages with a SYSTEM priority that have been queued for transmission and are waiting to be sent to the network by the selected logical terminal. This number includes the number of system messages which have been sent but not yet acknowledged. Urgent: Specifies the number of FIN messages with an URGENT priority that have been queued for transmission and are waiting to be sent to the network by the selected logical terminal. This number includes the number of FIN messages with urgent priority that have been sent but not yet acknowledged. Normal: Specifies the number of FIN messages with a NORMAL priority that have been queued and are waiting to be sent to the network by the selected logical terminal. This number includes the number of FIN messages with normal priority that have been sent but not yet acknowledged.

Field	Description
Session Details FIN / APC	<ul style="list-style-type: none"> • Actual Window Size: Specifies the value used in the current FIN session. • Messages Waiting ACK: Specifies the number of messages sent by the selected logical terminal, for which an ACK or NAK has not yet been received. • Session number: <ul style="list-style-type: none"> – FIN: If the logical terminal is not in session with FIN, then this field contains the session number of the last FIN session opened by the selected logical terminal. If the logical terminal has selected the FIN application, then this field contains the current FIN session initiated by the selected logical terminal. – APC: If the logical terminal is not logged in, then this field contains the session number of the last APC session opened by the selected logical terminal. If the logical terminal is logged in, then this field contains the current APC session initiated by the selected logical terminal. • Output Sequence Number: Specifies the last output sequence number received from SWIFT to the selected logical terminal. • Input Sequence Number: Specifies the last input sequence number sent to SWIFT by the selected logical terminal.
Exchanged Messages Sent / Received	<ul style="list-style-type: none"> • During This Session: Number of messages sent or received during the current session. • Since Last Reset: Number of messages sent or received since the last reset of the counter.

11.2.12 FIN Logical Terminal Details Window: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Scheduled Action Details Window" on page 29.

11.2.13 Connections to Alliance Gateway

Overview

The functionality for connections to Alliance Gateway is generic within Alliance Access Configuration:

- For details of the **Connections to Alliance Gateway** list, see "Connections to Alliance Gateway Lists" on page 34.
- For details of the **Gateway Connection Details** window, see "Gateway Connection Details Window" on page 35.

11.2.14 FIN Logical Terminal Functions

Overview

These functions enable you to manage the FIN logical terminals.

Functions

Function	Description	FIN Logical Terminals page	FIN Logical Terminal Details window
<input type="button" value="Add"/>	Enables you to add a logical terminal	✓	
<input type="button" value="Set Automatic"/> / <input type="button" value="Set Manual"/>	Enables you to set the operation mode of the logical terminal selected to Automatic or to Manual Procedure: "Change the Operation Mode of a Logical Terminal" on page 361	✓	✓
<input type="button" value="Login"/>	Logs the logical terminal on to Application Control (APC) Procedure: "Connect to the SWIFT Network" on page 357	✓	✓
<input type="button" value="Logout"/>	Logs the logical terminal off from Application Control (APC) Procedure: "Disconnect from the SWIFT Network" on page 359	✓	✓
<input type="button" value="Select"/>	Enables you to select FIN Procedure: "Connect to the SWIFT Network" on page 357	✓	✓
<input type="button" value="Quit"/>	Enables you to quit FIN Procedure: "Disconnect from the SWIFT Network" on page 359	✓	✓
<input type="button" value="Abort"/>	Aborts the logical terminal session Procedure: "Abort a Logical Terminal Session" on page 360	✓	✓
<input type="button" value="Enable"/>	Enables the one or more selected logical terminals This button is available to operators with the SWIFT Interface, Enable LT permission.	✓	
<input type="button" value="Disable"/>	Disables the one or more selected logical terminals This button is available to operators with the SWIFT Interface, Disable LT permission.	✓	
<input type="button" value="Delete"/>	Deletes the one or more selected logical terminals. This button is available to operators with the SWIFT Support, Remove LT permission.	✓	

11.2.15 Add and Configure a Logical Terminal

Purpose

This procedure enables you to add and configure a logical terminal.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**
- **SWIFT Support / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

To create or modify a logical terminal, your operator profile must have these actions:

- **SWIFT Support / Add LT**
- **SWIFT Support / Modify LT**

To enable or disable a logical terminal, your operator profile must have these actions:

- **SWIFT Interface / Disable LT**
- **SWIFT Interface / Enable LT**

Prerequisites

To add a logical terminal, the servers can be running either in housekeeping mode or in operational mode.

Procedure

1. From the list of logical terminals, click **Add**.

You can also add a logical terminal using the characteristics of an existing logical terminal. Select the check box of a logical terminal and click **Add As**.

The **FIN Logical Terminal Details** window opens.

2. From the **Configuration** tab, select a live or Test and Training BIC in the **Destination** drop-down list.
3. If you are working in a Test and Training environment, select a live signing BIC in the **Master BIC for T&T** drop-down list.
4. Type a terminal code in the **Code** field. Use a letter between A and Z.
5. Assign a message syntax table in the **Syntax Version** drop-down list.

Important Do not assign a new message syntax table to a live logical terminal before the message syntax stable is live on the network.

6. Type a window size in the **Requested Window Size** field.

You must enter a value between 1 and 99.

This value must match the FIN window size requested to SWIFT for the logical terminal.

7. Select a mode in the **Selection Mode** drop-down list:
 - Exclusive
 - Shared
 8. Click **Save**.
 9. When creating a logical terminal, you also have to define connections to Alliance Gateway. See "Add an Alliance Gateway Connection" on page 37.
 10. Click **Close**.
- The **FIN Logical Terminal Details** window closes.

11.2.16 Remove a Logical Terminal

Purpose

This procedure enables you to remove a logical terminal.

Users and permissions

In order to remove a logical terminal, it must be disabled first. To activate the **Disable** button and the **Delete** button, your operator profile must have these actions:

- **SWIFT Interface / Disable LT**
- **SWIFT Support / Remove LT**

Prerequisites

To remove a logical terminal, the servers can be running either in housekeeping mode or in operational mode and the logical terminal must be disabled.

Procedure

1. From the list of logical terminals, select the logical terminal you wish to remove.
2. Click **Disable**.
3. Select the same logical terminal again.
4. Click **Delete**.
5. Confirm that you want to delete the selected logical terminal by clicking **OK**.

Once a logical terminal is deleted, it cannot be recovered.

11.2.17 Connect to the SWIFT Network

Purpose

This procedure enables you to connect to the SWIFT network.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

- **SWIFT Support / Own Destination List**

Only the destinations defined with the **Own Destinations** permission are displayed.

To connect to the SWIFT network, your operator profile must have the following additional action:

- **SWIFT Interface / Login/Select**

Prerequisites

Before connecting to the SWIFT network, you must first start the SWIFT Interface Services (SIS) component. See "Description of a Component" on page 71.

Procedure

1. From the list of logical terminals, select the check box for a logical terminal in the left column.
2. Click **Login** to log on to Application Control (APC).
The **Login Confirmation** window opens.
3. Click **OK**.
A status popup message appears.
4. Once the logical terminal is logged on, select the logical terminal again and click **Select** to select FIN.
The **Select** window opens.
5. In the **Mode** drop-down list, select a mode:
 - **Input & Output:** The logical terminal can both send messages to and receive messages from the SWIFT network.
 - **Output Only:** The logical terminal can receive messages from the SWIFT network, but cannot send any messages to the network.
 - **Input Only:** The logical terminal can send messages to the SWIFT network, but cannot receive any messages from the network.
6. In the **Directed Queue** drop-down list, select whether to receive system messages that are addressed to the logical terminal from the SWIFT network or not:
 - **Select:** The logical terminal receives system messages
 - **Do not Select:** The logical terminal does not receive system messages.
7. In the **Delivery Subsets** selection list, select the delivery subsets for which you want the logical terminal to receive messages.
The default subsets are:
 - **NORMAL:** To receive all messages that have a normal delivery priority in the message header.
 - **URGENT:** To receive all messages that have an urgent delivery priority in the message header.

- **SYSTEM:** To receive all system messages addressed to the destination, but not to a specific logical terminal.

All the delivery subsets not already selected by another logical terminal are displayed in the **Selected** list. Move the delivery subsets for which you do not want the logical terminal to receive messages to the **Available** list.

8. Click **Select**.

The **Select** window closes.

A status popup message appears.

11.2.18 Disconnect from the SWIFT Network

Purpose

This procedure enables you to disconnect from the SWIFT network.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

- **SWIFT Support / Own Destination List**

Only the destinations defined with the **Own Destinations** permission are displayed.

To disconnect from the SWIFT network, your operator profile must have the following additional action:

- **SWIFT Interface / Login/Select**

Prerequisites

If the logical terminal is in `Automatic` mode, you have to switch to `Manual` mode first and then disconnect.

Procedure

1. From the list of logical terminals, select the check box for a logical terminal in the left column.
 2. Click **Quit** to quit FIN.
- The **Quit** window opens.
3. In the **Next Select** drop-down list, select when you want to enable the Select FIN command again for the logical terminal:
 - **No Restriction on next select:** Specifies that you can run the Select FIN command at any time.
 - **Restricted until:** Lets you specify a date and time before which the next login is forbidden for this particular logical terminal. The date and time specified must be within seven days of the current date and time.
 4. Click **Quit**.

A status popup message appears.

5. Click **Logout** to log off from Application Control (APC).

The **Logout** window opens.

6. In the **Next Login** field, select when you want to enable the Login command again for the logical terminal:

- **No Restriction on next login:** Lets you log on again using this logical terminal without restriction.
- **Restricted until:** Lets you specify a date and time before which the next login is forbidden for this particular logical terminal. The date and time specified must be within seven days of the current date and time.

Warning You cannot disable this restriction once it has been set. Be very careful when entering a **Next Login** date and time.

7. Click **Logout**.

The **Logout** window closes.

A status popup message appears.

The APC application for the selected logical terminal is terminated. The network can no longer send APC messages for that logical terminal.

Note Quit messages are not sent to the print queue. To print quit messages, you have to change the routing rules.

11.2.19 Abort a Logical Terminal Session

Purpose

This procedure enables you to abort a logical terminal session.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

- **SWIFT Support / Own Destination List**

Only the destinations defined with the **Own Destinations** permission are displayed.

To abort a logical terminal session, your operator profile must have the following additional action:

- **SWIFT Interface / Login/Select**

Procedure

1. From the list of logical terminals, select the check box for a logical terminal in the left column.
2. Click **Abort**.

- The **Abort Confirmation** window opens.
3. Click **OK**.
- The **Abort Confirmation** window closes.
- A status popup message appears.

11.2.20 Change the Operation Mode of a Logical Terminal

Purpose

This procedure enables you to change the operational mode of a logical terminal to one of the following modes:

- **Automatic** mode: enables you to schedule operations.
- **Manual** mode: deactivates automatic mode.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

- **SWIFT Support / Own Destination List**

Only the destinations defined with the **Own Destinations** permission are displayed.

To change the operation mode of a logical terminal, your operator profile must have the following additional action:

- **SWIFT Interface / Ena/Dis Auto Mode**

Procedure

1. From the list of logical terminals, select the check boxes for one or several logical terminals in the left column.

Tip

You can select all the logical terminals by selecting the check box in the column heading line.

2. Click either **Set Automatic** or **Set Manual**.

A status popup message appears.

11.2.21 Enable the Auto Reconnect Option

Purpose

This procedure enables you to enable the auto reconnect option.

To be able to use the auto reconnect option, you must enable the **Auto Re-Connect** option for the logical terminals that you are using. You also have to configure system parameters for the SWIFT Interface Services (SIS) component (**Usersync - Max Retries**, **Usersync - Max Time**, and **Usersync - Retry Timer**).

For the auto reconnect to work, you must configure the **Auto Re-Connect** option and system parameters before you begin the Login and Select for a logical terminal.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

- **SWIFT Support / Own Destination List**

Only the destinations defined with the **Own Destinations** permission are displayed.

To enable the auto reconnect option, your operator profile must have the following additional action:

- **SWIFT Interface / Ena/Dis Re-Connect**

Procedure

1. From the list of logical terminals, click the row of the logical terminal for which you want to enable the auto reconnect option.

The **FIN Logical Terminal Details** window opens.

2. In the **Auto Re-Connect** drop-down list, select **Enabled**.

3. Click **Save**.

A status popup message appears.

4. Click **Close**.

The **FIN Logical Terminal Details** window closes.

5. In the tree view, select the **System** node, then select the **Parameters** node to display the list of system parameters.

6. Configure the following parameters:

- **Usersync - Max Retries**: Maximum number of times to attempt to reconnect a failed session. The SWIFT Interface Services (SIS) component must be restarted for changes to this parameter to take effect.

Allowed values between 1 and 40. Default value: 20.

- **Usersync - Max Time**: Maximum time (in minutes) during which Alliance will attempt to reconnect. The SWIFT Interface Services (SIS) component must be restarted for changes to this parameter to take effect.

Allowed values between 1 and 60. Default value: 10.

- **Usersync - Retry Timer**: Time-out period (in seconds) between reconnect retries. The SWIFT Interface Services (SIS) component must be restarted for changes to this parameter to take effect.

Allowed values between 20 and 300. Default value: 120.

See "Parameters" on page 111.

11.2.22 Enable Automatic Logical Terminal Allocation

Purpose

This procedure enables you to enable automatic logical terminal allocation. For more information about the purpose and limitations of load balancing, see "Load Balancing FIN Messages over Logical Terminals" on page 346.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

- **SWIFT Support / Own Destination List**

Only the destinations defined with the **Own Destinations** permission are displayed.

To enable automatic logical terminal allocation, your operator profile must have the following additional entity:

- **System Management**

Security officers can enable the automatic logical terminal allocation.

Procedure

1. In the tree view, select the **System** node, then select the **Parameters** node to display the list of system parameters.
2. Configure the **LT load balancing** parameter.
See "Message" on page 118.
3. Restart the SWIFT Interface Services (SIS) component if required (that is, if you are in operational mode). If you are in housekeeping mode, then the change takes effect at the next restart in operational mode.

11.2.23 Monitor a SWIFT Session

Purpose

This procedure enables you to monitor a SWIFT session.

Users and permissions

To display the list or the details of logical terminals, or filter the list, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**

Only the destinations defined with the **List Own Destinations** permission are displayed.

- **SWIFT Support / Own Destination List**

Only the destinations defined with the **Own Destinations** permission are displayed.

To monitor SWIFT sessions, your operator profile must have either one of these actions:

- **SWIFT Interface / Own Destination List**
- **SWIFT Support / Own Destination List**

Procedure

1. From the list of logical terminals, click the row of the logical terminal which you want to monitor.
The **FIN Logical Terminal Details** window opens.
2. Click the **Monitoring** tab.
3. You can click **Refresh** to refresh the list.
The **Reset** buttons enable you to reset the counters.
4. Click **Close**.
The **FIN Logical Terminal Details** window closes.

11.3 Application Service Profiles

11.3.1 About Application Service Profiles

Application Service Profile

An Application Service Profile is a structured set of parameters that messaging interfaces and applications use to send and receive traffic correctly on a particular SWIFTNet service.

These parameters trigger the usage of features within SWIFTNet or describe what a messaging interface must do with traffic sent or received. The Application Service Profile parameters determine how Alliance Access handles these features.

The following parameters are available per service:

- RMA-related parameters
- End-to-end signing required and what format the signature can have
- Non-repudiation signing required
- Store-and-forward usage
- SWIFTNet Copy parameters
- `HeaderInfo` element required and usage of this element for the service

Application Service Profile package

SWIFT provides the Application Service Profiles to the customer in the form of an Application Service Profile package. You can download the Application Service Profile package from www.swift.com > Support > Resources > [Download Centre](#).

The package is a ZIP file that contains all the Application Service Profiles and contains the following types of files:

- **ApplProf.dig**, which contains the digest of each file contained in the ASP package

- The XML schema definitions (**AppIProfDigest.xsd**, **ServiceProfile.xsd**, **FINCopyServiceProfile.xsd**)
- The Application Service Profiles for SWIFTNet services, **<service>_<YYYY-MM-DDTHHMMSS>.spd**
- The FINCopy Profile files, **Live|TT<service>_[CID]_<YYYY-MMDDTHHMMSS>.fcp**
FINCopy Profiles are installed one by one.

Tip

After installing the Application Services Profiles package, an operator with appropriate permissions can hide any services that must not be visible to users of Alliance Access.

Removal of Application Service Profiles

You cannot remove Application Service Profiles after they are installed. If an incorrect package was installed, then a new installation of the correct ASP package must be performed.

RMA traffic filtering

After installing the Application Services Profiles package, an operator with appropriate permissions can hide activate or deactivate the **RMA Traffic Filtering** options.

For more information about traffic filtering using RMA, see the [RMA Service 7.1 Service Description](#).

Setting FileAct payload archiving

Operators who can install new Application Service Profiles (that is, those with the Access Control, Files on User Space permission) can specify the settings for the archiving of FileAct payloads. For more information, see the description of the **Set FileAct Payload Archival** button in the [Configuration Guide](#).

11.3.2 Application Service Profiles Page

Content

The **Application Service Profiles** page contains these elements:

- Filtering criteria and filtering functionality that enable you to filter the list entities on the **Application Service Profiles** page:
 - See "Application Service Profiles" on page 366
 - See "Functions" on page 22
- Details that relate to the Application Service Profiles
See "Application Service Profiles" on page 366
- Functions that enable you to manage the Application Service Profiles
See "Functions" on page 367

Display

Application Service Profiles

Filtering Criteria

Service	<input type="text"/>	Environment	<input type="text"/>	Visibility	<input type="text"/>
Requires RMA	<input type="text"/>			Trial Traffic Filtering	<input type="text"/>
<input type="button" value="Clear"/>					

Application Service Profiles

	Change View	Install	Show	Hide	Activate Trial Filtering	Deactivate Trial Filtering	Set FileAct Payload Archival	Report	FileAct Payload Archival					
<input type="checkbox"/>	Service	<input type="text"/>	Description	<input type="text"/>	Environment	<input type="text"/>	Visibility	<input type="text"/>	Publication Date	<input type="text"/>	Installation Date	<input type="text"/>	FileAct Payload Archival	<input type="text"/>
<input type="checkbox"/>	CLSB.CLS	<input type="text"/>	clsb.cls (Live)	<input type="text"/>	Production	<input type="text"/>	Visible	<input type="text"/>	2011/03/05 14:00:01	<input type="text"/>	2015/02/25 08:18:4	<input type="text"/>	Delete on message archival	<input type="text"/>
<input type="checkbox"/>	CLSB.CLSIPMTS	<input type="text"/>	clsb.clsipmts (Test)	<input type="text"/>	Production	<input type="text"/>	Hidden	<input type="text"/>	2011/03/05 14:00:01	<input type="text"/>	2015/02/25 08:18:4	<input type="text"/>	Delete on message archival	<input type="text"/>
<input type="checkbox"/>	SWIFT.ACCORD	<input type="text"/>	swift.accord (Live)	<input type="text"/>	Production	<input type="text"/>	Hidden	<input type="text"/>	2012/05/19 15:00:01	<input type="text"/>	2015/02/25 08:18:4	<input type="text"/>	Delete on message archival	<input type="text"/>
<input type="checkbox"/>	SWIFT.ACCORDIP	<input type="text"/>	swift.accordip (Test)	<input type="text"/>	Production	<input type="text"/>	Hidden	<input type="text"/>	2012/03/31 15:00:01	<input type="text"/>	2015/02/25 08:18:4	<input type="text"/>	Delete on message archival	<input type="text"/>
<input type="checkbox"/>	aaalsari.macugrt	<input type="text"/>	AALSARI_MACUG	<input type="text"/>	Production	<input type="text"/>	Hidden	<input type="text"/>	2011/03/05 14:00:01	<input type="text"/>	2015/02/25 08:18:4	<input type="text"/>	Delete on message archival	<input type="text"/>
<input type="checkbox"/>	aaalsari.macugrltp	<input type="text"/>	AAALSARI_MACUC	<input type="text"/>	Production	<input type="text"/>	Hidden	<input type="text"/>	2011/03/05 14:00:01	<input type="text"/>	2015/02/25 08:18:4	<input type="text"/>	Delete on message archival	<input type="text"/>
<input type="checkbox"/>	aaalsari.macugsnf	<input type="text"/>	AAALSARI_MACUC	<input type="text"/>	Production	<input type="text"/>	Hidden	<input type="text"/>	2011/03/05 14:00:01	<input type="text"/>	2015/02/25 08:18:4	<input type="text"/>	Delete on message archival	<input type="text"/>

Application Service Profiles

Application Service Profiles		
Field	Description	Filtering criteria
Service	<p>A description of the service.</p> <p>For filtering, you can specify the Service⁽¹⁾ value to use for filtering</p>	✓
Environment	<p>Whether the service exists in the live system or in the test system</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Production ITB <p>You can specify the Environment⁽¹⁾ value to use for filtering</p>	✓
Requires RMA	<p>Whether the service requires RMA</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Yes No <p>You can specify the Requires RMA⁽¹⁾ value to use for filtering</p>	✓
Visibility	<p>Whether the service is visible in the graphical user interfaces of the Alliance Web Platform packages</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Visible Hidden <p>You can specify the Visibility⁽¹⁾ value to use for filtering</p>	✓

Application Service Profiles		
Field	Description	Filtering criteria
Trial Traffic Filtering	<p>Whether RMA traffic filtering is active</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Active • Inactive <p>You can specify the Trial Traffic Filtering⁽¹⁾ value to use for filtering</p>	✓
Description	A description of the service	
Publication Date	The date of publication	
Installation Date	The date of installation	

(1) See "Application Service Profiles" on page 366

Functions

Function	Description
Install	Enables you to install an Application Service Profile Procedure: "Install an Application Service Profile" on page 368
Show	Changes the value of Visibility to Visible for the services that are currently selected Available only when services that have Visibility set to Hidden are selected Procedure: "Mark a Service as Hidden or Visible" on page 369
Hide	Changes the value of Visibility to Hidden for the services that are currently selected Available only when services that have Visibility set to Visible are selected Procedure: "Mark a Service as Hidden or Visible" on page 369
Activate Trial Filtering	If a trial period for RMA traffic filtering has been defined, activates RMA traffic filtering for the services that are currently selected Available only when services that have Trial Traffic Filtering set to Inactive are selected Procedure: "Activate or Deactivate RMA Traffic Filtering" on page 369
Deactivate Trial Filtering	If a trial period for RMA traffic filtering has been defined, deactivates RMA traffic filtering for the services that are currently selected Available only when services that have Trial Traffic Filtering set to Active are selected Procedure: "Activate or Deactivate RMA Traffic Filtering" on page 369

Function	Description
Set FileAct Payload Archival	<p>Enables you to set the FileAct payload archival action, which applies to To SWIFTNet and From SWIFTNet messages.</p> <p>The following three options are available:</p> <ul style="list-style-type: none"> • Delete on message archival: With this option, the payload of File messages for the service is deleted upon message archival. • Delete on message completion: With this option, the payload of File messages for the service is deleted upon message completion, for example, when all instances of that message are completed. • Archive: With this option, the payload of File messages for that service is archived with the message. As a result, the payload is also included in archive backups and restored when message archives are restored. This is visible in the Message Management, Message Search application, in which you can request to save the payload of a File message (in the File tab of Message Details, using the Save File button). You can save the file even if the message has already been archived (and either backed up or not, but not removed) or restored. The archive must have occurred using Alliance Access 7.1 or later. <p>This button is available when you select one or multiple services from the list, provided that not all selected services are FIN services. When only one service is selected, the action currently assigned to that service is displayed.</p>

11.3.3 Install an Application Service Profile

Purpose

This procedure provides instructions for installing an Application Service Profile package.

You can also use the `saa_manageasp` command, which is described in the *Administration Guide* for [AIX](#), [Linux](#), [Oracle Solaris](#), or [Windows](#).

Note You cannot schedule the installation of an Application Service Profile package.

Users and permissions

To install Application Service Profiles, your operator profile must have these actions:

- **SWIFT Support / Manage ASP**
- **Access Control / Files on User Space**

Prerequisites

Alliance Access must be running in either housekeeping or operational mode.

Procedure

1. Download the latest Application Service Profile package from www.swift.com > Support > Resources > [Download Centre](#).

Make a note of the **Security number** that is associated with the package. This is the digest value of the file.

2. Click **Install**.
- The **Install Application Service Profile** window opens.
3. Click **Browse**.
- The **Choose file** window opens.
4. Select the file that contains the Application Service Profile package, and click **Open**.
- The **Choose file** window closes. The name and path of the file appears in the **Local File Name** field of the **Install Application Service Profile** window.
5. Click **Install**.
- The **Install Application Service Profile** window closes and the **Check File Digest** window opens.
6. If the digest in the **Check File Digest** window matches the **Security number** of the package (see step1), then click **OK**.
- The **Check File Digest** window closes.

A status popup message appears.

If the installation is successful, then the services contained in the Application Service Profile package appear in the list in the **Application Service Profile** page.

11.3.4 Mark a Service as Hidden or Visible

Purpose

This procedure enables you to mark a service as hidden or visible.

If you are not using a given service, you can decide to hide it so that it does not appear in the graphical user interfaces of the Alliance Web Platform packages.

Users and permissions

To mark services as hidden or visible, your operator profile must have this action:

- **SWIFT Support / Manage ASP**

Procedure

1. From the list of Application Service Profiles, select the check box of one or several services in the left column.
 2. Given the option which is already selected, click **Show** or **Hide**.
- The **Visibility** field changes to **Visible** or **Hidden**.

A status popup message appears.

11.3.5 Activate or Deactivate RMA Traffic Filtering

Purpose

This procedure enables you to activate or deactivate RMA traffic filtering.

This has an effect only if a trial period for RMA traffic filtering has been defined for a given service.

Users and permissions

To activate or deactivate RMA traffic filtering, your operator profile must have this action:

- **SWIFT Support / Manage ASP**

Procedure

1. From the list of Application Service Profiles, select the check box of one or several services in the left column.
2. Given the option which is already selected, click **Activate Trial Filtering** or **Deactivate Trial Filtering**.

The **Trial Traffic Filtering** field changes to **Active** or **Inactive**.

A status popup message appears.

11.4 FIN Copy Profiles

11.4.1 About FIN Copy Profiles

Concept

In order to allow the use of FIN copy services for a selected destination, FIN Copy Profiles have to be installed in Alliance Access and have destinations assigned to them.

Application Service Profile package

See "Application Service Profile package" on page 364.

11.4.2 FINCopy Service

Overview

To use the FINCopy service, you must, in addition to the normal Alliance Access configuration:

- complete the necessary registration procedures with your central institution
- install a FINCopy service parameter file into Alliance Access
- assign the FINCopy service to the LTs (own destinations) to be used to send and receive copy messages
- specify whether message authorisation (RMA) is required (default is "not required")
- activate the relevant FINCopy service in Alliance Access.

Messages sent using FINCopy services are known as Copy Service Messages. These messages are recognised by SWIFT Support Services by the presence of field tag 103 in block 3 of the message - the user header block.

FINCopy can operate in the following modes:

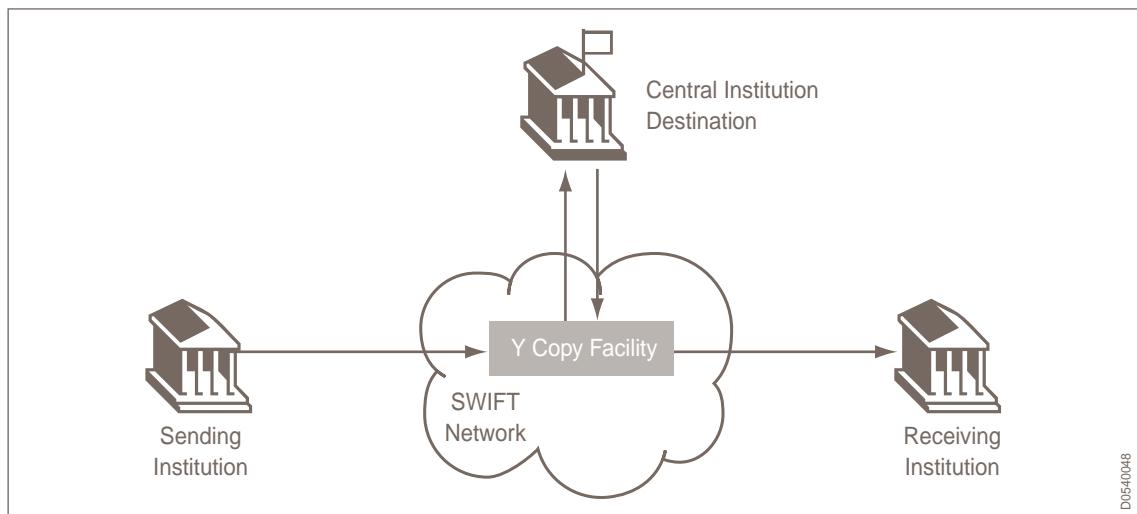
- Y-Copy mode
- T-Copy mode
- Bypassed.

11.4.2.1 Y-Copy Mode

Overview

In Y-Copy mode, messages are intercepted by the Y-Copy facility. Y-Copy either authorises the message and delivers it to the recipient or rejects the message, for example, aborts the copy process and notifies the sender.

Y-Copy is the default mode for the FINCopy service on Alliance Access.



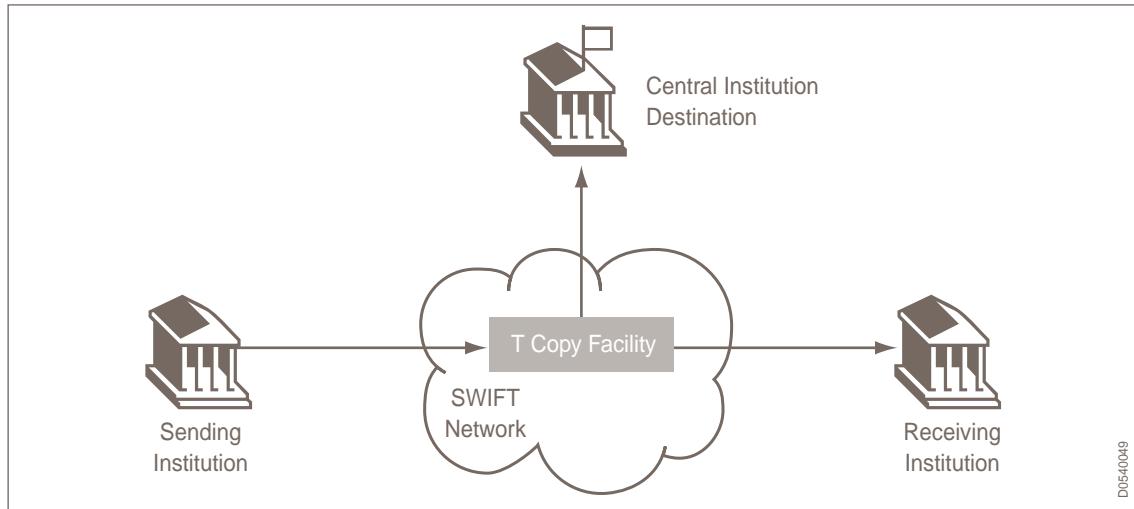
Before the message is delivered to the receiving institution, the Copy Service sends a partial, or a full copy of the message to the central institution. The central institution analyses the information contained in this message. Based on internal calculations, the central institution decides whether the copy service can release the message to the receiving institution. In this way, the receiving institution only receives authorised messages.

A Proprietary Authentication Code (PAC) trailer may be appended to the message before delivery.

11.4.2.2 T-Copy Mode

Overview

In T-Copy mode, messages are only *copied* to the central institution. The recipient receives the message independently of any authorisation from the central institution.



A Proprietary Authentication Code (PAC) trailer is *not* appended to the message before delivery.

11.4.2.3 Bypassed

Overview

This mode is essentially used in disaster situations. In bypassed mode, no copying to the Central Institution Destination (CID) is performed. Messages are still intercepted by the copy service, but they are not copied to the central institution. Subsequently, no authorisation is required before the message is delivered.

A Proprietary Authentication Code (PAC) trailer is still appended to the message before delivery, but it is empty to signify to the recipient that the message has not been authorised by the central institution.

11.4.3 FIN Copy Profiles Page

Content

The **FIN Copy Profiles** page contains these elements:

- Details that relate to the FIN Copy Profiles
 - See "Details" on page 373
- Functions that enable you to manage the FIN Copy Profiles
 - See "Functions" on page 375

Display

FIN Copy Profiles					
Rows in list: 2 , in selection: 1					
	Change View	Install	Delete	Activate	Deactivate
<input type="checkbox"/>	FCP ID	Central Institution	FCP Status	Live	RMA Bypass
<input checked="" type="checkbox"/>	ZCP	COPZBEB0	Inactive	No	No
<input type="checkbox"/>	ZCP	COPZBEBB	Inactive	Yes	No

Details

Column	Description
FCP ID	The identifier of the FIN Copy Profile
Central Institution	The identifier of the central institution
FCP Status	Whether the FIN Copy Profile is active These are the possible values: <ul style="list-style-type: none">• Active• Inactive
Live	Whether the FIN Copy Profile is live These are the possible values: <ul style="list-style-type: none">• Yes• No
Requires RMA	Whether RMA is used for messages. These are the possible values: <ul style="list-style-type: none">• Yes• No

11.4.4 FIN Copy Profile Details Window

Content

The **FIN Copy Profile Details** window contains these elements:

- Details that relate to the FIN Copy Profiles
 - See "Details" on page 374
- Functions that enable you manage the FIN Copy Profiles
 - See "Functions" on page 375

Display

FIN Copy Profile Details

Identification

FCP ID	ZCP
Live	No
Central Institution	COPZBEB0
FCP Status	Active

Parameters

Authentication	Double
Full Copy	No
Requires RMA	No

Own Destinations

Available

>>

>

<

<<

Selected

- SAAABEB0
- SAABBEB0
- SAACBEB0
- SAADBEB0
- SAAEBEB0
- SAAFBEB0
- SAAGBEB0
- SAAHBEB0
- SAAIBEB0

Included in cold start

Details

Field	Description
FCP ID	The identifier of the FIN Copy Profile
Live	See Live in "Details" on page 373
Central Institution	The identifier of the central institution
FCP Status	See FCP Status in "Details" on page 373
Authentication	<p>The authentication type</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Normal • Double
Full Copy	<p>Whether full copies are sent to the central institution. If No is selected, then partial copies are sent.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Yes • No
Requires RMA	See Requires RMA in "Details" on page 373
Own Destinations	The Available list contains the list of possible destinations.
Included in cold start	Indicates whether or not the FIN Copy Profile must be included in cold start processing.

11.4.5 FIN Copy Profile Functions

Overview

The functions that enable you manage the FIN Copy Profiles are available when the Alliance Access instance for the current Alliance Access Configuration session is running in either operational or housekeeping mode.

Functions

Function	Description	FIN Copy Profiles page	FIN Copy Profile Details window
Install	Enables you to install FIN Copy Profiles Procedure: "Install a FIN Copy Profile" on page 375	✓	x
Delete	Deletes the FIN Copy Profiles that are currently selected	✓	x
Activate	Activates the FIN Copy Profiles that are currently selected Available when only FIN Copy Profiles that have FCP Status set to Inactive are selected	✓	✓
Deactivate	Deactivates the FIN Copy Profiles that are currently selected Available when only FIN Copy Profiles that have FCP Status set to Active are selected	✓	✓

11.4.6 Install a FIN Copy Profile

Purpose

This procedure enables you to install FIN Copy Profiles.

Users and permissions

To install FIN Copy Profiles, your operator profile must have these actions:

- **SWIFT Support / Install VAS**
- **Access Control / Files on User Space**

Prerequisites

- You must have an Application Service Profile package (archive file) that contains the FIN Copy Profiles.
See "Application Service Profile package" on page 364
- The Alliance Access instance for the current Alliance Access Configuration session must run in housekeeping mode.

Procedure

1. Click **Install**.

- The **Install FIN Copy Profiles** window opens.
2. Click **Browse**.
- The **Choose file** window opens.
3. Select the Application Service Profile package that you require and click **Open**.
- The **Choose file** window closes and the path name of the Application Service Profile package appears in the **Local File Name** field of the **Install FIN Copy Profiles** window.
4. Click **Install**.
- The **Install FIN Copy Profiles** window closes and the **Check File Digest** window opens.
5. If the digest in the **Check File Digest** window matches the digest that you have received, then click **OK**.
- The **Check File Digest** window closes and the **Install FIN Copy Profiles** window opens.
6. Select the FIN Copy Profiles that you require from the list and click **Install**. If necessary, use the filtering functionality available (see "Functions" on page 22).
- A status popup message appears.
- If the installation is successful, then the FIN Copy Profiles appear in the list on the **FIN Copy Profiles** page.
7. Click **Close**.
- The **Install FIN Copy Profiles** window closes.
- The installation of the FIN Copy Profiles is complete.

11.4.7 Activate or Deactivate a FIN Copy Profile

Purpose

This procedure enables you to activate a FIN Copy Profile to enable Alliance Access to use it. Deactivating a profile suspends its usage.

Note For T-Copy mode, the central institution does not have to activate the FIN Copy Profile. Only the participants of the service must activate the FIN Copy Profile.

Users and permissions

To activate or deactivate RMA traffic filtering, your operator profile must have these actions:

- **SWIFT Support / Activate VAS**
- **SWIFT Support / De-activate VAS**

Procedure

1. From the list of FIN Copy Profiles, select the check box of one or several profiles in the left column.
2. Click **Activate** or **Deactivate**, as appropriate.

The **FCP Status** field changes to **Active** or **Inactive**.

A status popup message appears.

11.4.8 Delete a FIN Copy Profile

Purpose

This procedure enables you to delete a FIN Copy Profile.

Users and permissions

To delete FIN Copy Profiles, your operator profile must have this action:

- SWIFT Support / De-install VAS

Prerequisites

Before deleting a profile, you have to deactivate it.

Procedure

1. From the list of FIN Copy Profiles, select the check box of one or several profiles in the left column
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
A status popup message appears.

11.5 Emission Profiles

11.5.1 Emission Profile

SWIFTNet profiles

The flow of messages to and from SWIFTNet is managed through the following profiles in Alliance Access:

- emission profiles for outgoing messages
- reception profiles for incoming messages

Emission Profile

An emission profile controls the message flow of outgoing messages.

The emission profile defines the messaging service and its requestor DN, delivery mode, and Delivery Notification queue (for store-and-forward mode). The messaging service is associated with an Application Service Profile which provides requirements for specific SWIFTNet services.

It also provides various parameters for the InterAct and FileAct messages that are sent for a given service (for example, signature, non-repudiation, or window size), and parameters such as the input channel for the store-and-forward mode.

You can configure schedules to activate and deactivate an emission profile automatically.

For each profile defined, a SWIFTNet connection must also be assigned. Profiles must be enabled and activated to be ready for use, before Alliance Access transmits InterAct and FileAct messages to SWIFTNet.

FIN Test and Training

An emission profile must be defined for each licensed live BIC8 that will be used to sign all authorisation messages for FIN Test and Training. That licensed BIC is referred to as the Signing BIC for Test and Training.

11.5.2 Emission Session

Overview of emission session

1. The InterAct or FileAct messages that Alliance Access sends are routed first to the **_SI_to_SWIFTNet** queue.
For information about this queue, see "List of Exit Queues" on page 448.
2. When an emission profile is activated, Alliance Access starts an emission session, and at regular time intervals, checks for messages in the **_SI_to_SWIFTNet** queue.

The configuration parameter, **Emission: EP Polling Timer**, determines the length of the intervals.

Important Deactivating an emission or reception profile aborts all ongoing file transfers.

3. Alliance Access retrieves the InterAct or FileAct message instances from the **_SI_to_SWIFTNet** on the basis of the SWIFTNet service and requestor DN.

Some of the SWIFTNet settings of the messages are checked against the values contained in the Application Service Profile that is associated with the SWIFTNet service defined in the emission profile.

If these SWIFTNet settings are not compliant with the values present in the Application Service Profile, then the message is rejected locally, otherwise the message is sent to SWIFTNet.

Note The connection with SWIFTNet is not established until a message is detected in the **_SI_to_SWIFTNet**, and is ready for sending.

4. When an emission profile is activated, then Alliance Access sends the number of messages up to the defined window size (for the **_SI_to_SWIFTNet** queue).

When a store-and-forward emission profile requires the use of an input channel:

- The name of the input channel is added to the emission profile definition.
- A consistency check is made between the owning institution of the input channel and the requestor DN mentioned in the emission profile: these must match.
- For the window size, the minimum value is 1 and there is no maximum value. The default value is 12.

The next messages are sent when a technical acknowledgement is received, or after a timeout because of lack of activity.

For each message, a user unique message identifier (UUMID) is generated.

Note If no corresponding emission profile is defined for some messages present in the **_SI_to_SWIFTNet** queue, then those messages are ignored by the selection process and stay in the queue until a corresponding emission profile is defined, or the messages are removed manually.

5. A sequence number, starting at 1 for each new session, is assigned to a message and is incremented for each new message sent in the session.

For each message emission attempt, an "appendix" is created containing key information about emission session and message status. A session number is also maintained per emission profile and incremented each time the emission profile is activated. The session holder for the session is the emission profile or the input channel if the emission profile uses one.

11.5.3 Emission Profiles Page

Content

The **Emission Profiles** page contains these elements:

- A filtering criterion and filtering functionality that enable you to filter the list entities on the **Emission Profiles** page:
 - See "Details" on page 379
 - See "Functions" on page 22
- Details of the available emission profiles
See "Details" on page 379
- Functions that enable you to manage the emission profiles
See "Functions" on page 386

Display

Emission Profiles											
Filtering Criteria											
Emission Profiles											
Change View	Refresh	Add	Enable	Disable	Activate	Deactivate	Set Automatic	Set Manual	Delete	Report	Previous
<input type="checkbox"/>	Name ▲	Connection	InterAct	Store-and-Forward	swift.fpmi.st	cn=relax2,o=saa...				Manual	Disabled
<input type="checkbox"/>	FpML_X	beax017	InterAct	Store-and-Forward	swift.fpmi.st	cn=relax2,o=saa...				Automatic	Enabled
<input type="checkbox"/>	FpML_Y		InterAct	Store-and-Forward	swift.fpmi.st	cn=relax2,o=saa...				Manual	Disabled
<input type="checkbox"/>	FpML_Z		InterAct	Store-and-Forward	swift.fpmi.st	cn=relax2,o=saa...				Manual	Disabled

Details

Column	Description	Filtering criteria
Name	The emission profile name	✓
Connection	The Alliance Gateway connections	
Service	The code for the SWIFTNet service that you are using	

Column	Description	Filtering criteria
Messaging Service	<p>These are the possible values:</p> <ul style="list-style-type: none"> • InterAct • FileAct • InterAct & FileAct 	
Delivery Mode	<p>These are the possible values:</p> <ul style="list-style-type: none"> • Real-Time • Store-and-Forward 	
Delivery Notification Queue	<p>Name of the store-and-forward queue that must be used to store store-and-forward delivery notifications (failed delivery notifications and optional successful delivery notifications). Queue names can be up to 30 characters long.</p> <p>This field is only visible if Delivery Mode is Store-and-Forward.</p>	
Requestor DN	The requestor DN that you are using for the SWIFTNet service used	
Input Channel	The input channel, which is used for InterAct messaging services that operate in store-and-forward mode.	
Operation Mode	<p>Indicates the mode in which the emission profile is. In Alliance Access, there are two modes in which the emission profile can operate:</p> <ul style="list-style-type: none"> • Manual: none of the scheduled operations are activated • Automatic: enables you to schedule operations. 	
Status	<p>The current status of the emission profile</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Enabled • Disabled 	

Column	Description	Filtering criteria
Session Status	<p>The session status of the emission profile</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Active: The profile has been activated and the session for this profile is in progress. • Inactive: The profile has been deactivated and the session is inactive. • Activating: The profile was inactive, the profile is in the process of being activated. • Deactivating: The profile was active, but the session has been interrupted and the profile is in the process of being "deactivated". The system attempts to resume the session automatically. • Interrupted: The profile was active, but the session has been interrupted. The system attempts to resume the session automatically. 	

11.5.4 Emission Profile Details Window: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details for the configuration of the emission profile selected

See "Details" on page 382

- Functions that enable you to manage the emission profile

See "Functions" on page 386

Display

Emission Profile Details - becqbe44_rma

Configuration **Monitoring** **Scheduling**

Name	becqbe44_rma
Status	Enabled / Inactive
Service	swift.rma
Requestor DN	o=becqbe44,o=swift
Operation Mode	Manual
Retry Limit	2
Security Level	With signature and non repudiation
Messaging Service	InterAct
Delivery Mode	Store-and-Forward
Delivery Notification Queue	becqbe44_rma
Input Channel Name	Do not use an Input Channel
Window Size	5
Positive Delivery Notification	<input type="checkbox"/>

Connections to Alliance Gateway Rows in list: 1, in selection: 0

Change View	Add	Delete	Move down	Move up
Sequence	Connection Name	Authoriser DN		
1	sms1d			

Buttons: Close, Refresh, Report, Disable, Activate, Set Automatic, Previous, Next

Details

Field	Description
Name	The emission profile name. 20 characters maximum, no spaces allowed.
Status	<p>The status of the emission profile and session</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Enabled / Active Enabled / Inactive Disabled / Inactive
Service	The code for the SWIFTNet service that you are using. 30 characters maximum.
Requestor DN	The requestor DN that you are using for the SWIFTNet service used
Operation Mode	Indicates the mode in which the emission profile is. In Alliance Access, there are two modes in which the emission profile can operate. The two modes of operation are Manual and Automatic . The automatic mode enables you to schedule operations. When the emission profile is operating in manual mode, none of the scheduled operations are activated.
Retry Limit	<p>Indicates the number of retries for each message (re-transmission after emission failure). The value can be from 0 to 5. The default is 2.</p> <p>This field is displayed and applicable only to emission profiles defined for a Store-and-Forward service.</p>

Field	Description
Security Level	<p>These are the possible values:</p> <ul style="list-style-type: none"> Without Signature: The messages that are sent using this profile do not have to be signed. With Signature: the messages that are sent using this profile must be signed. If this method is selected, then you can choose the signature method to sign the InterAct or FileAct messages. <p>Note The InterAct messages that relate to relationship management authorisations are always signed.</p> <ul style="list-style-type: none"> With signature and non repudiation: Messages sent using this profile must be signed and non-repudiation is required. If this method is selected, then you can choose the Signature Method to sign InterAct or FileAct messages
Signature Method	<p>The method used to sign messages. These are the possible values:</p> <ul style="list-style-type: none"> Crypto Block: a signature is placed on each individual InterAct message. Signature List: all messages within one InterAct message share the same signature, which is based on the digest values that are generated from the content of the message.
Messaging Service	<p>These are the possible values:</p> <ul style="list-style-type: none"> InterAct FileAct InterAct & FileAct
Delivery Mode	<p>These are the possible values:</p> <ul style="list-style-type: none"> Real-Time Store-and-Forward
Delivery Notification Queue	<p>Only displayed if the Delivery Mode is Store-and-Forward. Indicates the name of the store-and-forward queue that must be used to store store-and-forward delivery notifications (failed delivery notifications and optional successful delivery notifications). 30 characters maximum.</p>
Input Channel Name	<p>Only displayed if the Message Service is InterAct and the Delivery Mode is Store-and-Forward. You can select an input channel in the drop-down list or select Do not use an Input Channel.</p>
Delivery Notif via SysMsg	<p>If selected for a store-and-forward emission profile, specifies that the delivery notifications related to InterAct/FileAct messages sent by means of this emission profile must be received as system messages. If not selected, the delivery notifications are received as internal messages.</p>
Window Size	<p>Window size used for the emission. The minimum value is 1 and there is no maximum value. The default is 5 if the delivery mode is real-time and 12 if the delivery mode is store-and-forward.</p>

Field	Description
Positive Delivery Notification	Indicates whether successful delivery notifications are required. You can select this checkbox if the Messaging Service is FileAct or InterAct & FileAct and the Delivery Mode is Real-Time
Responder DN	Used to specify to which distinguished name the delivery notification must be sent (100 characters maximum). Present when Positive Delivery Notification is selected.
Request Type	Used to specify the request type to use when sending the delivery notification Present when Positive Delivery Notification is selected.
Connections to Alliance Gateway	<ul style="list-style-type: none"> Sequence: ID automatically assigned to the connection. You can have four connections maximum. Connection Name: Alliance Gateway connection assigned to the emission profile. The Alliance Gateway connections are defined in the Gateway Connectivity node (System node). Use Specific Authoriser DN: Authoriser DN assigned to the emission profile. If you do not specify an Authoriser DN, then Alliance Gateway determines the Authoriser DN to use. For more information about the Authoriser DN, see "Gateway Connection Details Window" on page 35. For more information about the Alliance Gateway connections, see the following sections: <ul style="list-style-type: none"> "Connections to Alliance Gateway Lists" on page 34 "Gateway Connection Details Window" on page 35

11.5.5 Emission Profile Details Window: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details for the monitoring of the emission profile selected
See "Details" on page 385
- Functions that enable you to manage the emission profile
See "Functions" on page 386

Display

The screenshot shows the 'Emission Profile Details - saacbebb_rma' window. The 'Monitoring' tab is selected. The window displays the following information:

- Status:** Disabled / Inactive
- Session Number:** 1
- Pending Messages:**
 - Urgent:** 0
 - Normal:** 0
- Sent Messages:**
 - During This Session:** 0
 - Since Last Reset:** 0 Reset

At the bottom, there are buttons for **Close**, **Refresh**, **Report**, **Enable**, **Set Automatic**, **Previous**, and **Next**.

Details

Field	Description
Status	<p>The status of the emission profile and session</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Enabled / Active • Enabled / Inactive • Disabled / Inactive
Session Number	The session number
Pending Messages	<ul style="list-style-type: none"> • Urgent: Number of urgent messages queued • Normal: Number of normal messages queued
Sent Messages	<ul style="list-style-type: none"> • During This Session: Number of messages successfully sent (by local requestor DN) in the current session • Since Last Reset: Number of messages successfully sent (by local requestor DN) since the last reset of the counter

11.5.6 Emission Profile Details Window: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Scheduled Action Details Window" on page 29.

11.5.7 Emission Profile Functions

Overview

These functions enable you to manage emission profiles.

Functions

Function	Description	Emission Profiles page	Emission Profile Details window
Add / Add As	Enables you to add an emission profile You can also add an emission profile using the characteristics of an existing emission profile with the Add As button Procedure: "Add an Emission Profile" on page 386	✓	x
Enable	Enables you to enable an emission profile Procedure: "Enable and Activate an Emission Profile" on page 389	✓	✓
Disable	Enables you to disable an emission profile Procedure: "Deactivate and Disable an Emission Profile" on page 391	✓	✓
Activate	Enables you to activate an emission profile Procedure: "Enable and Activate an Emission Profile" on page 389	✓	✓
Deactivate	Enables you to deactivate an emission profile Procedure: "Deactivate and Disable an Emission Profile" on page 391	✓	✓
Set Automatic / Set Manual	Enables you to set the operation mode to Automatic or to Manual Procedure: "Change the Operation Mode of an Emission Profile" on page 392	✓	✓
Delete	Enables you to delete an emission profile Procedure: "Delete an Emission Profile" on page 392	✓	x

11.5.8 Add an Emission Profile

Purpose

This procedure enables you to add an emission profile.

Users and permissions

To display the list or the details of emission profiles, or filter the list, your operator profile must have this action:

- **SWIFTNet Interface / Open/Print EProf**

Only the services and destinations defined with the **Service(s)** and **Own Destination(s)** permissions are displayed.

To add or modify an emission profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Add EProf**
- **SWIFTNet Interface / Modify EProf**

Procedure

1. From the list of emission profiles, click **Add**.

You can also add an emission profile using the characteristics of an existing emission profile. Select the check box of an emission profile and click **Add As**.

The **Emission Profile Details** window opens.

2. In the **Name** field, type the name of the emission profile (20 characters maximum, no spaces allowed).

Once created, you cannot change the name of the emission profile.

3. In the **Service** drop-down list, select the code for the SWIFTNet service that you are using. For example, `swift.rma`. For non-repudiation, the service name must be configured with `NR Optional` or `NR Mandated`, otherwise the message is rejected?

Once created, you cannot change the service.

4. In the **Requestor DN** field, type the requestor DN that you are using for the SWIFTNet service defined (70 characters maximum).

Once created, you cannot change the requestor DN.

Note It is possible to leave the Requestor DN blank, so that the emission profile can be used for a specific service and for any requestor DN.

In such case:

- the default delivery notification queue must be left blank
- you cannot define input channels for this profile

It is recommended that you do not mix different types of Emission Profiles for the same service. That is, either all have a Requestor DN specified, or only one is used without a Requestor DN specified.

5. In the **Retry Limit** field, indicate the number of retries for each message (retransmission after emission failure). The value can be from 0 to 5.

When the retry limit is reached, the message is routed with a Transmission Failure result.

The following table provides an overview of the retry conditions:

Retry summary

Retry behaviour	Retry until (reject locally upon failure to deliver)	Applies to
Retry with an incremental delay calculated by Alliance Access, taking into account the emission expiry of the message and the number of previous emission attempts.	The absolute expiry time present in the message has been reached (YYYYMMDDHHMM).	InterAct and FileAct real-time services only
Rejected locally if there was a failed delivery in the last 30 minutes for the correspondent. For X number of times, with an interval of Y seconds.	The maximum number of retries (X) set by the emission profile has been reached. X is defined in Retry Limit parameter in the Emission Profile (default is 2). Y is defined in the Retry Timer parameter in the system configuration parameters (default is 60 seconds).	InterAct and FileAct Store-and-Forward services only

For more information on expiry date and time, see "Message Partner Details Window: Configuration Tab" on page 305 (the **Emission Expiry** field), and the **Expiry Date Time** field in "Message Details Page" in the [Message Management Guide](#).

Note An event (28159) is logged when an error is returned for an SnF InterAct message emission attempt, to indicate not only the error but also that emission will be retried. Such retries only happen when using input channels and always use the same ISN as in the previous attempt.

6. In the **Security Level** drop-down list, select one of the following values:

- Without Signature
- With Signature
- With signature and non repudiation

7. In the **Messaging Service** drop-down list, select one of the following values:

- InterAct
- FileAct
- InterAct & FileAct

8. In the **Delivery Mode** drop-down list, select one of the following values:

- Real-Time
- Store-and-Forward

If this method is selected, then you can indicate the following:

- **Delivery Notification Queue:** Indicate the name of the store-and-forward queue that must be used to store store-and-forward delivery notifications (failed delivery notifications and optional successful delivery notifications). 30 characters maximum.

Important You must ensure also that an equivalent store-and-forward reception profile is created, which includes this Delivery Notification queue.

- If the **Message Service** is InterAct, then the **Input Channel Name** drop-down list appears: Select an input channel in the drop-down list or select Do not use an Input Channel.

The selection must match the SWIFTNet service characteristics as provisioned centrally.

9. In the **Window Size** field, indicate a window size. The minimum value is 1 and there is no maximum value (the default is 12).
10. Select the **Positive Delivery Notification** check box, if you require notifications of a successful delivery.

If you select the **Positive Delivery Notification** check box, then the following fields are displayed:

- **Responder DN:** Specify to which distinguished name the delivery notification must be sent (100 characters maximum).
- **Request Type:** Specify the request type to use when sending the delivery notification.

11. Click **Save**.

A status popup message appears.

12. When creating an emission profile, you also have to define connections to Alliance Gateway before the emission profile can be enabled. See "Add an Alliance Gateway Connection" on page 37.

13. Click **Close**.

The **Emission Profile Details** window closes.

Once created, you can modify an emission profile if the profile is **Disabled** (see "Deactivate and Disable an Emission Profile" on page 391).

11.5.9 Enable and Activate an Emission Profile

Purpose

This procedure enables you to enable and activate an emission profile.

When you have completed the setup of an emission profile, you must enable it ready for use and then activate it to initiate message traffic. You can also create schedules to allow profiles to be automatically "activated" and "deactivated".

Users and permissions

To display the list or the details of emission profiles, or filter the list, your operator profile must have this action:

- **SWIFTNet Interface / Open/Print EProf**

Only the services and destinations defined with the **Service(s)** and **Own Destination(s)** permissions are displayed.

To enable and activate an emission profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Enable EProf**
- **SWIFTNet Interface / Activate EProf**

Input channels

When enabling a store-and-forward emission profile that uses an input channel, Alliance Access checks that if the input channel is shared with other store-and-forward emission profiles that are already enabled. If it is shared, the window size defined for the emission profile being enabled is the same as the window size defined for the other emission profiles that share the same input channel. Otherwise, the emission profile is not enabled and an explicit error message is returned to the operator.

When activating a store-and-forward emission profile using an input channel, Alliance Access passes the window size defined at the emission profile level in the Open Channel request to store-and-forward. Because Alliance Access always requests to open an input channel in forced mode, this enables store-and-forward to assign an actual window size to the emission profile session, as follows:

- If the input channel is shared by other activated emission profiles, then the window size of the shared input channel is assigned to the emission profile session.
- If the input channel is not shared by other activated emission profiles and the input channel is being recovered, then the same window size as before the failure is assigned to the emission profile/input channel session.
- If the input channel is not shared by other activated emission profiles and the input channel is not being recovered, the window size defined at the emission profile level is assigned to the emission profile/input channel session if it is not greater than the SWIFT store-and-forward service maximum value. Otherwise, the store-and-forward maximum value is assigned to the emission profile/input channel session.

Prerequisites

You must define at least a primary connection (and associated authoriser DN) before the emission profile can be enabled.

Before enabling and activating an emission profile, you must first start the SWIFTNet Interface Services (SNIS) component. See "Description of a Component" on page 71.

Procedure

1. From the list of emission profiles, select the check box for the emission profile that you want to enable in the left column.
2. Click **Enable**.

A status popup message appears.

- The status changes to Enabled.
3. Select the check box for the emission profile again.
 4. Click **Activate**.

A status popup message appears.

The session status changes to Active.

11.5.10 Deactivate and Disable an Emission Profile

Purpose

This procedure enables you to deactivate and disable an emission profile.

Important Deactivating an emission profile aborts all ongoing file transfers.

You can also create schedules to allow profiles to be automatically "activated" and "deactivated".

If the emission profile is in **Automatic** mode, then you have to switch to **Manual** mode first and then deactivate and disable the profile.

Users and permissions

To display the list or the details of emission profiles, or filter the list, your operator profile must have this action:

- **SWIFTNet Interface / Open/Print EProf**

Only the services and destinations defined with the **Service(s)** and **Own Destination(s)** permissions are displayed.

To deactivate and disable an emission profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Deactivate EProf**
- **SWIFTNet Interface / Disable EProf**

Procedure

1. From the list of emission profiles, select the check box for the emission profile that you want to deactivate in the left column.
 2. Click **Deactivate**.
- A status popup message appears.
- The session status changes to **Inactive**.
3. Select the check box for the emission profile again.
 4. Click **Disable**.
- A status popup message appears.
- The status changes to **Disabled**.

11.5.11 Change the Operation Mode of an Emission Profile

Purpose

This procedure enables you to change the operation mode of an emission profile.

Users and permissions

To display the list or the details of emission profiles, or filter the list, your operator profile must have this action:

- **SWIFTNet Interface / Open/Print EProf**

Only the services and destinations defined with the **Service(s)** and **Own Destination(s)** permissions are displayed.

To change the operation mode of an emission profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Enable EProf Auto** (to change the operational mode of an emission profile to automatic)
- **SWIFTNet Interface / Disable EProf Auto** (to change the operational mode of an emission profile to manual)

Procedure

1. From the list of emission profiles, select the check boxes for one or several emission profiles in the left column. You can select all the emission profiles by selecting the check box in the column heading line.
2. Given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

11.5.12 Delete an Emission Profile

Purpose

This procedure enables you to delete an emission profile.

Users and permissions

To display the list or the details of emission profiles, or filter the list, your operator profile must have this action:

- **SWIFTNet Interface / Open/Print EProf**

Only the services and destinations defined with the **Service(s)** and **Own Destination(s)** permissions are displayed.

To delete emission profiles, your operator profile must have the following additional action:

- **SWIFTNet Interface / Remove EProf**

Prerequisites

You can delete an emission profile if the profile is **Disabled** (see "Deactivate and Disable an Emission Profile" on page 391).

Procedure

1. From the list of emission profiles, select the check boxes of one or several emission profiles in the left column.
2. Click **Delete**.
The **Delete Confirmation** window opens.
3. Click **OK**.
The **Delete Confirmation** window closes.
A status popup message appears.

11.5.13 Monitor an Emission Profile Session

Purpose

This procedure enables you to monitor an emission profile session.

Users and permissions

To display the list or the details of emission profiles, or filter the list, your operator profile must have this action:

- **SWIFTNet Interface / Open/Print EProf**

Only the services and destinations defined with the **Service(s)** and **Own Destination(s)** permissions are displayed.

To monitor an emission profile session, your operator profile must have the following additional entity:

- **Monitoring**

Procedure

1. From the list of emission profiles, click the row of the emission profile which you want to monitor.
The **Emission Profile Details** window opens.
2. Click the **Monitoring** tab.
3. You can click **Refresh** to refresh the list.
The **Reset** button enables you to reset the counter.
4. Click **Close**.
The **Emission Profile Details** window closes.

11.6 Input Channels

11.6.1 Input Channels

Introduction

The introduction of input channels and input sequence numbers (ISNs) in store-and-forward provides Sender-to-Receiver FIFO, gap detection, and duplicate detection.

InterAct store-and-forward messages exchanged over these input channels are numbered sequentially. In the event of a transmission failure, the transmission is retried, using the same sequence number (without any additional PDE indication).

For each input channel, store-and-forward maintains a sliding window of statuses of received messages and gaps between received messages. Within that window, it can identify duplicates and replay its original responses (accepted messages only, rejected messages are ignored by store-and-forward and considered as gaps). For more information, see advanced delivery control in the [SWIFTNet Service Description](#).

The input channel is an attribute of store-and-forward emission profiles. The activation or deactivation of an emission profile (either manual or automatic) opens or closes the associated input channel if required.

When Alliance Access opens an input channel, it logically establishes an input session with SWIFTNet and receives an input session token. During such an input session, the session token is repeated in all InterAct store-and-forward messages sent. These messages are numbered in sequence.

The number of messages that can be sent by Alliance Access without receiving an acknowledgement is controlled by the input channel window size. This window size is defined at opening time and the sequence number of each message sent must be within it.

Requirements

Alliance Access uses input channels in an exclusive manner. This means that an Alliance Access instance cannot share an input channel for message transfer with any other application.

When an emission profile is activated, the associated input channel may be opened in forced mode. This means that any message transfer by other applications using this channel are interrupted.

Important Attempting to use the same input channel by several applications may cause the connection of the emission profile/input channel to bounce back and forth from the different applications, resulting in PDE and Naked messages.

Setting up input channels

When an institution subscribes for the first time to the store-and-forward service, SWIFT automatically creates two generic input channels for that institution (for live and pilot environments). Their names are **<BIC8>_generic** and **<BIC8>_generic!p** where **<BIC8>** is the BIC8 of the institution.

Events are recorded to show the opening and closing of the input channel, and to log actions on the input channels (create, delete, adopt, and remove).

Multiple emission profiles can use the same input channel.

11.6.2 Input Channels Page

Content

The **Input Channels** page contains these elements:

- Details of the available input channels
See "Details" on page 395
- Functions that enable you to manage the input channels
See "Functions" on page 395

Display

Input Channels		Rows in list: 20 , in selection: 1							
		Change View	Adopt	Create on SWIFTNet	Delete	Delete from SWIFTNet	Report	< Previous	Next >
	Name								
<input type="checkbox"/>	saaaabbb_generic								
<input checked="" type="checkbox"/>	saaaabbb_generic								
<input type="checkbox"/>	saaaabbb_genericclp								
<input type="checkbox"/>	sabbbbbb_generic								
<input type="checkbox"/>	sabbbbbb_genericclp								

Details

Column	Description
Name	The name of the input channel

Functions

Function	Description
Adopt	Enables you to adopt an input channel Procedure: "Adopt an Input Channel" on page 397
Create on SWIFTNet	Enables you to create an input channel on SWIFTNet Procedure: "Create an Input Channel on SWIFTNet" on page 395
Delete	Enables you to delete an input channel Procedure: "Delete an Input Channel" on page 398
Delete from SWIFTNet	Enables you to delete an input channel from SWIFTNet Procedure: "Delete an Input Channel from SWIFTNet" on page 396

11.6.3 Create an Input Channel on SWIFTNet

Purpose

This procedure enables you to create an input channel on SWIFTNet.

Users and permissions

To create input channels, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print IChan**
- **SWIFTNet Interface / Create IChan**

Prerequisites

The BIC8 that you want to create the input channel for must be in use in an active SWIFTNet Adapter.

Procedure

1. Click **Create on SWIFTNet**.
The **Create Input Channel on SWIFTNet** window opens.
2. Select the BIC8 that you require from the drop-down list in the first part of the **Input Channel** field.
3. Enter the reference in the second part of the **Input Channel** field.
You can enter a maximum of 20 alphanumeric characters.
4. Enter the appropriate value for the environment in the third part of the **Input Channel** field:
 - **x** designates developer testing
 - **p** designates pilot operations (Test and Training)
 - No value designates live operations
5. Select the value that you require from the **Connection** drop-down list.
6. Select the **Use Specific Authoriser DN** check box, if required.
The **Authoriser DN** field appears.
7. Enter the value for the **Authoriser DN**, if required.
8. Click **Create on SWIFTNet**.
The **Create Input Channel on SWIFTNet** window closes.
A status popup message appears.

The system creates the input channel on SWIFTNet and the new input channel appears in the list on the **Input Channels** page.

11.6.4 Delete an Input Channel from SWIFTNet

Purpose

This procedure enables you to delete an input channel from SWIFTNet.

This procedure only deletes the input channel from SWIFTNet, the input channel remains in Alliance Access.

You cannot recreate an input channel on SWIFTNet once it has been deleted from SWIFTNet.

Users and permissions

To delete input channels from SWIFTNet, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print IChan**
- **SWIFTNet Interface / Delete IChan**

Prerequisites

You must remove the emission profiles configured with the selected input channel before you can delete the input channel from SWIFTNet. To remove emission profiles, see "Delete an Emission Profile" on page 392.

Procedure

1. Select the check box of the input channel that you require.
 2. Click **Delete from SWIFTNet**.
- The **Delete Input Channel from SWIFTNet** window opens.
3. Select the value that you require from the **Connection** drop-down list.
 4. Select the **Use Specific Authoriser DN** check box, if required.
- The **Authoriser DN** field appears.
5. Enter the value for the **Authoriser DN**, if required.
 6. Click **Delete from SWIFTNet**.
- The **Delete Input Channel from SWIFTNet** window closes.
- A status popup message appears.
- The system deletes the input channel from SWIFTNet.

11.6.5 Adopt an Input Channel

Purpose

This procedure enables you to adopt an input channel from another application so that Alliance Access can use it.

Users and permissions

To adopt input channels, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print IChan**
- **SWIFTNet Interface / Adopt IChan**

Procedure

1. Click **Adopt**.
- The **Adopt Input Channel** window opens.
2. Select the BIC8 that you require from the drop-down list in the first part of the **Input Channel** field.

3. Enter the remainder of the input channel name in the second and third parts of the **Input Channel** field, as necessary.
4. Click **Adopt**.

The **Adopt Input Channel** window closes.

A status popup message appears.

The adopted input channel appears in the list on the **Input Channels** page.

11.6.6 Delete an Input Channel

Purpose

This procedure enables you to delete an input channel from Alliance Access.

This procedure only deletes the input channel from Alliance Access, the input channel remains on SWIFTNet.

Users and permissions

To delete input channels, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print IChan**
- **SWIFTNet Interface / Remove IChan**

Procedure

1. Select the check box of the input channel that you require.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

The **Delete Confirmation** window closes.

A status popup message appears.

The system removes the input channel from the list on the **Input Channels** page.

11.7 Reception Profiles

11.7.1 Reception Profile

SWIFTNet profiles

The flow of messages to and from SWIFTNet is managed through the following profiles in Alliance Access:

- emission profiles for outgoing messages
- reception profiles for incoming messages

Reception profile

A reception profile controls the message flow of incoming messages.

The reception profile defines the delivery mode and the queue (for store-and-forward mode) for the MX messages received.

You can configure schedules to activate and deactivate a reception profile automatically.

For each profile defined, a SWIFTNet connection must also be assigned. Profiles must be enabled and activated to be ready for use, before Alliance Access receives InterAct and FileAct messages from SWIFTNet.

FIN Test and Training

A reception profile must be defined for each licensed live BIC8 that will be used to sign all authorisation messages for FIN Test and Training. That licensed BIC is referred to as the Signing BIC for Test and Training.

11.7.2 Reception Session

Overview of reception session

1. Alliance Access stores the InterAct or FileAct messages that it receives from SWIFTNet in the **_SI_from_SWIFTNet** queue.
For information about this queue, see "List of System Queues" on page 454.
2. When a reception profile is activated, Alliance Access starts a reception session and checks for messages in the **_SI_from_SWIFTNet** queue.

Note If the reception profile fails to access the **_SI_from_SWIFTNet** queue, then the profile becomes inactive.

Important Deactivating an emission or reception profile aborts all ongoing file transfers.

3. InterAct or FileAct message instances are routed immediately from this queue to other queues or to message partners, such as a back-office application.
4. A session number is maintained for each reception profile and incremented each time the reception profile is activated. Each time a message is received or an attempt to retrieve a message is made, an "appendix" is created containing key information about reception session and message status.
5. **For real-time mode:**

An empty InterAct response is generated for each message received. The signing and non-repudiation parameters used for the request are used in the response.

The routing of messages is driven by the message reception registry (MRR) central mechanism and is based on requestor DN, responder DN, SWIFTNet service, and request type.

Service providers must configure the central MRR rules to allow the routing of InterAct and FileAct requests to a SWIFTNet Link server. The MRR allows the definition of a primary BCS address (SWIFTNet Link identifier and SWIFTNet Link endpoint) and a secondary BCS address which can be selected if the primary SWIFTNet Link is unavailable. The session holder is the SWIFTNet Link endpoint on which the message was received.

Note

Enabling a real-time reception profile without a service or responder DN defined is only possible if there is no other real-time reception profile without a service or responder DN already enabled and assigned to the same Alliance Gateway connection. This applies regardless of whether the enable request originates from the Web Platform GUI, the Workstation GUI, or the `saa_manage` command-line tool.

Messages received over a real-time SWIFTNet service must be routed to a real-time reception profile that is assigned to the Alliance Gateway connection from which the message was received and that matches the service and responder DN of the message. If no such reception profile exists, the message is routed to the unique real-time reception profile that is assigned to the Alliance Gateway connection from which the message was received and that is not associated with any service/responder DN. If no such profile exists, the message cannot be received.

6. For store-and-forward mode

An output channel that is associated with a store-and-forward queue must first be opened before it is possible to receive messages from that queue. Therefore, the authoriser DN must have an RBAC access role granted to access the queue.

Upon successful opening of the output channel, a store-and-forward session identifier is created by the central store-and-forward engine, and messages delivery is started. If the reception profile fails to open the output channel, then the reception profile becomes inactive.

Store-and-forward queues can contain both messages and delivery notifications (positive or negative, as specified at message emission time). Messages are stored in store-and-forward queues as according to the MRR routing rules.

The Traffic Reconciliation component must reconcile the delivery notification with the original message instance. To do this, a pseudo MX delivery notification message, or the delivery notification system message (depending on the setting of the emission profile field **Delivery Notif via SysMsg**), is created and routed to the `_TR_REC` queue through an internal routing rule.

11.7.3 Reception Profiles Page

Content

The **Reception Profiles** page contains these elements:

- A filtering criterion and filtering functionality that enable you to filter the list entities on the **Reception Profiles** page:
 - See "Details" on page 401
 - See "Functions" on page 22
- Details of the available reception profiles
 - See "Details" on page 401
- Functions that enable you to manage the reception profiles
 - See "Functions" on page 407

Display

Reception Profiles

Filtering Criteria

Name

Reception Profiles Rows in list: 100 , in selection: 0

<input type="button" value="Change View"/>	<input type="button" value="Refresh"/>	<input type="button" value="Add"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Activate"/>	<input type="button" value="Deactivate"/>	<input type="button" value="Set Automatic"/>	<input type="button" value="Set Manual"/>	<input type="button" value="Delete"/>	<input type="button" value="Report"/>	<input type="button" value="Previous"/>	<input type="button" value="Next"/>
Name	Delivery Mode	Connection	Queue Name	Operation Mode	Output Channel	Status	Session Status					
<input type="checkbox"/> Delivery_A	Store-and-Forward		saabbebb_delivery	Manual		Disabled	Inactive					
<input type="checkbox"/> Delivery_B	Store-and-Forward		saacbebb_delivery	Manual		Disabled	Inactive					
<input type="checkbox"/> Delivery_C	Store-and-Forward		saacbebb_delivery	Manual		Disabled	Inactive					

Details

Column	Description	Filtering criteria
Name	The reception profile name The wildcard characters % and _ enable you to search for a group of reception profiles.	✓
Output Channel	The Output Channel (for store-and-forward delivery mode)	
Delivery Mode	These are the possible values: <ul style="list-style-type: none"> • Real-Time • Store-and-Forward 	
Connection	The name of the Alliance Gateway connection	
Queue Name	The name of the store-and-forward queue that must be used with the reception profile	
Output Channel	The output channel, which is used for InterAct messaging services that operate in store-and-forward mode.	
Operation Mode	Indicates the mode in which the reception profile is. In Alliance Access, there are two modes in which the reception profile can operate. The two modes of operation are Manual and Automatic . The automatic mode enables you to schedule operations. When the reception profile is operating in manual mode, none of the scheduled operations are activated.	
Status	The current status of the reception profile These are the possible values: <ul style="list-style-type: none"> • Enabled • Disabled 	

Column	Description	Filtering criteria
Session Status	<p>The status of the reception session</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Active: The profile has been activated and the session for this profile is in progress. • Inactive: The profile has been deactivated and the session is inactive. • Activating: The profile was inactive, the profile is in the process of being activated. • Deactivating: The profile was active, but the session has been interrupted and the profile is in the process of being "deactivated". The system attempts to resume the session automatically. • Interrupted: The profile was active, but the session has been interrupted. The system attempts to resume the session automatically. 	

11.7.4 Reception Profile Details Window: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details for the configuration of the reception profile selected
See "Details" on page 403
- Functions that enable you to manage the reception profile
See "Functions" on page 407

Display

Reception Profile Details - saabbebb_rma

Configuration Monitoring Scheduling

Name: saabbebb_rma

Status: Disabled / Inactive

Operation Mode: Manual

Delivery Mode: Store-and-Forward

Queue Name: saabbebb_rma

Use Specific Output Channel:

Use Specific Window Size:

OSN Resequencing:

Available Subsets and Order: Urgent, Normal, System_Urgent, System_Normal, FileAct_Urgent, FileAct_Normal, InterAct_Urgent

Selected Subsets and Order: System, InterAct, FileAct

Connections to Alliance Gateway

Rows in list: 1, in selection: 0

Add	Delete	Move down	Move up
Sequence	Connection Name	Authoriser DN	
1	sms1d		

Close Refresh Report Enable Set Automatic Previous Next

Details

Field	Description
Name	The reception profile name. 20 characters maximum, no spaces allowed.
Status	<p>The status of the reception profile and session</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Enabled / Active Enabled / Inactive Disabled / Inactive
Service	<p>The SWIFTNet service for which the message is received.</p> <p>If Delivery Mode is set to Real-Time, this field is available. This field and the Responder DN field must either be both populated or both empty.</p> <p>Using this field (along with the Responder DN field) enables you to specify the authoriser DN to be used by Alliance Gateway for the delivery notification that must be sent to correspondents of the customer that have requested to receive such delivery notifications for their real-time messages. For more information on specifying the authoriser DN, see "Gateway Connection Details Window" on page 77.</p> <p>After the real-time reception profile has been created, this field can be modified only if the reception profile has been disabled.</p>

Field	Description
Responder DN	<p>The receiver of a message, which is a Responder DN level 2 (BIC8) and its descendants.</p> <p>If Delivery Mode is set to Real-Time, this field is available. This is a free-text field. This field and the Service field must either be both populated or both empty.</p> <p>Using this field (along with the Service field) enables you to specify the authoriser DN to be used by Alliance Gateway for the delivery notification that must be sent to correspondents of the customer that have requested to receive such delivery notifications for their real-time messages. For more information on specifying the authoriser DN, see "Gateway Connection Details Window" on page 77.</p> <p>After the real-time reception profile has been created, this field can be modified only if the reception profile has been disabled.</p>
Operation Mode	<p>Indicates the mode in which the reception profile is. In Alliance Access, there are two modes in which the reception profile can operate. The two modes of operation are Manual and Automatic. The automatic mode enables you to schedule operations. When the reception profile is operating in manual mode, none of the scheduled operations are activated.</p>
Delivery Mode	<p>These are the possible values:</p> <ul style="list-style-type: none"> • Real-Time • Store-and-Forward
Queue Name	<p>The name of the store-and-forward queue that must be used with the reception profile. 30 characters maximum, _ ! - can be used.</p> <p>Only displayed if the Delivery Mode is Store-and-Forward.</p>
Use Specific Output Channel	<p>If the Use Specific Output Channel check box is selected, then the Output Channel drop-down list is displayed.</p> <p>Only displayed if the Delivery Mode is Store-and-Forward.</p>
Use Specific Window Size	<p>If the Use Specific Window Size check box is selected, then the Window Size field is displayed.</p> <p>Window size used for the reception. The value can be from 1 to 100. The default is 10.</p> <p>Only displayed if the Delivery Mode is Store-and-Forward.</p>
Subsets and Order	<p>The type of traffic and the order in which the traffic is delivered. The default order is: System, InterAct, FileAct. You can specify a maximum of 6 types.</p> <p>Only displayed if the Delivery Mode is Store-and-Forward.</p>
OSN Resequencing	<p>For Store-and Forward reception profiles only, if selected, Alliance Access applies OSN resequencing to messages received from that reception profile, regardless of the value of the <code>SAA_DO_RESEQ_<RPname></code> environment variable value.</p> <p>If not selected, Alliance Access either applies or doesn't apply OSN resequencing to messages received from that Store-and-Forward reception profile, based on the value of the <code>SAA_DO_RESEQ_<RPname></code> environment variable value.</p>

Field	Description
Connections to Alliance Gateway	<ul style="list-style-type: none"> Sequence: ID automatically assigned to the connection. You can have four connections maximum. Connection Name: Alliance Gateway connection assigned to the reception profile. The Alliance Gateway connections are defined in the Gateway Connectivity node (System node). Authoriser DN: Authoriser distinguished name assigned to the reception profile. For more information about the Alliance Gateway connections, see the following sections: <ul style="list-style-type: none"> "Connections to Alliance Gateway Lists" on page 34 "Gateway Connection Details Window" on page 35

11.7.5 Reception Profile Details Window: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details for the monitoring of the reception profile selected
See "Details" on page 406
- Functions that enable you to manage the reception profile
See "Functions" on page 407

Display

Reception Profile Details

Configuration Monitoring Scheduling Help

Status **Disabled / Inactive**

Session Number 0

Received Messages

During This Session 0

Since Last Reset 0 **Reset**

Close Refresh Report Enable Set Automatic Previous Next

Details

Field	Description
Status	<p>The status of the reception profile and session.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> Enabled / Active Enabled / Inactive Disabled / Inactive
Session Number	The session number
Received Messages	<ul style="list-style-type: none"> During This Session: Number of messages successfully received (for local responder DN) in the current session. Since Last Reset: Number of messages successfully received (for local responder DN) since the last reset of the counter.

11.7.6 Reception Profile Details Window: Scheduling Tab

Overview

The functionality for scheduled actions is generic within Alliance Access Configuration:

- For details of the **Scheduling** tab, see "Tabs with Scheduled Actions Lists" on page 28.
- For details of the **Scheduled Action Details** window, see "Scheduled Action Details Window" on page 29.

11.7.7 Reception Profile Functions

Overview

These functions enable you to manage reception profiles.

Functions

Function	Description	Reception Profiles page	Reception Profile Details window
Add / Add As	Enables you to add a reception profile You can also add a reception profile using the characteristics of an existing reception profile with the Add As button Procedure: "Add a Reception Profile" on page 407	✓	x
Enable	Enables you to enable a reception profile Procedure: "Enable and Activate a Reception Profile" on page 409	✓	✓
Disable	Enables you to disable a reception profile Procedure: "Deactivate and Disable a Reception Profile" on page 410	✓	✓
Activate	Enables you to activate a reception profile Procedure: "Enable and Activate a Reception Profile" on page 409	✓	✓
Deactivate	Enables you to deactivate a reception profile Procedure: "Deactivate and Disable a Reception Profile" on page 410	✓	✓
Set Automatic / Set Manual	Enables you to set the operation mode to Automatic or to Manual Procedure: "Change the Operation Mode of an Emission Profile" on page 392	✓	✓
Delete	Enables you to delete a reception profile Procedure: "Delete a Reception Profile" on page 411	✓	x

11.7.8 Add a Reception Profile

Purpose

This procedure enables you to add a reception profile.

Users and permissions

To display the list or the details of reception profiles, or filter the list, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print RProf RT** (for real-time reception profiles)
- **SWIFTNet Interface / Open/Print RProf SnF** (for store-and-forward reception profiles)

For store-and-forward, only the destinations defined with the **Own Destination(s)** permission are displayed.

To add or modify a reception profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Add RProf**
- **SWIFTNet Interface / Modify RProf**

Procedure

1. From the list of reception profiles, click **Add**.

You can also add a reception profile using the characteristics of an existing reception profile. Select the check box of a reception profile and click **Add As**.

The **Reception Profile Details** window opens.

2. In the **Name** field, type the name of the reception profile (20 characters maximum, no spaces allowed).

Once created, you cannot change the name of the reception profile.

3. In the **Delivery Mode** drop-down list, select one of the following values:

- Real-Time
- Store-and-Forward

If this method is selected, then you can indicate the following:

- **Queue Name:** Indicate the name of the store-and-forward queue that must be used with this reception profile. 30 characters maximum, _ ! - can be used.
- **Use Specific Output Channel:** Select an output channel in the **Output Channel** drop-down list.
- **Use Specific Window Size:** Indicate a window size in the **Window Size** field. The value can be from 0 to 100.
- **Subsets and Order:** Select the type of traffic and the order in which the traffic is delivered. The default order is: System, InterAct, FileAct.

Note To receive delivery notifications, verify that the **InterAct** subset is selected.

For a description of the different types of delivery notifications, see the [SWIFTNet Messaging Operations Guide](#).

The selection must match the SWIFTNet service characteristics as provisioned centrally.

4. Click **Save**.

A status popup message appears.

5. When creating a reception profile, you also have to define connections to Alliance Gateway before the reception profile can be enabled. See "Add an Alliance Gateway Connection" on page 37.
6. Click **Close**.

The **Reception Profile Details** window closes.

Once created, you can modify a reception profile if the profile is **Disabled**.

11.7.9 Enable and Activate a Reception Profile

Purpose

This procedure enables you to enable and activate a reception profile.

When you have completed the setup of a reception profile, you must enable it ready for use and then activate it to initiate message traffic. You can also create schedules to allow profiles to be automatically "activated" and "deactivated".

For information about how an emission session happens, see the [Configuration Guide](#).

Users and permissions

To display the list or the details of reception profiles, or filter the list, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print RProf RT** (for real-time reception profiles)
- **SWIFTNet Interface / Open/Print RProf SnF** (for store-and-forward reception profiles)

For store-and-forward, only the destinations defined with the **Own Destination(s)** permission are displayed.

To enable and activate a reception profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Enable RProf**
- **SWIFTNet Interface / Activate RProf**

Prerequisites

You must define at least a primary connection (and associated authoriser DN) before the reception profile can be enabled.

Before enabling and activating a reception profile, you must first start the SWIFTNet Interface Services (SNIS) component. See "Description of a Component" on page 71.

Procedure

1. From the list of reception profiles, select the check boxes for one or several reception profiles in the left column.
 2. Click **Enable**.
- A status popup message appears.
- The status changes to **Enabled**.
3. Select the check box for the reception profile again.
 4. Click **Activate**.

A status popup message appears.

The session status changes to `Active`.

11.7.10 Deactivate and Disable a Reception Profile

Purpose

This procedure enables you to deactivate and disable a reception profile.

Important Deactivating a reception profile aborts all ongoing file transfers.

You can also create schedules to allow profiles to be automatically "activated" and "deactivated".

If the reception profile is in `Automatic` mode, you have to switch to `Manual` mode first and then deactivate and disable the profile.

Users and permissions

To display the list or the details of reception profiles, or filter the list, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print RProf RT** (for real-time reception profiles)
- **SWIFTNet Interface / Open/Print RProf SnF** (for store-and-forward reception profiles)

For store-and-forward, only the destinations defined with the **Own Destination(s)** permission are displayed.

To deactivate and disable a reception profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Deactivate RProf**
- **SWIFTNet Interface / Disable RProf**

Procedure

1. From the list of reception profiles, select the check box for the reception profile that you want to deactivate in the left column.

2. Click **Deactivate**.

A status popup message appears.

The session status changes to `Inactive`.

3. Select the check box for the reception profile again.

4. Click **Disable**.

A status popup message appears.

The status changes to `Disabled`.

11.7.11 Change the Operation Mode of a Reception Profile

Purpose

This procedure enables you to change the operation mode of a reception profile.

Users and permissions

To display the list or the details of reception profiles, or filter the list, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print RProf RT** (for real-time reception profiles)
- **SWIFTNet Interface / Open/Print RProf SnF** (for store-and-forward reception profiles)

For store-and-forward, only the destinations defined with the **Own Destination(s)** permission are displayed.

To change the operation mode of a reception profile, your operator profile must have the following additional actions:

- **SWIFTNet Interface / Enable RProf Auto** (to change the operational mode of a reception profile to automatic)
- **SWIFTNet Interface / Disable RProf Auto** (to change the operational mode of a reception profile to manual)

Procedure

1. From the list of reception profiles, select the check boxes for one or several reception profiles in the left column. You can select all the reception profiles by selecting the check box in the column heading line.
2. Given the operation mode which is already selected, click **Set Automatic** or **Set Manual**.

11.7.12 Delete a Reception Profile

Purpose

This procedure enables you to delete a reception profile.

Users and permissions

To display the list or the details of reception profiles, or filter the list, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print RProf RT** (for real-time reception profiles)
- **SWIFTNet Interface / Open/Print RProf SnF** (for store-and-forward reception profiles)

For store-and-forward, only the destinations defined with the **Own Destination(s)** permission are displayed.

To delete a reception profile, your operator profile must have the following additional action:

- **SWIFTNet Interface / Remove RProf**

Prerequisites

You can delete a reception profile if the profile is **Disabled**.

Procedure

1. From the list of reception profiles, select the check box of one or several reception profiles in the left column.
2. Click **Delete**.

3. The **Delete Confirmation** window opens.
 3. Click **OK**.
- The **Delete Confirmation** window closes.
- A status popup message appears.

11.7.13 Monitor a Reception Profile Session

Purpose

This procedure enables you to monitor a reception profile session.

Users and permissions

To display the list or the details of reception profiles, or filter the list, your operator profile must have these actions:

- **SWIFTNet Interface / Open/Print RProf RT** (for real-time reception profiles)
- **SWIFTNet Interface / Open/Print RProf SnF** (for store-and-forward reception profiles)

For store-and-forward, only the destinations defined with the **Own Destination(s)** permission are displayed.

To monitor a reception profile session, your operator profile must have the following additional entity:

- **Monitoring**

Procedure

1. From the list of reception profiles, click the row of the reception profile which you want to monitor.

The **Reception Profile Details** window opens.

2. Click the **Monitoring** tab.

3. You can click **Refresh** to refresh the list.

The **Reset** button enables you to reset the counter.

4. Click **Close**.

The **Reception Profile Details** window closes.

11.8 Output Channels

11.8.1 Output Channels

Definition

Output channels are used to identify output sessions with SWIFT. An output session is used to control the way and the order in which messages or files are delivered by SWIFT to the receiver.

During an output session SWIFT delivers traffic to a messaging interface with an output sequence numbering which allows to control the order of delivery and to identify missing messages.

Output sessions existed already before the concept of output channels was introduced. Output sessions were in fact queue sessions. At a given time only one session existed for a given queue.

Starting an output session was equivalent to acquiring the queue. Stopping an output session was equivalent to releasing the queue.

The concept of output channel allows multiple output sessions on a queue in such a way that these output sessions are easily identified and managed. Indeed, without output channels, there is only one output session possible at a given time for a queue, and there is only one output sequence numbering for that queue. That output sequence numbering is maintained across the output sessions, so that the order of the messages delivered from that queue can be established.

When using output channels, each output channel has its own output sequence numbering maintained across output sessions for that output channel. When opening an output channel, traffic is delivered from the queue specified within the opening of the output channel.

For more information, see advanced delivery control in the [SWIFTNet Service Description](#).

11.8.2 Output Channels Page

Content

The **Output Channels** page contains these elements:

- Details of the available output channels
 - See "Details" on page 414
- Functions that enable you to manage the output channels
 - See "Functions" on page 414

Display

Output Channels		Rows in list: 20 , in selection: 1							
		Change View	Adopt	Create on SWIFTNet	Delete	Delete from SWIFTNet	Report	Previous	Next >
	Name								
<input type="checkbox"/>	saaabebb_generic								
<input type="checkbox"/>	saaabebb_generic\p								
<input type="checkbox"/>	saabbebb_generic								
<input type="checkbox"/>	saabbebb_generic\p								

Details

Column	Description
Name	The name of the output channel

Functions

Function	Description
Adopt	Enables you to adopt an output channel Procedure: "Adopt an Output Channel" on page 415
Create on SWIFTNet	Enables you to create an output channel on SWIFTNet Procedure: "Create an Output Channel on SWIFTNet" on page 414
Delete	Enables you to delete an output channel Procedure: "Delete an Output Channel" on page 416
Delete from SWIFTNet	Enables you to delete an output channel from SWIFTNet Procedure: "Delete an Output Channel from SWIFTNet" on page 415

11.8.3 Create an Output Channel on SWIFTNet

Purpose

This procedure enables you to create an output channel on SWIFTNet for one of your licensed BIC8.

Users and permissions

To create output channels, your operating profile must have these actions:

- **SWIFTNet Interface / Open/Print OChan**
- **SWIFTNet Interface / Create OChan**

Procedure

1. Click [Create on SWIFTNet](#).
The **Create Output Channel on SWIFTNet** window opens.
2. Select the BIC8 that you require from the drop-down list in the first part of the **Output Channel** field.
3. Enter the reference in the second part of the **Output Channel** field.
You can enter a maximum of 20 alphanumeric characters.
4. Enter the appropriate value for the environment in the third part of the **Output Channel** field:
 - **x** designates developer testing
 - **p** designates pilot operations (Test and Training)
 - No value designates live operations
5. Select the value that you require from the **Connection** drop-down list.

6. Select the **Use Specific Authoriser DN** check box, if required.

The **Authoriser DN** field appears in the **Create Output Channel on SWIFTNet** window.

7. Enter the value for the **Authoriser DN**.

If you do not select this check box, then Alliance Gateway determines the DN to be used. Alliance Gateway selects a DN with the same BIC8 as in the **Output Channel** field.

8. Click **Create on SWIFTNet**.

The **Create Output Channel on SWIFTNet** window closes.

The system creates the output channel on SWIFTNet and the new output channel appears in the list on the **Output Channels** page.

11.8.4 Delete an Output Channel from SWIFTNet

Purpose

This procedure enables you to delete an output channel from SWIFTNet.

This procedure only deletes the output channel from SWIFTNet, the output channel remains in Alliance Access.

You cannot recreate an output channel on SWIFTNet once it is deleted from SWIFTNet.

Users and permissions

To delete output channels from SWIFTNet, your operating profile must have these actions:

- **SWIFTNet Interface / Open/Print OChan**
- **SWIFTNet Interface / Delete OChan**

Prerequisites

You must remove the emission profiles configured with the selected output channel before you can delete the output channel from SWIFTNet.

Procedure

1. Select the check box of the output channel that you require.

2. Click **Delete from SWIFTNet**.

The **Delete Output Channel from SWIFTNet** window opens.

3. Click **Delete from SWIFTNet**.

The **Delete Output Channel from SWIFTNet** window closes.

The system deletes the output channel from SWIFTNet.

11.8.5 Adopt an Output Channel

Purpose

This procedure enables you to adopt an output channel from another application so that Alliance Access can use it.

Users and permissions

To adopt output channels, your operating profile must have these actions:

- **SWIFTNet Interface / Open/Print OChan**
- **SWIFTNet Interface / Adopt OChan**

Procedure

1. Click **Adopt**.

The **Adopt Output Channel** window opens.

2. Select the BIC8 that you require from the drop-down list in the first part of the **Output Channel** field.
3. Enter the remainder of the output channel name in the second and third parts of the **Output Channel** field, as necessary.
4. Click **Adopt**.

The **Adopt Output Channel** window closes.

A status popup message appears.

The system adopts the output channel and the adopted output channel appears in the list on the **Output Channels** page.

11.8.6 Delete an Output Channel

Purpose

This procedure enables you to remove an output channel from Alliance Access.

This procedure only deletes the output channel from Alliance Access, the output channel remains on SWIFTNet.

Users and permissions

To delete output channels, your operating profile must have these actions:

- **SWIFTNet Interface / Open/Print OChan**
- **SWIFTNet Interface / Remove OChan**

Procedure

1. Select the check box of the output channel that you require.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

The system deletes the output channel.

A status popup message appears.

The output channel disappears from the list on the **Output Channels** page.

11.9 Advanced Real-Time File Handler

11.9.1 Advanced Real-Time File Handler

Overview

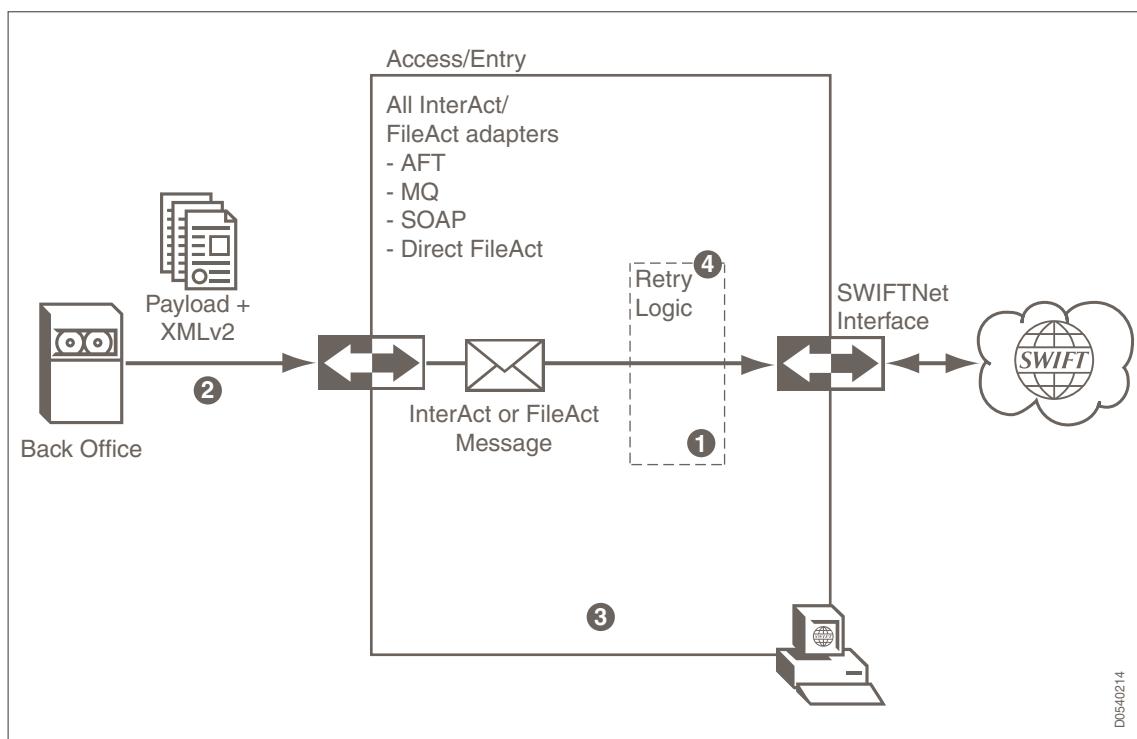
The Advanced Real-Time File Handler enhances Alliance Access retry logic to deal with the unavailability of correspondents to receive real-time emission flows.

This logic is based on an emission expiry date and time attribute that is set for each real-time InterAct or FileAct message to send, along with enhanced emission logic to retry with variable intervals when a real-time correspondent is not available. The emission will be rejected only when the emission expiry date and time is reached.

The emission expiry date and time can either be set explicitly by the back office when providing the message (by means of an XMLv2 parameter), statically defined in each message partner, or set to a default value if not specified by either the back office or a message partner.

The Advanced Real-Time File Handler also introduces an on-hold state for correspondents, which prevents any emission attempts for the affected real-time service. Correspondents can be put on hold automatically by Alliance Access following emission failures, or this can be performed manually by an operator.

The Advanced Real-Time File Handler also improves the monitoring of real-time flows for external systems, indicating the correspondents that are on hold and the current status of each emission flow, including the emission retries.



1	Re-design of retry logic and correspondent state
2	Emission expiry date and time <ul style="list-style-type: none"> • In XMLv2 • Statically configured in message partner

	<ul style="list-style-type: none"> • System-wide default value
3	<p>Reporting and monitoring functions</p> <ul style="list-style-type: none"> • File status • Correspondent status
4	<p>Manual actions</p> <ul style="list-style-type: none"> • Change correspondent status (put on hold, release, and force status) • Cancel emission

Emission expiry date and time

The emission expiry date and time of a message is the date and time after which Alliance Access no longer attempts to send an InterAct or File message, should the emission repeatedly fail until that date and time, and rejects the message as expired. You can assign an emission expiry date and time to messages by either:

- setting an emission expiry date and time directly in each message you submit to Alliance Access from a back-office application through a message partner whose connection is based on XMLv2. In this case, the emission expiry date and time applies only to that specific message.
- defining an emission expiry time interval in the message partner. In this case, the emission expiry date and time of each message received from a back-office application via the message partner is calculated by adding the message partner expiry time interval to the message creation date and time. This is possible with all message partners, regardless of their connection method.

When both are present, the value set at the message level takes precedence over the value set at the message partner level.

If you do not define an expiry date and time as described above, a default expiry date and time will be assigned to all InterAct and FileAct messages. You can modify the default by means of the **Default emission expiry** global configuration parameter.

Alliance Access constantly checks for expired messages in the `_SI_To_SWIFTNet` queue and immediately rejects them locally. You continue to get a single notification message indicating the final success or failure of the emission.

If a real-time InterAct or FileAct message expires while being transmitted, the transmission continues normally and the message is not rejected locally.

Note If you have the **Message File, Change expiry d/t** permission, you can use Message Management to change the emission expiry date/time. For more information, see changing the emission expiry date and time in the [Message Management Guide](#).

Automatically holding and releasing correspondents for a real-time service

When Alliance Access experiences emission failures when sending messages to a correspondent over a real-time service (for a period defined by the **Corr. on hold criteria** global configuration parameter - the default value is 10 minutes), Alliance Access automatically puts that correspondent on hold for that real-time service for 30 minutes. During this time, Alliance Access does not try to send any message to that combination. After the hold period, Alliance Access restarts sending messages to that correspondent.

Note that correspondents are identified by their institution-level distinguished name (DN) and that holding or releasing a correspondent applies to that correspondent and all of its descendants.

-
- Note** A correspondent (and its descendants) on hold for a real-time service can exceptionally be released when all of the following are true:
- when its release date and time have not been reached
 - the value of the **Last modified by** field for the correspondent is set to SYSTEM
 - an acknowledgement for a message that was sent for that correspondent (or any of its descendants)/real-time service combination before it was put on hold was received after the combination was put on hold.
-

Manually holding and releasing correspondents for a real-time service

You can also put a correspondent on hold for a real-time service by means of either the `saa_manager` command-line tool or the **Correspondent/Real-Time Service on Hold** GUI, which is available with the Web Platform-based Configuration package. As a result, Alliance Access stops sending messages to that correspondent /real-time service combination. You can specify the date and time when the combination can be released and when Alliance Access can restart sending messages to it. If you add a correspondent/real-time service combination without specifying a release date/time, that combination will be put on hold forever until it is manually released.

Using the same tool or GUI, you can also release a correspondent for a real-time service with immediate effect.

Alliance Access emission retry logic

Alliance Access uses advanced real-time emission logic for InterAct and FileAct messages. This advanced logic:

- is based on calculating a next emission date and time for each message upon each emission attempt failure, date and time before which Alliance Access does not try to send the message. The calculation of the next emission date and time of a message takes into account the message emission expiry date and time as well as the number of failed emission attempts (if any) having occurred so far, and is designed to ensure that messages are sent as soon as possible (without retrying too frequently, but before their emission expiry date and time). Alliance Access retries sending a real-time message at the following intervals: two minutes, five minutes, 10 minutes, then 20 minutes, until the message expires.
- prioritises message emission based on message priority (urgent messages first), message expiry date and time (messages with earlier emission expiry date and time first), and first-in first-out (FIFO) order

Cancellation of message instance emissions

You can cancel message instance emission from the Message Management, Message/Instance Search application. This applies to all message instances (that is, FIN, InterAct, and FileAct messages) that are sitting in an emission queue and whose transfer is not on-going. This also applies to File message instances whose transfer is on-going.

Message emission monitoring

Alliance Access logs sufficient information in the Event Journal to enable you to monitor the various stages of its attempts to send messages. Message expiry is logged as a separate event.

You can view the emission expiry date and time and the next emission date and time of all messages in the Message Management, Message Search application.

You can view any on-going file transfer for a particular File message in the Message Details view of the Message Management, Message Search application.

Related information

"Message Partner Details Window: Configuration Tab" on page 305

"Correspondent/Real-Time Service on Hold" on page 420

"Emission" on page 117

"Message" on page 118

"Add an Emission Profile" on page 386

"Changes in Revision 2.0.4" on page 690

[Message Management Guide](#)

11.10 Correspondent/Real-Time Service on Hold

11.10.1 Correspondent/Real-Time Service on Hold

Definition

This page lists all of the correspondent/real-time service combinations that are on hold and for which, as a result, Alliance Access does not attempt to send InterAct or FileAct messages. When a correspondent/real-time service is on hold, the correspondent and all of its descendants are on hold for that real-time service.

With the Correspondent/Real-Time Service on Hold GUI, you can:

- implement in Alliance Access the automatic hold and release of a combination of a correspondent and real-time service. A correspondent is a Responder DN level 2 (that is, a BIC8) and its descendants.
- put a correspondent/real-time service combination on hold (with or without a release date and time) or update the release date and time
- immediately release the combination of a correspondent (and its descendants) and a real-time service
- stop systematically rejecting messages for a correspondent/real-time service combination that is on hold

Automatically holding correspondents

When an emission attempt to a specific InterAct/FileAct correspondent/real-time service combination fails, Alliance Access marks that combination as on hold for 30 minutes if all previous emission attempts to that combination have failed for a technical reason (that is, a reason other than being aborted or rejected manually) during a period at least equal to the period defined in the `Corr. on hold criteria` global system configuration parameter. If this global system configuration parameter is set to 0, then Alliance Access never puts the correspondent/real-time service combinations on hold automatically. Alliance Access assigns the SYSTEM operator to that operation, to distinguish between when Alliance Access automatically puts a correspondent/real-time service combination on hold and when this is the result of customer action (by means of the command-line tool or GUI).

During the time when the correspondent/real-time is on hold, there is no attempt to send messages to that correspondent/real-time service combination. However, the fact that a correspondent/real-time service combination is on hold never causes the messages involved to be systematically rejected locally.

Note Detection of correspondents on hold occurs at the level of individual emission profiles. However, the correspondent/real-time service combination is considered as on hold by all real-time emission profiles.

11.10.2 Correspondent/Real-Time Service on Hold Page

Content

The **Correspondent/Real-Time Service on Hold** page contains these elements:

- Details of the correspondent/real-time service combination
See "Details" on page 421
 - Functions that enable you to manage the correspondents
See "Functions" on page 422

Display

Correspondent/Real-Time Service on Hold				
Filtering Criteria				
DN	Service Name			
<input type="button" value="Clear"/>	<input type="button" value="Submit"/>	<input type="button" value="Report"/>		
Correspondent/Real-Time Service on Hold				
Change View	Add	Refresh	Release	Report
<input type="checkbox"/>	DN	Service Name	Release Date and Time	Last Modified Date and Time
<input type="checkbox"/>	o=saabebbe, o=swift	test	2013/04/20 00:00:00	2013/04/02 13:32:48
<input type="checkbox"/>	o=saabebbe, o=swift	test	2013/04/19 00:00:00	2013/04/02 13:33:37
<input type="checkbox"/>	o=saabebbe, o=swift	abcd1234	2013/04/20 00:00:00	2013/04/11 13:55:44
<input type="checkbox"/>	o=sagbeb, o=swift	abcd1234	2013/04/12 00:00:00	2013/04/08 15:08:06
Rows in list: 4 , in selection: 0				
◀ Previous Next ▶				

Details

Column	Description
Responder DN	The correspondent, which is a Responder DN level 2 (BIC8) and its descendants
Service name	The real-time service name for which the correspondent (and its descendants) is on hold
Release date and time	The date and time at which the correspondent (and descendants)/real-time service combination will be released (and removed from the table)
Last modified by	The name of the operator who last modified the correspondent/real-time service combination record. If Alliance Access has put the combination on hold, the name of the operator is SYSTEM.

Last modified date and time	The date and time when the combination was last modified
Creation date and time	The date and time at which the record was created in the table
Creating operator	The name of the operator who created the record
Comment	A free-text comment with a maximum of 255 characters

Functions

Function	Description
<input type="button" value="Add/Add-as"/>	Enables you to put a correspondent identified by its DN level 2 (and its descendants) on hold for a specific real-time service Procedure: "Put a Correspondent on Hold" on page 423
<input type="button" value="Refresh"/>	Enables you to update the list with the latest information available
<input type="button" value="Release"/>	Enables you to immediately release one or more correspondent (and descendants)/real-time service combinations that are on hold. Once released, a selected combination is removed from the list Procedure: "Release a Correspondent That Is on Hold" on page 423
<input type="button" value="Report"/>	Enables you to create a report of the correspondent/real-time services currently on hold Procedure: "Generate a Report of Correspondents" on page 424

11.10.3 View or Update the Correspondent/Real-Time Service on Hold List

Purpose

This procedure enables you to view the list of correspondent/real-time service combinations that are on hold. You can view the name of the operator who created or last modified it (in the case the Alliance Access put the correspondent on hold, the name is SYSTEM), the last modification date and time, the release date and time (optional), and the comment (optional).

You can also update the release date and time and the comment of a correspondent (and its descendants)/real-time service combination that is on hold.

To refresh the list with the latest information available, click .

Users and Permissions

To view the list, your operating profile must have this permission:

- **SWIFTNet Interface**

Procedure

1. To view the details of a correspondent (and its descendants)/real-time service combination, select a combination in the list. A pop-up is displayed that contains the details of that combination.
2. To update the release date and time and/or the comment of a correspondent (and its descendants)/real-time service combination, select a combination in the list, make your updates in the details pop-up, then click **Save**.

11.10.4 Put a Correspondent on Hold

Purpose

This procedure enables you to put correspondent/real-time service combinations on hold. You can optionally specify a release date and time and comment. If no release date and time is specified, then the correspondent (and its descendants)/ real-time service combination is considered to be placed permanently on hold.

Users and Permissions

To put a correspondent on hold, your operating profile must have this permission:

- **SWIFTNet Interface**

Procedure

1. In the **Filtering Criteria** window, specify a **Responder DN** and **Service name**, then click **Submit**.
2. Select a combination from the list, then click **Add/Add as**. In the pop-up that is displayed, you can optionally specify a release date and time and comment.
3. Click **Save**.

11.10.5 Release a Correspondent That Is on Hold

Purpose

This procedure enables you to immediately release a correspondent/real-time service combination that is on hold. When released, the selected combination or combinations are removed from the list.

Users and Permissions

To release a correspondent that is on hold, your operating profile must have this permission:

- **SWIFTNet Interface**

Procedure

1. Select a combination from the list of combinations on hold.
2. Click **Release**. The combination is removed from the list of combinations that are on hold.
3. Click **Close** to remove the confirmation pop-up.

11.10.6 Generate a Report of Correspondents

Purpose

This procedure enables you to generate a report of the correspondent/real-time service combinations that are on hold.

Users and Permissions

To generate a report of correspondents that are on hold, your operating profile must have this permission:

- **SWIFTNet Interface**

Procedure

1. Click **Report**.
2. A report is displayed that contains details of all of the combinations on hold.

12 CRnet Interface

The CRnet Interface

Alliance Access interfaces with the Communications Router Network service through the CRnet Interface application. CRnet has two purposes:

- To configure Alliance Access so that it provides a secure exchange of data with customer applications using CRFI or CRPI

CRFI is used in data exchange between CREST and Alliance.

CRPI is a real-time communications application, used in file transfer between a Customer Host system and Alliance.

- To manage communications (files and interactive messages) between Alliance Access and a Customer Host system.

12.1 Dashboard

Description

The dashboard enables you to start and stop the CRnet component, manage your sessions, and display the event log.

Secure Sessions				Rows in list: 2, in selection: 0
Change View	Open Session	Close Session	Type	Status
<input type="checkbox"/>	CREST		File Transfer	Open
<input type="checkbox"/>	CREST		Interactive	Open

- "Starting the CRnet Component"
- "Stopping the CRnet Component"
- "Secure Sessions"
- "CRnet Log Entries"

12.1.1 Starting the CRnet Component

Procedure

1. From the **CRnet Interface Dashboard** page, click **Start CRnet**.
2. In the **Confirm Start** dialog box, click **OK**.

A progress bar is displayed during the start process.

12.1.2 Stopping the CRnet Component

Procedure

1. From the **CRnet Interface Dashboard** page, click **Stop CRnet**.
2. In the **Confirm Stop** dialog box, click **OK**.

Progress is displayed in the status pane.

12.1.3 Secure Sessions

12.1.3.1 Opening a Secure Session

1. Select a session from the **Secure Sessions** pane.

Tip You can change the width of the columns displayed by dragging the column boundary left or right as required. Click **Save Column widths** to keep the settings for the next time you log on.

2. Click the **Open Session** tab.

Secure Sessions				Rows in list: 2, in selection: 1
	Name	Type	Status	
<input type="checkbox"/>	CREST	File Transfer	Open	
<input checked="" type="checkbox"/>	CREST	Interactive	Closed	

12.1.3.2 Closing a Secure Session

1. Select a session from the **Secure Sessions** pane.

Tip You can change the width of the columns displayed by dragging the column boundary left or right as required. Click **Save Column widths** to keep the settings for the next time you log on.

2. Click the **Close Session** tab.

Secure Sessions				Rows in list: 2, in selection: 1
	Name	Type	Status	
<input checked="" type="checkbox"/>	CREST	File Transfer	Open	
<input type="checkbox"/>	CREST	Interactive	Closed	

Note Secure sessions are automatically stopped when the servers of Alliance Access are shut down.

12.1.3.3 Viewing Details of a Secure Session

1. Select a session from the **Secure Sessions** pane.
2. Click the **Detail** tab.

Note The **Detail** tab is only available when the CRNet component is started.

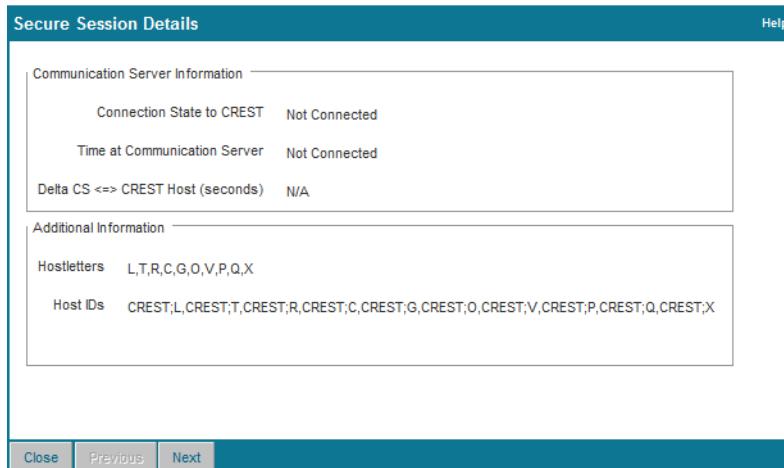
The **Secure Session Details** window appears showing information about the selected session. For more information, see "Secure Sessions Details Page" on page 427.

12.1.3.4 Secure Sessions Details Page

Content

The **Secure Session Details** page provides access to the session information.

Display



Details

Column	Description
Connection State to CREST	Connected: A secure session is open to the communication server. Not Connected: There is not a secure session open to the communication server.
Time at Communication Server	Value in hh:mm:ss: A secure session is open to the communication server. Not Applicable: There is not a secure session open to the communication server.
Delta CS <=> [host]	Time difference in seconds: This value represents the time difference between the host and the communication server. Not Applicable: There is not a secure session open to the communication server.
Hostletters	Alpha characters: These letters are used in the file for a File Transfer session. They represent the modes in which files can be sent (for example, L = Live).
Host IDs	[service name];[letter]: These letters are the host IDs to be used for an interactive session, separated by a comma if there are multiple values.

Functions

Function	Description
Close	Close the page.
Next	Displays details of the next session.
Previous	Displays details of the previous session.

12.1.4 CRnet Log Entries

Description

This pane displays a record of all log entries relating to the CRnet component. This includes error messages, if an error occurs during starting or stopping the CRnet component or establishing connections.



12.2 Configuration

12.2.1 Communication

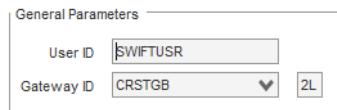
12.2.1.1 Configuring the Host Services

Prerequisite

The CRnet component must be stopped before changing the CRnet configuration options.

Procedure

1. The host services are configured using the **General Parameters** pane on the **Communications** page.



2. If adding or modifying the parameters, the following details are required:

Field	Action
User ID	The CREST User ID provided by Euroclear EUI.

Field	Action
Gateway ID	Select an identifier for the gateway from the drop-down list. Every gateway that SWIFT issues has a unique, customer-specific, eight-character BIC identifier which is derived from the Alliance Access licence.

3. When finished, Click **Save**.

12.2.1.2 Gateway Connections

Procedure

1. The gateway connections are configured from the **Communications** page.

Gateway Connection Details

Sequence	1
Connection Name	besd055
Authoriser DN	cn=auth5 ,o=crstgb2l,o=swift
Requestor DN	ou=beax041,ou=crest ,o=crstgb2l,o=swift

Close

Note The CRnet component must be stopped before changing the CRnet configuration options.

2. From this page you can:
- Click **Add** to add a new or secondary connection
 - Delete a connection by selecting the connection and clicking **Delete**
 - Change the order of the gateways, by selecting one and clicking **Move Up** or **Move Down**.
 - Modify an existing connection by clicking on it.
3. If adding or modifying a connection, the following details are required:

Field	Action
Connection Name	Select the connection that identifies the Alliance Gateway (SAG) that is to be used.
Authoriser DN	Type the distinguished name that is associated with a signing certificate on the selected SAG.
Requestor DN	Type the distinguished name that is the customer address that SWIFTNet recognises as "sender". Users receive the customer address during SWIFTNet provisioning.

Gateway Connection Details

Sequence	1
Connection Name	besd055
Authoriser DN	cn=auth5 ,o=crstgb2l,o=swift
Requestor DN	ou=beax041,ou=crest ,o=crstgb2l,o=swift

Close

- Once the details have been entered, click **Save**, and then **Close**.

12.2.1.3 Workstation Listeners

Definition

A Workstation listener is a server process that runs on Alliance Access and listens for the connection requests from a Workstation client (a client process that runs on a remote system).

The Network Service Layer (NSL) and CRPI use Workstation listeners to connect to Alliance Access.

You can configure multiple Workstation listeners, for clients inside or outside any firewalls.

Prerequisite

The CRnet component must be stopped before changing the CRnet configuration options.

To add or edit a Workstation listener

- The host services are configured using the **Workstation Listeners** pane on the **Communications** page.

CRNet Interface - Communication Configuration

Workstation Listeners

	IP Address	Listen Port	Min Port	Max Port	External IP
<input type="checkbox"/>	10.4.164.113	11813	2048	65535	
<input type="checkbox"/>	10.4.164.114	11814	2048	65535	

- In the **Workstation Listeners** area, do one of the following actions:

- Click **Add**, to add a workstation listener.
- Click a workstation listener to edit its details.
- Select a workstation listener and click the **Delete** tab to remove it.

If you are adding or viewing a listener, the **Workstation Listener Information** page appears.

Workstation Listener Details

IP Address	172.24.50.97
Listen Port	11812
Port Range	2048 To 65535
External IP	

Close **Previous** **Next**

3. In the **IP Address** field, type the IP address of the gateway to which the workstations will connect.
The IP address is the IP address of the server to which client requests are sent.
4. In the **Listen Port** field, specify the listener port of the server.
5. In **Port Range** and **To** fields, define the range of ports that are available on the LAN for communicating with the server.
The default port range is between 2048 and 65535. You can change these default values, if necessary. For example, certain ports may be blocked if there are firewalls active on the LAN.
6. If a firewall exists between the workstation client and the gateway performs Network Address Translation, then specify the external IP address in **External IP**.
This is the IP Address used by the client (NSL or CRPI) to communicate with the Workstation listener.
7. Click **Save**, and then **Close**.

12.2.2 Configuring Customer Applications

Overview

This section describes how to configure Alliance Access so that it can exchange CRnet data with local applications using CRFI or CRPI.

Note	You must stop the CRnet component before you configure, add, or remove any customer applications. For more information, see "Stopping the CRnet Component" on page 426 for instructions.
-------------	--

Names of customer applications

For each local application using CRFI or CRPI, you must use the CRnet Interface to define a name for the application. Then, you must specify which operators use the local application. This completes the configuration (assuming that you accept the default values set up by Alliance Access). No further action is required.

Every local application is known to Alliance Access as a message partner. To control the flow of messages through the system, Alliance Access routes messages between different message queues. Messages coming from local message partners are routed to input message queues for further processing.

Output messages for message partners (received from the SWIFT network) are routed to exit points. Each exit point is assigned to a particular message partner. An exit point is essentially a routing queue used to store output messages for that partner.

After you name the application, the CRnet Interface automatically creates the following:

- a "To" message partner and a "From" message partner that are associated with the application. The names of the message partners are based on the local application name that you specified (you can change these names if you want)
- an input message queue for the application (for messages sent from the application to CREST)

- three exit points for the application (for messages to the application from CREST):
 - **CR<F/P><Application name>acks**
 - **CR<F/P>Application name>nacks**
 - **CR<F/P><Application name>responses**
 where **F** represents CRFI and **P** represents CRPI.
- the routing rules that apply to the message queues. Alliance Access uses these rules to determine how to route a message (for example, to another message queue, to the SWIFT network, or to an exit point).

12.2.2.1 Holding and Releasing Queues

Overview

If any problems occur with the transfer of data, then you may need to hold and release the queues of the application. You perform these tasks using the **Hold** and **Release** buttons.

To hold or release a queue:

1. In the **CRnet Interface** menu item, expand **Configuration** then select **CRFI Applications** or **CRPI Applications**.

The **Applications Configuration** pane is displayed.

For example:

CRnet Interface - CRPI Applications Configuration							Rows in list: 2, in selection: 0	
CRPI Applications							◀ Previous	Next ▶
	Change View	Add	Delete	Hold	Release			
<input type="checkbox"/>	Name	Status	Input Queue			From Message Partner	To Message Partner	Operator(s)
<input type="checkbox"/>	CRPIWP	Released	CRICRPIWP			CRPfrCRPIWP	CRPtoCRPIWP	COP9
<input type="checkbox"/>	CRPIWS	Released	CRICRPIWS			CRPfrCRPIWS	CRPtoCRPIWS	COP7

2. To hold a queue, select the application from the list displayed, and then click **Hold**.
The selected application queue is held.
3. To release a queue, select the application from the list displayed, and then click **Release**.
The selected application queue is released.

For more details on holding and releasing queues, see queues and routing in the [System Management Guide](#).

12.2.2.2 CRFI Applications Configuration

12.2.2.1 Configuring CRFI Applications

Procedure to add an application

1. Select CRnet Interface - Configuration - CRFI Applications .

This page shows information about the applications defined for CRFI, such as application name, current status, input and output queues with associated message partners, and operators.

2. Click **Add**.

The **Add Application** window appears:

Click **Help** to display the online help for the **Details** page.

3. Type an application name, then click **Next** .

The **CRFI Application Details** window appears:

4. Assign an operator to the defined application. Locate the list **Available**. This list contains all operators that are available.

5. Double-click an operator to transfer it to the **Selected** list (or use the arrows).
6. Alliance Access has automatically created input and output message partners, based on the application name. Now you must configure the defined message partners.
7. In the **CRFI From Message Partner Name** tab, the properties that Alliance Access created for the input message partner are displayed.
For a description of the fields displayed in this window, see "Details Page" on page 435.
8. In the **CRFI To Message Partner Name** tab the properties that Alliance Access created for the output message partner are displayed.
9. After entering all the required information, click **Save**.

Procedure to modify an application

1. Select the application to be modified.
2. Make any changes to the defined information for the application.
3. After finishing your changes, click **Save**.

Alliance Access automatically updates the application configuration.

Procedure to remove an application

1. Select the required application.
2. Click **Delete**.

Related information

For more information about using CRFI applications, see the *Customer Application Integration Guide for CREST* for [Windows](#) or [UNIX](#).

12.2.2.2 Add Page

Content

The **Add CRFI Application** enables you create the name for the CRFI application, and provide configuration details.

Display

Details

Field	Description
CRFI Application Name	The name of the application you are adding. The name must be unique.

Functions

Function	Description
<input type="button" value="Help"/>	Display the application details required.
<input type="button" value="Cancel"/>	Exit without adding the application.
<input type="button" value="Next"/>	Continue to the Details page.

12.2.2.3 Details Page

Content

The **CRFI Application Details** page provides enables you to configure or modify the CRFI application details.

Display

Details

Field	Description
CRFI Application Name	The name of the application.
Assigned Operators	Shows the list of operators available and the operators selected.

Functions

Function	Description
<input type="button" value="Close"/>	Closes the page.
<input type="button" value="Help"/>	Displays the online help.
<input type="button" value="Next"/>	Displays the next page.
<input type="button" value="Previous"/>	Displays the previous page.

General Tab

Here you can select the operators that will use the application.

CRFI Application Details

General CRFI From Message Partner CRFI To Message Partner

CRFI Application Name: FDSDSF

Assigned Operators

Operator List Available Selected

COP1 COP10 COP3
COP6 COP7 COP8

Close Previous Next

Details

Field	Description
CRFI Application Name	The name of the application.
Assigned Operators	Shows the list of operators available and the operators selected.

CRFI From Message Partner Tab

Here you can specify the details for incoming messages.

CRFI Application Details

General CRFI From Message Partner CRFI To Message Partner

Configuration for CRFI From Message Partner: CRFfrCRFIWP

Top Directory: /beax041_i1/access/CRF/CRFIWP/INP/

Backup Directory: /beax041_i1/access/CRF/CRFIWP/INP_BCK/

Post-Processing Script: /beax041_i1/access/CRF/CRFIWP/INP/

Delete sent files from Top Directory:

Clean up file system:

File retention in file system (days): 5

Idle time (seconds): 12

CRnet File Format: Standard

CRnet Input Queue: CRICRFIWP

Close Previous Next

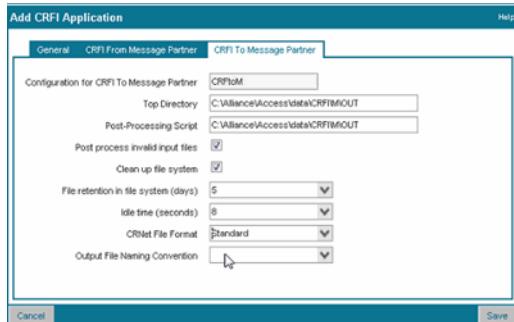
Details

Field	Description
Top Directory	The path of the directory where the input files are stored.
Backup Directory	The path of the backup directory where the input files are stored.
Post-Processing Script	The path of the location of the post-processing script, to execute after a file has been sent. The script receives two parameters: the path name of the Top Directory and the file name of the file that has been sent.

Field	Description
Delete sent files from Top Directory ?	Indicates whether files are deleted after being sent. Click <input type="checkbox"/> Yes or <input type="checkbox"/> No.
Clean up file system ?	Indicates whether the file system is cleaned. Click <input type="checkbox"/> Yes or <input type="checkbox"/> No.
File retention in file system (days)	Displays the number of days (1-60) that the files are kept in the system before being deleted. Valid if Clean up file system ? is set to Yes
Idle Time (seconds)	Displays the time, in seconds (1-60), that the system waits to check whether any files are present in the input queue.
CRnet File Format	Displays the format of the CRnet files. Click <input type="checkbox"/> Standard or <input type="checkbox"/> Extended.
CRnet Input Queue	Displays the input queue for CRnet files, based on the application name, used to send files from the communication server to Alliance Access. The maximum number of files in the input queue is 5,000. Once this figure is reached, the CRFI does not function. The files stay in the input queue and no warning or error is generated.

CRFI To Message Partner Tab

Here you can specify the details for outgoing messages.



Details

Field	Description
Top Directory	The path of the directory where the output files are stored.
Post-Processing Script	The path of the location of the post-processing script, to execute after a file has been sent. The script receives two parameters: the path name of the Top Directory and the file name of the file that has been sent.
Post-process invalid input files?	When an input file fails validation, a status file is placed in the output directory. A user can specify whether to run a post-processing script in addition to this action. If you select Yes, then the output post-processing script is run when an input file fails validation.
Clean up file system ?	Indicates whether the file system is cleaned. Click <input type="checkbox"/> Yes or <input type="checkbox"/> No.

Field	Description
File retention in file system (days)	Displays the number of days that the files are kept in the system before being deleted. Valid if Clean up file system ? is set to Yes .
Idle Time (seconds)	Displays the time, in seconds, that the system waits to check whether any files are present in the output queue.
CRnet File Format	Displays the format of the CRnet files. Click Standard or Extended . Click Standard or Extended .
Output File Naming Convention	Determines the naming scheme for unique file names. Click Time Stamp or Sequence Number .

12.2.2.3 CRPI Applications Configuration

12.2.2.3.1 Configuring CRPI Applications

Procedure to add an application

1. Select **CRnet Interface - Configuration - CRPI Applications**.

CRnet Interface - CRPI Applications Configuration

CRPI Applications						Rows in list: 2, in selection: 0	
	Change View	Add	Delete	Hold	Release	◀ Previous	Next ▶
	Name	Status	Input Queue	From Message Partner	To Message Partner	Operator(s)	
<input type="checkbox"/>	CRPIWP	Released	CRICRPIWP	CRPfrCRPIWP	CRPtoCRPIWP	COP9	
<input type="checkbox"/>	CRPIWS	Released	CRICRPIWS	CRPfrCRPIWS	CRPtoCRPIWS	COP7	

This page shows information about the applications defined for CRPI, such as application name, current status, input and output queues with associated message partners.

2. Click **Add** to add a new application. The **Add Application** page appears. Click **Help** to display the online help for the **Details** page.
3. Type an application name, then click **Next** to proceed. The **CRPI Application** page appears.
4. Enter the names of the Message Partners to be used.
5. Now you must assign an operator (or operators) to the application.
6. Double-click an operator to transfer it from the **Available** column to the **Selected** column (or use the arrows).
7. After entering all the required information, click **Save**.

Tip	For more information about using CRPI applications, see the <i>Customer Application Integration Guide for CREST</i> for Windows or UNIX .
------------	---

Procedure to modify an application

1. Select on the application to be modified.
2. Make any changes to the defined information for the application.
3. After finishing your changes, click . Alliance Access automatically updates the application configuration.

Procedure to remove an application

1. Select the required application.
2. Click .

12.2.2.3.2 Add Page

Content

The **Add CRPI Application** page provides enables you to configure the CRPI application details.

Display

Details

Field	Description
CRPI Application Name	The name of the application you are adding. The name must be unique.

Functions

Function	Description
<input type="button" value="Help"/>	Display the application details required.
<input type="button" value="Cancel"/>	Exit without adding or deleting the application.
<input type="button" value="Next"/>	Continue to the Details page.

12.2.2.3.3 Details Page

Content

The **CRPI Application Details** page provides enables you to configure or modify the CRPI application details.

Display

CRPI Application Details

CRPI Application Name: CRPIWP

CRPI From Message Partner Name: CRPfrCRPIWP

CRPI To Message Partner Name: CRPtoCRPIWP

Assigned Operators

Operator List	Available	Selected
COP1 COP10 COP2 COP3 COP4 COP5		COP9
<input type="button" value=">>"/> <input type="button" value=">"/> <input type="button" value="<"/> <input type="button" value="<<"/>		

Details

Field	Description
CRPI Application Name	Name of the application you are adding, modifying, or viewing.
CRPI From Message Partner Name	The name of the message partner is generated automatically when CRPI is added. You cannot change this value.
CRPI To Message Partner Name	The name of the message partner is generated automatically when CRPI is added. You cannot change this value.
Assigned Operators	<p>Available: operators that can be selected Selected: operators that are selected</p> <p>Only operator names of eight characters or less appear, and only those operators not already used in other CRnet applications. Operators are defined in the Security Definition application of Alliance Access.</p>

Functions

Function	Description
<input type="button" value="Close"/>	Closes the page.
<input type="button" value="Help"/>	Displays the online help.
<input type="button" value="Next"/>	Displays the next page.
<input type="button" value="Previous"/>	Displays the previous page.

13 Routing

13.1 Overview of Routing in Alliance Access

Routing functions

Alliance Access provides customers with extensive message-routing functions, supporting MT, MX, and FileAct messages.

Alliance Access can route several instances of the same message independently. For example, Alliance Access can send one instance to the back office and a copy instance to the printer.

Message queues

Alliance Access stores messages internally in queues. Each message queue has a set of routing rules that determines the flow of messages from one queue to the next queue for processing.

For example, during message preparation, Alliance Access holds messages in queues according to the message status.

At all stages of processing, Alliance Access can change the status of a message, return the message changes to the sender, and copy messages.

An operator with appropriate permission can control a queue by holding or releasing it, which stops and starts the flow of messages.

An administrator can also set thresholds on the queues, to generate warnings when the number of messages in a queue reaches a specified level. Also, if a message is older than the maximum message age limit that is set, then the queue is put in an exceptional state and an event (by default configured as an alarm) is logged.

Routing points

Alliance Access routes messages through a series of routing points.

Routing points consist of these elements:

- a queue where messages are stored
- a message processing function
- a set of routing rules

Each routing point has a queue of messages that are processed by a specific message processing function. A message processing functions fetches, processes, and routes the queued messages at a routing point, to achieve a specific set of results. For example, a message processing function could route a message to another routing point where it would appear in a list of message pending investigation by an operator.

Alliance Access does not impose a fixed flow or any rigid routing requirements at these routing points. However, there is a minimal set of internal routing rules to protect the integrity and behaviour of Alliance Access. A routing rule defines the way in which message instances are transformed and moved between routing points.

Alliance Access assigns routing rules to routing points, and can also associate these rules with routing schema. Each routing point has one default rule and action, which is applied if no other rules are defined or applicable.

On top of the routing rules that you can define, each routing point contains a number of system routing rules which are applied before the user routing rules to ensure the proper behaviour of

the system. These rules are not visible, not modifiable and only specify non-sensitive actions. Default rules only specify sensitive actions. User rules can specify both.

For examples of default routing points, see the Default Printouts on the release media, or on www.swift.com, under Support > [Documentation \(User Handbook\)](#).

Routing rules

Alliance Access uses routing rules to route messages between queues. Alliance Access applies only the routing rules that are defined in the active routing schema. However, several routing schema can include the same routing rule.

Each routing rule is made up of two parts:

- condition: triggers Alliance Access to perform a specific action that is defined in the rule.
- action: the action that Alliance Access performs on the message instance if the trigger conditions are met. The action can be:
 - sensitive
 - non-sensitive

The condition is applied to a set of keywords that Alliance Access extracts from the message. If the keywords in the message match the condition, then the routing rule is triggered.

Tip Alliance Access normalises the value of **Requestor DN** or **Responder DN** before it saves the message in the database. To normalise the DN, Alliance Access removes spaces and converts all uppercase letters to lowercase. Therefore, any condition that uses a Requestor DN or Responder DN must use the normalised value of a DN.

Alliance Access uses the Message Syntax Table for MT messages and the Deployment Packages for MX messages to extract keywords from the messages. For a list of the message keywords that are defined by default, see "List of Message Keywords" on page 517. Customers can also define additional routing keywords for extraction of specific fields (full or partial) of a given message. The values of these fields are used as message search criteria and for routing purposes.

An operator with appropriate permissions can define message routing rules. Customers can specify that Alliance Access routes messages to a queue and sends these messages to a correspondent. Alliance Access accesses the Correspondent Information File to find the network that the customer prefers. Customers can define routing rules to ensure that Alliance Access directs messages of a specific formats to the appropriate network.

Routing schema

An routing schema groups a set of routing rules in Alliance Access. Only one schema is active.

To process messages that arrive at a routing point, Alliance Access uses only those routing rules that it has assigned to the active schema.

Alliance Access is delivered with a schema named **A**. This schema is active by default.

Customers can use the pre-defined routing schema, or duplicate the schema and modify it to match specific processing requirements. Duplicating the schema allows an operator with appropriate permissions to modify the schema without affecting the current processing of messages in Alliance Access.

Message processing function

Each routing point has a queue. This queue contains all message instances to be processed by the associated message processing function. A message processing function is the processing entity that transforms or processes an instance in some way. Typically, a message processing function reads a message instance from the queue of the routing point, processes the message instance and submits the message instance for onward routing, together with the function result.

Routing keywords

Keywords are used to simplify the definition of a trigger condition for routing rules and are linked to a particular message syntax table.

13.2 How message routing works

Overview

This section provides an overview of how Alliance Access processes and routes message instances internally.

Processing and routing of message instances

1. Alliance Access reads the rules in the active routing schema.
 2. For a queue at a specific routing point, a message processing function reads a message instance from a queue, and determine which routing rules to apply to the message instance.
- Alliance Access applies the rules in sequential order, from the lowest to the highest. If none of the
3. The condition is applied to a set of keywords that Alliance Access extracts from the message. If the keywords in the message match the condition, then the routing rule is triggered.

The following elements can trigger a routing rule:

- `function result`: based on the associated message processing function processing result
 - `message`: based on conditional statements referring to specific message attributes
 - `message and function result`: based on the combination of message processing function processing result and message attributes
 - `always`: always apply the routing rule
4. If a routing rule is triggered, then Alliance Access performs the action that is defined in the rule.

The following actions are sensitive actions:

- complete the message instance
- move the message instance to another queue
- move the message instance to the addressee

The following actions are non-sensitive actions:

- create new instances (copy or notification) of the message instance and move the new instances to another queue
 - append a new intervention to the message instance, in either free format or in full text)
 - assign a new unit to the message instance or to the newly created message instances
5. If other routing rules are triggered, then Alliance Access also performs the actions that the define. At a minimum, Alliance Access applies the default routing rule.

The default routing rule is only applied if no routing rules are assigned to the queue, or if none of the assigned rules are applicable.

Sequence of routing rules

A number identifies a routing rule. By default, the first routing rule added is given the number 100. Alliance Access applies the rules in sequential order using the routing rule number, from the lowest to the highest.

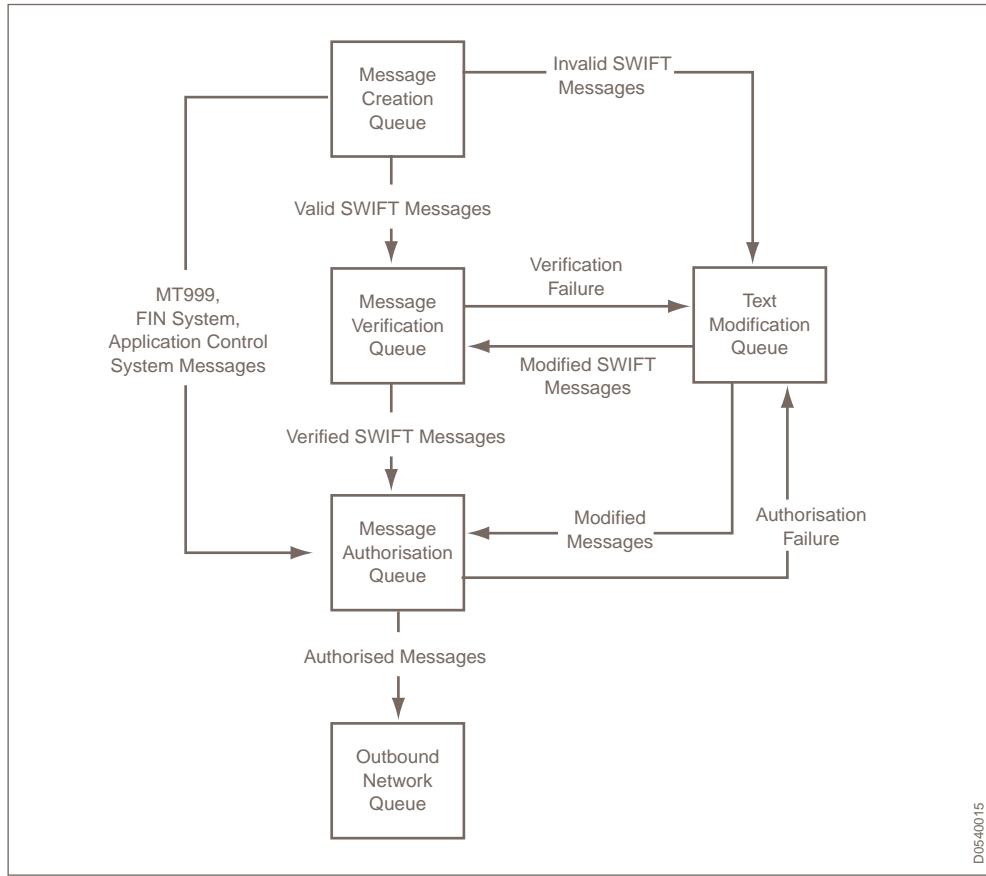
To change the order of the routing rules, an operator must duplicate the routing rules, change the order of the rules by providing each rule with a new sequence number). Then, the operator must delete the original set of rules.

When designing new rules, consider all the processing that must be performed at the selected queue. If an action is performed too early, then it can prevent important processing from occurring later. For example, if the first rule in the sequence is "complete the instance", then none of the other rules in the list are applied.

It is recommended to leave gaps in the sequence numbering of the rules so that other rules can be inserted easily in the correct order at a later date. For example, instead of numbering the rules 101, 102, 103, and so on, number them with gaps of 100, that is 100, 200, 300, and so on.

Example of message routing

Assuming that the default routing rules apply, the figure below shows a simplified version of the normal message flow for SWIFT messages:



Note

The flow of invalid and modified messages to and from the Text Modification queue. In these cases an operator must move the messages to the Text Modification queue. Alliance Access does not route messages as part of the normal message flow.

13.3 Configuration of Routing in Alliance Access

Overview

This section describes how to configure routing in Alliance Access.

Actions required

1. Review the parameters for the **Queue** class of configuration parameters. Verify that the values are applicable for the business, and modify them if required.
For more information, see "Queue" on page 122.
2. Review the parameters for the **Message** class of security parameters that relate to message routing. Verify that the values are applicable for the business, and modify them if required.
For more information, see "Message" on page 130.

3. Navigate to **Routing > Routing Schemas**.

Add a routing schema, or clone an existing routing schema. For more information, see:

- "Add a Routing Schema" on page 538
- "Clone a Routing Schema" on page 538

4. Navigate to **Routing > Routing Keywords**.

For more information see:

- a. "Add a Routing Keyword" on page 533
- b. "Add a Message Mapping" on page 534

If user-defined keywords are required, set up the keywords and link them to a particular message syntax table.

5. Navigate to **Routing > Queues**.

Set up routing rules, define conditional statements, and assign the rules to the routing schema.

For more information see:

- a. "Add a Queue" on page 502
- b. "Define Routing Rules" on page 503
- c. "Specify an Order of Activation and Assign Routing Rules to a Schema (Description Tab)" on page 504
- d. "Define Trigger Conditions (Condition Tab)" on page 504
- e. "Define Routing Actions (Action Tab)" on page 508

Note

Place the routing rules in the order in which Alliance Access must apply them. The order of the rules has an impact on the results of the message processing.

6. Navigate to **Routing > Routing Schemas**.

Approve the routing schema, and then activate it.

For more information, see "Approve and Activate a Routing Schema" on page 539.

13.4 Queues

13.4.1 Message Queues

Types of queues

Alliance Access stores messages internally in the following types of queues:

- exit points
- system
- IPLA, if the Integration Platform licence option is installed
- user-defined

If the Alliance Developer Kit (ADK) component is installed, then additional queues are available for the ADK.

Exit point queues

An exit point is a special routing point that Alliance Access uses to route message instances through the Application interface to message partners. An exit point must be assigned to every message partner profile that defines how to send messages to that message partner.

An exit point is controlled by a message processing function, which performs a specific action on every message in the queue. Alliance Access includes default exit point queues that Alliance Access uses to process all kinds of messages. For more information about the default exit points, see "List of Exit Queues" on page 448.

An operator can define additional exit points for specific routing purposes, depending on operator profile entitlements.

System queues

System queues are defined at installation time and determine the flow of messages with Alliance Access. Users cannot remove system queues.

In general, system queues are processed by their own private Message Processing Functions but, when the processing requirements of system queues are closely related, the same Message Processing Function can be assigned to several queues.

For more information about the system queues, see "List of System Queues" on page 454.

IPLA queues

IPLA queues are queues that are created for Integration Platform (IPLA) components by means of the `ipla_admin -install` command-line tool.

This type of queue can be removed only by means of the `ipla_admin -remove` command-line tool. In order to remove an IPLA queue, you must specify the type of object (that is, queue) and the name of the specific queue to be removed. For more information on this command, see the *Integration Platform Developer Guide*.

User-defined queues

User-defined queues are used solely for the purpose of routing messages based on their content. A user-defined queue can route messages only from one user-defined queue to another user-defined queue.

Note The `_OI_to_OTHER` queue has the characteristics of a user-defined queue.

After an operator creates a user-defined queue, the operator must also define the routing rules that route messages to that queue. Therefore, the operator must add the user-defined queue as target of the `Dispose to` action in the appropriate routing rules.

The routing rules can be created in the same way as for any other queue. User-defined queues are displayed in the list of valid routing targets. There is no message processing function for a user-defined queue. Therefore, a condition for a routing rule cannot be based on a function result.

Note When a new routing rule is added to a user-defined queue, the **Condition On** field (within the **Condition** tab) defaults to Always. However, if the **Function** option is selected, then the **Function Result Available** and **Selected** boxes are displayed without a routing result.

On top of the routing rules that you can define, each routing point contains a number of system routing rules which are applied before the user routing rules to ensure the proper behaviour of the system. These rules are not visible, not modifiable and only specify non-sensitive actions. Default rules only specify sensitive actions. User rules can specify both.

13.4.1.1 List of Exit Queues

AI_to_APPLI

All exit queues, except **_SI_to_SWIFT**, **_SI_to_SWIFTNet** are processed by a single Message Processing Function, identified as **AI_to_APPLI**. The processing results returned by this MPF are the same for all exit queues and are therefore described only once in this section. The two possible processing results are:

- Success: The message has been delivered successfully to the message partner.
By default, a message producing this processing result is completed.
- Failure: The MPF is unable to reconstruct the message correctly. Such a problem may occur, for example, when the version number of the Message Syntax Table assigned to the LT through which a SWIFT message was received (and accepted because minimum validation was applied) is incorrect.
By default, a message producing this processing result is routed to the follow-up queue (**ToBeInvestigated**).

BatchMXAcks

This is the queue of ACK notifications related to outgoing MX messages created by message partners and entered into Alliance Access through the Application Interface. The AI input session uses the File Transfer connection method.

These notifications are created at the SWIFTNet outbound routing point and routed to this exit queue when the message is ACK'd. The reception of a positive acknowledgement causes the MPF associated with the SWIFT outbound queue (**_SI_to_SWIFTNet**) to return a processing result equal to "Success".

BatchMXRejects

This is the queue of NAK notifications related to outgoing MX messages created by message partners and entered into Alliance Access through the Application Interface. The AI input session uses the File Transfer connection method.

These notifications are created at the SWIFT outbound routing point and routed to this exit queue when the message is NAK'd. The reception of a negative acknowledgement causes the MPF associated with the SWIFT outbound queue (**_SI_to_SWIFTNet**) to return a processing result equal to "Failure".

BatchSwiftAcks (Batch Ack Queue)

This is the queue of SWIFT ACK notifications related to outgoing messages created by message partners and entered into Alliance Access through the Application Interface. The AI input session uses the File Transfer connection method, for example, batch transfer of messages using a DOS, UNIX, or Linux file.

These notifications are created at the SWIFT outbound routing point and routed to this exit queue when the message is ACK'd by APC/FIN. The reception of a positive acknowledgement causes the MPF associated with the SWIFT outbound queue (**_SI_to_SWIFT**) to return a processing result equal to "Success".

BatchSwiftNaks (Batch Nack Queue)

This is the queue of SWIFT NAK notifications related to outgoing messages created by message partners and entered into Alliance Access through the Application Interface. The AI input session uses the File Transfer connection method, for example, batch transfer of messages using a DOS, UNIX, or Linux file.

These notifications are created at the SWIFT outbound routing point and routed to this exit queue when the message is NAK'd by APC or FIN. The reception of a negative acknowledgement causes the MPF associated with the SWIFT outbound queue (_SI_to_SWIFT) to return a processing result equal to "NAK'd".

DeliveryNotifAcks

The following traffic reconciliation notification instances are routed from the _TR_NOTIF routing point to this queue:

- DeliveryNotifAcks. MT 011 notifications.

The MPF at this routing point is **AI_to_APPLI**.

From this exit point, you can send delivery notification instances to a message partner with Connection Method Print or to a message partner with Data Format CAS2, MQ-MT or XML version 2.

For more information about the configuration parameter that affects this queue, see "Traffic Recon " on page 124.

Note As of Alliance Access release 7.1.10, the Responder DN field is included in the delivery notification, allowing you to route a delivery notification instance based on the Responder DN.

DeliveryNotifNaks

The following traffic reconciliation notification instances are routed from the _TR_NOTIF routing point to this queue:

- DeliveryNotifNaks. MT 010, MT 015, and MT 019 notifications.

The MPF at this routing point is **AI_to_APPLI**.

From this exit point, you can send delivery notification instances to a message partner with Connection Method Print or to a message partner with Data Format CAS2, MQ-MT or XML version 2.

For more information about the configuration parameter that affects this queue, see "Traffic Recon " on page 124.

Note As of Alliance Access release 7.1.10, the Responder DN field is included in the delivery notification, allowing you to route a delivery notification instance based on the Responder DN.

FileActAcks

This is the queue of ACK notifications related to outgoing FileAct messages created by message partners and entered into Alliance Access through the Application Interface. The AI input session uses the File Transfer connection method.

These notifications are created at the SWIFTNet outbound routing point and routed to this exit queue when the message is ACK'd. The reception of a positive acknowledgement causes the

MPF associated with the SWIFT outbound queue (**_SI_to_SWIFTNet**) to return a processing result equal to "Success".

FileActReceived

This is the exit queue to which all incoming FileAct messages received from SWIFTNet are routed with success from the SWIFTNet inbound routing point.

FileActReject

This is the queue of NAK notifications related to outgoing FileAct messages created by message partners and entered into Alliance Access through the Application Interface. The AI input session uses the File Transfer connection method.

These notifications are created at the SWIFT outbound routing point and routed to this exit queue when the message is NAK'd. The reception of a negative acknowledgement causes the MPF associated with the SWIFT outbound queue (**_SI_to_SWIFTNet**) to return a processing result equal to "Failure".

FileDeliveryNotifAck

The following traffic reconciliation notification instances are routed from the **_TR_NOTIF** routing point to this queue:

- FileDeliveryNotifAck. Positive FileAct delivery notifications.

The MPF at this routing point is **AI_to_APPLI**. From this exit point, you can send the delivery notification instances to a message partner with connection method printer or File Transfer XML.

FileDeliveryNotifNak

The following traffic reconciliation notification instances are routed from the **_TR_NOTIF** routing point to this queue:

- FileDeliveryNotifNak. Negative FileAct delivery notifications.

The MPF at this routing point is **AI_to_APPLI**. From this exit point, you can send the delivery notification instances to a message partner with connection method printer or File Transfer XML.

LocalMXAcks

This is the queue of ACK notifications related to outgoing MX messages generated by Alliance Access or outgoing MX user-to-user messages created manually through Message Management (available on Alliance Web Platform).

The notifications are created at the SWIFTNet outbound routing point and routed to this exit queue when the message is ACK'd. The reception of a positive acknowledgement causes the MPF associated with the SWIFTNet outbound queue (**_SI_to_SWIFTNet**) to return a processing result equal to "Success".

LocalMXRejects

This is the queue of NAK notifications related to outgoing MX messages generated by Alliance Access or outgoing MX user-to-user messages created manually through Message Management (available on Alliance Web Platform).

The notifications are created at the SWIFTNet outbound routing point and routed to this exit queue when the message is NAK'd. The reception of a negative acknowledgement causes the

MPF associated with the SWIFTNet outbound queue (**_SI_to_SWIFTNet**) to return a processing result equal to "Failure".

LocalSwiftAcks (Local Ack Queue)

This is the queue of SWIFT ACK notifications related to outgoing messages generated by Alliance Access or outgoing FIN user-to-user messages created manually through the Message Preparation component of Alliance Access. The messages are:

- MT 047: Delivery Instructions Redefinition Request
- MT 090: User-to-SWIFT message
- MT 0nn: All system messages
- MT 101 through MT 999: FIN messages created manually through the Message Preparation component.

The notifications are created at the SWIFT outbound routing point and routed to this exit queue when the message is ACK'd by APC/FIN. The reception of a positive acknowledgement causes the MPF associated with the SWIFT outbound queue (**_SI_to_SWIFT**) to return a processing result equal to "Success".

LocalSwiftNaks (Local Nack Queue)

This is the queue of SWIFT NAK notifications related to outgoing messages generated by Alliance Access or outgoing FIN user-to-user messages created manually through the Message Preparation component of Alliance Access. These messages are described above.

The notifications are created at the SWIFT outbound routing point and routed to this exit queue when the message is NAK'd by APC/FIN. The reception of a negative acknowledgement causes the MPF associated with the SWIFT outbound queue (**_SI_to_SWIFT**) to return a processing result equal to "NAK'd".

MXDeliveryNotifAcks

The following traffic reconciliation notification instances are routed from the **_TR_NOTIF** routing point to this queue:

- MXDeliveryNotifAcks. MX notifications.

The MPF at this routing point is **_AI_to_APPLI**. From this exit point, you can send the delivery notification instances to a message partner with connection method printer or File Transfer XML.

MXDeliveryNotifNaks

The following traffic reconciliation notification instances are routed from the **_TR_NOTIF** routing point to this queue:

- MXDeliveryNotifNaks. MX notifications.

The MPF at this routing point is **_AI_to_APPLI**. From this exit point, you can send the delivery notification instances to a message partner with connection method printer or File Transfer XML.

MXReceived

This is the exit queue to which all incoming MX messages received from SWIFTNet are routed with success from the SWIFTNet inbound routing point.

MXSystem

This is the exit queue to which all incoming MX delivery notifications received from SWIFTNet are routed from the SWIFTNet inbound routing point. A copy is sent to **_TR_REC** for matching the notification with the original message instance.

MXToBeInvestigated (follow-up queue)

This is the default target queue specified for MX messages failing to match any of the conditional routing criteria specified in the sequence of routing rules at a routing point.

Received (Message Inbound Queue)

All incoming messages received from APC/FIN are routed to this exit queue from the SWIFT inbound routing point, except:

- system messages (MT 0nn)
- statement messages (MT 940, MT 950, MT 970, and MT 996)

_SI_to_SWIFT (SWIFT Outbound Queue)

This is the queue of SWIFT messages ready to be sent to the SWIFT network. It is sometimes referred to as the SWIFT "ready" queue. The queue contains, most of the time, messages created at several processing points in the system:

- FIN messages in CAS format received from the Application Interface when the disposition state requested by the CAS protocol specifies "Ready" or when routing point **_SI_to_SWIFT** is requested.
- FIN messages received from the Application Interface, if the message partner has the permissions to bypass verification and authorisation.
- FIN messages entered into the system by the Application Interface and routed from the AI inbound queue by internal default routing.
- APC and FIN System Messages created using the Message Creation application.
- MT 047 message created by the Redefine Delivery command available in the SWIFT Interface application. The message is routed from the system outbound queue (**_SI_system_msg**) as well.
- Messages created using the Message Creation application. In general, these messages are routed to the SWIFT outbound queue from the authorisation queue (**MP_authorisation**).

However, when the operator has the proper bypass permissions, messages may also be moved directly to the SWIFT outbound queue from any of the other queues involved in the preparation of messages, for example:

- Message creation queue (**MP_creation**)
- Verification queue (**MP_verification**)
- Modification queues (**MP_mod_emi_secu**, **MP_mod_text**, **MP_mod_transmis**).

Acceptance criteria: Message instance must be an original input SWIFT message.

Assigned MPF: **_SI_to_SWIFT**

With the default routing rules, the processing results returned by this MPF are:

- Success: The outgoing message was positively acknowledged by APC/FIN.

By default, a message producing this processing result is completed and a notification is routed to one of the four ACK queues.

- Naked: The outgoing message was negatively acknowledged by APC/FIN.

By default, a message producing this processing result is completed and a notification is routed to one of the four NAK queues.

When created using the Message Creation application, the message is routed to the modification queue (MP_mod_text) instead.

- Inactive correspondent: By default, a message producing this processing result is routed to the _MP_mod_transmis queue.

Other processing results which can be returned by this MPF are:

- Authorisation not present: No authorisation record was found. By default, an outgoing message producing this processing result is routed to the re-authentication queue (**_MP_mod_emi_secu**).
- Not authorised by RMA: A valid enabled authorisation was found, but the message was not permitted. By default, an outgoing message producing this processing result is routed to the re-authentication queue (**_MP_mod_emi_secu**).
- Failure: The processing of the outgoing message fails. By default, an outgoing message producing this processing result is routed to the follow-up queue (**ToBeInvestigated**).

An outgoing message whose processing fails for one of the reasons mentioned above is routed by default to the follow-up queue (**ToBeInvestigated**).

Note	FIN messages are sent in FIFO order with respect to the priority and position in the queue.
-------------	---

SI_to_SWIFTNet (SWIFTNet Emission Queue)

This is the queue which provides a collection point for InterAct or FileAct messages ready for emission.

Acceptance criteria: Message instance must be a normal original input MX message.

Assigned MPF: **_SI_to_SWIFTNet**

With the default routing rules, the processing results returned by this MPF are:

- "Success": The outgoing message was positively acknowledged.

By default, a message producing this processing result is completed and a notification is routed to the MX delivery ACK queues.

- "Nacked": The outgoing message was negatively acknowledged.

By default, a message producing this processing result is completed and a notification is routed to the MX delivery NAK queues.

An outgoing message whose processing fails for one of the reasons mentioned above is routed by default to the follow-up queue (**MXToBeInvestigated**).

Note	Real-time messages are sent according to the message expiry date time. Store-and-forward messages are sent in FIFO order with respect to the priority and position in the queue.
-------------	--

Statement (Statement Queue)

Incoming statement messages are routed to this exit queue from the SWIFT inbound routing point. The messages are:

- MT 940: Customer Statement Message
- MT 950: Statement Message
- MT 970: Netting Statement
- MT 996: Answer to an MT 995 Query

System (System Inbound Queue)

All incoming system messages are routed to this exit queue from the SWIFT inbound routing point except:

- MT 021: FIN Retrieval

However, a copy of each MT 021 FIN retrieval message is routed to the system inbound queue as well (**System**).

ToBeInvestigated (Follow-up Queue)

This is the default target queue specified for MT messages failing to match any of the conditional routing criteria specified in the sequence of routing rules at a routing point.

The follow-up queue is also invoked when MPFs fail to process messages which are insufficiently validated or improperly routed.

13.4.1.2 List of System Queues

Overview

This section describes the system queues defined in Alliance Access.

Tip For more information on the terminology used in this section, see the [FIN Operations Guide](#).

AI_from_APPLI (AI Inbound Queue)

All messages entering Alliance Access through the Application Interface (AI) are queued at one single point of entry, before being routed onwards. This single queue is used for all AI input sessions, regardless of the connection method used by the message partner and regardless of the message format. You cannot route messages to this queue.

Acceptance criteria: Creator MPF must be AI_from_APPLI.

Assigned MPF: **AI_from_APPLI**

With the default routing rules, this MPF returns the following result:

- Success: The message was added successfully onto the AI inbound queue.

This MPF can also return the following results:

- Failure
- **Disposition Error:** The message partner details do not allow the message to be disposed in the AI inbound queue.

- Original Broadcast

AI_waiting_ack

This queue holds the messages sent from a standalone Alliance Access system. This queue is only visible if you have licence option **07:STANDALONE REC**.

Acceptance criteria: Any message is accepted.

Assigned MPF: **AI_from_APPLI**

With the default routing rules, this MPF returns the following result:

- Success: The message was added successfully onto the AI inbound queue.

This MPF can also return the following results:

- Failure
- **Disposition Error:** The message partner details do not allow the message to be disposed in the AI inbound queue.
- Original Broadcast

CR_from_CRNET

This queue receives files from the communication server and routes them to the appropriate operator, based on the operator ID.

CR_from_WS

This queue routes files to the **CRI<application name>** queue.

CR_to_WS

This queue routes files from the CR_from_CRNET queue to applications.

IPLA_DLQ

This queue is a "dead letter queue" that stores messages that have failed during processing within Integration Platform (IPLA). If you have licence option **63:IPLA**, you are responsible for monitoring this queue and for taking the appropriate action for the messages that it contains. Depending on the design of a Camel route, messages that failed processing could potentially go to other queues.

MP_authorisation (Message Authorisation Queue)

The queue of messages awaiting authorisation consists of:

- Messages verified by the Message Approval application (the default message flow). These messages include those NAK'd by SWIFT and routed to verification from the modification queue.
- SWIFT MT 999 messages, SWIFT FIN System Messages, and SWIFT APC system messages created by an operator through the Message Creation application.
- FIN messages created by an operator through the Message Creation application, or messages manually corrected through the Message Modification application (including those NAK'd by SWIFT), provided the operator has the proper entitlements and permissions to move these messages directly into the authorisation queue.

- Messages in CAS format received through the Application Interface when the disposition state requested by the CAS protocol specifies "Authorise" or when routing point "**MP_authorisation**" is requested.
- Messages received through the Application Interface, if the message partner does not have the permission to bypass authorisation.

Acceptance criteria: Message instance cannot be a notification.

Assigned MPF: **mpa**

With the default routing rules, this MPF returns the following result:

- Success: The message was processed successfully and is valid.

Messages for the SWIFT network that produce this result are routed to the SWIFT outbound queue (**_SI_to_SWIFT**).

Messages for the application (APPLI) network that produce this result are routed to an exit point specified in the message.

This MPF can also return the following result:

- Failure

_MP_creation (Message Creation)

This is a transient queue for messages created by an operator through the Message Creation application, that is, FIN user-to-user messages (MT 101 to MT 999) and system messages.

A newly created message (when valid) gets queued when an operator invokes one of the commands to move or route the message onwards. If the operator uses the "Route" command, then the MPF invokes the services of the routing software to route the message onto the next queue. If the operator does not use the "Route" command, then the MPF itself moves the message directly into the queue selected by the operator.

Since the message is routed immediately after the MPF completes its processing, there will never be more entries in this queue than the total number of operators entering messages). These entries, however, are barely observable when the queue is monitored, because the time span during which these messages are queued is very short.

Acceptance criteria: Creator MPF must be mpc.

Assigned MPF: **mpc**

With the default routing rules, this MPF returns the following result:

- Success: The message was successfully processed (created) and added onto the queue.

By default, a SWIFT financial message producing this processing result is routed to the verification queue. SWIFT text messages are sent to **_MP_authorisation**.

This MPF can also return the following results:

- Failure
- Discard
- Invalid message.

MP_mod_emi_secu (Emission Security Modification)

This is a queue for messages that require authentication or authorisation. A SWIFT or MX message is added to the Emission Security Modification queue if Alliance Access cannot authenticate it or authorise it. The messages in this queue are mostly input messages.

Acceptance criteria: Creator MPF must be mpc.

Assigned MPF: **mpm**

With the default routing rules, this MPF returns the following result:

- **Success:** The message was successfully processed and is valid.

This MPF can also return the following results:

- Failure
- Discard
- Invalid message.

MP_mod_rec_secu (Reception Security Modification)

This is a queue for output messages that require authentication (only FIN messages allow authentication to be used). Alliance Access and SWIFTNet Link use the related security mechanisms to authenticate and authorise output messages. The output messages that Alliance Access and SWIFTNet Link cannot authenticate or authorise are first routed to this queue. If the message is being sent has failed PKI and digest authentication or the "authorisation to receive" checks, then it is routed to this queue. Then if the authentication, and authorisation are successful, the messages are routed according to the routing rules. If unsuccessful, the messages remain in the queue.

Acceptance criteria: Message instance must be an output message and must be an original instance.

Assigned MPF: **mpm**

This MPF can return the following results:

- Success
- Failure
- Discard
- Invalid message.

MP_mod_reception (Modify After Reception)

This queue is for output SWIFT messages.

Acceptance criteria: Message instance must be an output message and must be an original instance.

Assigned MPF: **mpm**

This MPF can return the following results:

- Success
- Failure
- Discard

- Invalid message.

_MP_mod_text (Text Modification)

This is a queue for messages that have failed message validation, or messages that need data modification (only special fields cannot be modified, for example, sender). A SWIFT or MX message is added to the Text Modification queue, in most cases, if any of the following conditions apply:

- If one or more errors exist in the construction, or syntax of a message, making it syntactically incorrect as far as Alliance Access is concerned
- If an error in the content of a message (for example, an incorrect amount) was identified during verification or authorisation
- If a SWIFT message has been NAK'd by SWIFT due to the message being sent to an unknown address.

Note that any SWIFT message sent to an unknown address is NAK'd by SWIFT. The NAK'd message is added to the Text Modification queue, not the Transmission Modification queue.

Acceptance criteria: Message instance cannot be a notification.

Assigned MPF: **mpm**

With the default routing rules, this MPF returns the following result:

- Success: The message was successfully processed and is valid.

This MPF can also return the following results:

- Failure
- Discard
- Invalid message.

_MP_mod_transmis (Transmission Modification)

A SWIFT message is added to this queue if the integrated application address specified for the receiver of a message is not valid.

Acceptance criteria: Message instance cannot be a notification.

Assigned MPF: **mpm**

With the default routing rules, this MPF returns the following result:

- **Success:** The message was successfully processed and is valid.

This MPF can also return the following results:

- Failure
- Discard
- Invalid message.

_MP_recovery

In the event of a FIN cold start, all completed messages that are not yet identified as delivered are re-activated and routed to this queue.

Acceptance criteria: Message instance cannot be a notification.

Assigned MPF: **mpa**

This MPF can return the following results:

- Success: The message was successfully processed (verified) and is valid.
By default, a message producing this processing result is routed to the authorisation queue (MP_authorisation).
- Failure.

MP_verification

The queue of messages awaiting verification consists of:

- FIN messages created by an operator through the Message Creation application, or messages manually corrected through the Message Modification application (including those marked by SWIFT) and following the default message flow
- SWIFT messages in CAS format received from the Application Interface when the disposition state requested by the CAS protocol specifies "Verify" or when routing point "MP_verification" is requested
- SWIFT messages received from the Application Interface, if the message partner does not have the permission to bypass verification.

Acceptance criteria: Message instance must be an input message and must be an original instance.

Assigned MPF: **mpa**

This MPF can return the following results:

- Success: The message was successfully processed (verified) and is valid.
By default, a message producing this processing result is routed to the authorisation queue (MP_authorisation).
- Failure.

SI_delivery_subset (Delivery Subset Queue)

This queue is assigned to an MPF process which updates the definitions of current SWIFT delivery subsets and the status of future subsets. The messages routed to this queue are notifications related to incoming MT 015, MT 055, and MT 067 messages. The system routing table associated with the SWIFT inbound routing point (**_SI_from_SWIFT**) creates these messages. The notifications are completed after being processed. The following entries can be found in the queue:

- Notification related to an incoming MT 067. This response to an MT 047 redefines current subsets.
- Notification related to an incoming MT 055. This response to an MT 035 redefines current subsets.
- Notification related to an incoming MT 015 - Delayed NAK. SWIFT cancelled the MT 047 request due to an invalid definition of subset criteria. The notification updates the status of future subsets.
- Notification related to an outgoing MT 047. This notification updates the status of future subsets.

Acceptance criteria: Message format must be SWIFT

Assigned MPF: **_SI_delivery_subset**

This MPF can return the following results:

- Success
- Failure.

_SI_from_SWIFT (SWIFT Inbound Queue)

This is the transient queue through which all MT messages received from SWIFT are routed to various routing points and exit queues. An incoming SWIFT MT message gets queued on its arrival in the system, and then routed immediately after the MPF completes its processing.

Consequently, there is never more than one entry in the queue at any given point in time. This entry, however, is barely observable when the queue is monitored because the time span during which the message is queued is very short.

Thus, in practice, the message count of this queue always reads "0". You cannot route messages to this queue.

Acceptance criteria: Creator mpf must be **_SI_from_SWIFT**.

Assigned MPF: **_SI_from_SWIFT**

With the default routing rules, this MPF can return the following results:

- Authorisation not present: No authorisation record was found.

By default, an incoming message producing either of these processing results is routed to the re-authentication queue (**_MP_mod_rec_secu**).

- FINCopy service Bypassed: When a Central Institution maintaining a FINCopy service has a problem, one of the fallback options for the Central Institution is to ask SWIFT to set the service into bypass mode. For more information, see the information regarding fallback in the [FINCopy Service Description](#).

In such a case, the PAC trailers contain no value. It is this criteria that is caught by the routing when you select the result FINCopy service Bypassed.

- Failure: The incoming message failed authentication, using all three receive keys.

By default, an incoming message producing this processing result is routed to the re-authentication queue (**_MP_mod_rec_secu**).

- Invalid Certificate Policy ID: No valid certificate policy ID was found.

By default, an incoming message producing this processing result is routed to the re-authentication queue (**_MP_mod_rec_secu**).

- Invalid digest: The digest values do not match.

By default, an incoming message producing this processing result is routed to the re-authentication queue (**_MP_mod_rec_secu**).

- Invalid Sign DN: The login and select acknowledgement has not been signed by a valid Sign DN.

By default, an incoming message producing this processing result is routed to the re-authentication queue (**_MP_mod_rec_secu**).

- Not Authorised by RMA: A valid enabled authorisation was found, but the message was not permitted.

By default, an incoming message producing this processing result is routed to the re-authentication queue (**_MP_mod_rec_secu**).

- Signature Auth. failure: The signature verification failed, this result can be applicable to the MAC equivalent or PAC equivalent signature.

By default, an incoming message producing this processing result is routed to the re-authentication queue (**_MP_mod_rec_secu**).

- Success: The incoming message passed checksum validation and authentication successfully.

By default, a message producing this processing result is routed, according to its message type, to one of the following three exit queues:

- the statement queue (Statement)
- the system inbound queue (System)
- the message inbound queue (Received).

_SI_from_SWIFTNet (SWIFTNet Reception Queue)

This is the transient queue through which all InterAct or FileAct messages received from SWIFTNet are routed to various routing points and exit queues. An incoming MX message gets queued on its arrival in the system, and then routed immediately after the MPF completes its processing.

Consequently, the queue does not contain more than one entry at any given point in time. However, this entry is barely observable when the queue is monitored because the time span during which the message is queued is very short. Thus, in practice, the message count of this queue always reads "0". You cannot route messages to this queue.

Acceptance criteria: Creator mpf must be **_SI_from_SWIFTNet**.

Assigned MPF: **_SI_from_SWIFTNet**

This MPF can return the following results:

- Success: message is routed to the MXReceived queue
- Failure: message is routed to the MXToBeInvestigated queue
- Authorisation does not allow message
- Authorisation not enabled
- Authorisation not in validity period
- No authorisation
- Signature verification failure.

By default, an incoming InterAct message that produces one of these processing results is routed to the re-authentication queue (**_MP_mod_rec_secu**). For an incoming FileAct message, the message will not be stored in the interface and event 28117 will be generated.

_SI_system_msg (System Outbound Queue)

This is a transient queue for the APC and FIN system message (for example, MT 047 redefine delivery subsets) created using the SWIFT Interface application (SIA).

Since the messages are routed immediately to the SWIFT outbound queue (**_SI_to_SWIFT**) after the MPF completes its processing, there is never more than one entry in the queue at any

given point in time. This entry, however, is barely observable when the queue is monitored because the time span during which the message is queued is very short.

Thus, in practice, the message count of this queue always reads "0".

Acceptance criteria: Creator mpf must be **_SI_system_msg**.

Assigned MPF: **_SI_system_msg**

This MPF can return the following results:

- Success: The message was added successfully onto the queue.

By default, a message producing this processing result is routed to the SWIFT outbound queue (**_SI_to_SWIFT**).

- Failure.

_SS_alarm_creation (Alarm Queue)

This is a queue through which alarm messages are created before being sent to the message receiver.

Acceptance criteria: Creator mpf must be **SS_alarm_creation**.

Assigned MPF: **SS_alarm_creation**

With the default routing rules, this MPF returns the following result:

- Success. The alarm message can be successfully routed to the message addressee.

This MPF can also return the following result:

- Failure.

_TR_NOTIF (Traffic Reconciliation Notification)

This queue is used for traffic reconciliation, for example, to match a message report to a message instance. The notification is created in the **TR_NOTIF** routing point.

Acceptance criteria: Creator mpf must be **TR_REC**.

Assigned MPF: **TR_REC**

With the default routing rules, this MPF can return the following results:

- Delivered
- Not delivered
- Delayed delivery.

This MPF can also return the following result:

- Not matched

_TR_REC (Traffic Reconciliation Received)

This queue contains all the network reports (MT 010, 011, 015 and 019) that must be matched to a message instance.

Assigned MPF: **TR_REC**

With the default routing rules, this MPF can return the following results:

- Delivered

- Not delivered
- Not matched
- Delayed delivery.

Unroutable (Unroutable messages)

This is a queue to manage messages that cannot be successfully routed to any other queue in the case of a message not matching the acceptance criteria of a queue. It is the responsibility of the user to investigate and define what next to do with this message.

Assigned MPF: **Dummy_mpfn**

This MPF can return the following results:

- Success
- Failure.

13.4.1.3 OI_to_OTHER Queue

Description

When the correspondent has been assigned the OTHER network, an operator can move the message to the **_OI_to_OTHER** queue.

An operator can specify the OTHER network for a Correspondent in the **Preferred Network** tab of **Correspondent Details** window.

Routing

The **_OI_to_OTHER** queue has the properties of a user-defined queue but an operator cannot delete the routing.

Note To route messages in a queue to **_OI_to_OTHER**, an operator must add **_OI_to_OTHER**, as target of the **Dispose** to action in the appropriate routing rules.

Standalone Alliance Access

If a standalone Alliance Access is installed for message creation and repair, then the **_OI_to_OTHER** queue has an important role in the routing of messages to the master Alliance Access. For more information about the use of this queue for the standalone Alliance Access, see the *Installation Guide for AIX, Linux, Oracle Solaris, or Windows*.

13.4.2 Queues Page

Content

The **Queues** page contains these elements:

- Filtering criteria and functionality that enable you to filter the list entities on the **Queues** page:
 - See "Queues" on page 464
 - See "Functions" on page 22
- Details of the queues defined for the current Alliance Access instance

See "Queues" on page 464

- Functions that enable you to manage the queues

See "Functions" on page 465

Display

Queues

Queues		Filtering criteria
Field	Description	
Name	The name of the queue. You can specify the Name ⁽¹⁾ value to use for filtering	✓
Type	<p>Specifies the Type ⁽¹⁾ values to use for filtering:</p> <ul style="list-style-type: none"> • Available contains the list of values available • Selected contains the values to use for filtering <p>The queue type</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • ADK • Exit Point • System • IPLA • User-defined 	✓
Status	<p>The current status of the queue</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Held • Released <p>If the queue is held, then the associated MPF cannot process the messages in it.</p>	

Queues		
Field	Description	Filtering criteria
Visible Routing Rules	<p>Determines whether to filter on visible routing rules. If you select this check box, then the system returns only the queues that are configured to display the routing rules (Queue Details window Routing Rules tab).</p> <p>By default, the following queues have visible routing rules:</p> <ul style="list-style-type: none"> • _OI_to_OTHER • _SI_from_SWIFT • _SI_to_SWIFT • _SI_from_SWIFTNet • _SI_to_SWIFTNet • _TR_NOTIF 	✓

(1) See "Queues" on page 464

13.4.3 Queue Functions

Overview

These functions enable you to manage the queues.

Functions

Function	Description	Queues page	Queue Details window	Routing Rule Details window
Add / Add As	<p>Queues page:</p> <ul style="list-style-type: none"> • Enables you to add a queue <p>Queue Details window Routing Rules tab:</p> <ul style="list-style-type: none"> • Enables you to add a routing rule <p>Procedure: "Add Entities" on page 26</p>	✓	-	✗
Hold	Holds a released queue	✓	✓	✗
Release	Releases a held queue	✓	✓	✗
Delete	Deletes a queue	✓	✓ ⁽¹⁾	✗

(1) Present only on the **Routing Rules** tab

13.4.4 Queue Details Window

Overview

The **Queue Details** window uses tabs to group related information together.

13.4.4.1 Queue Details Window: Configuration Tab

Content

The **Configuration** tab contains these elements:

- Details that relate to the configuration of the queues
See "Details" on page 466
- Functions that enable you to manage the queues
See "Functions" on page 465

Display

Queue Details - MXReceived

Help

Configuration Routing Info Monitoring

Name: MXReceived

Type: Exit Point

Function Assigned: AI_to_APPLI

Message Partner: MXPrinter

Processing Order: FIFO

Queue Threshold: 500 Messages

Maximum Message Age: 0 Days

Close Refresh Report Hold Previous Next

Details

Field	Description
Name	The name of the queue
Type	See Type in "Queues" on page 464
Function Assigned	See Function Assigned in "Queues" on page 464
Message Partner	See Message partner in "Queues" on page 464
Processing Order	See Processing Order in "Queues" on page 464
Queue Threshold	The number of messages that may be present in a queue before an alarm is generated

Field	Description
Maximum Message Age	<p>Specifies the maximum message age</p> <p>If a message instance stays longer in the queue than the value set, then this triggers an event and puts the queue in an exceptional state.</p> <p>To specify a value, type a numeric value in the first field and select the units that you require from the drop-down list in the second field.</p> <p>The possible values are as follows:</p> <ul style="list-style-type: none"> • Days • Hours • Minutes <p>0 means that no alarm will be generated.</p>
Acceptance Criteria	Specifies the acceptance criteria

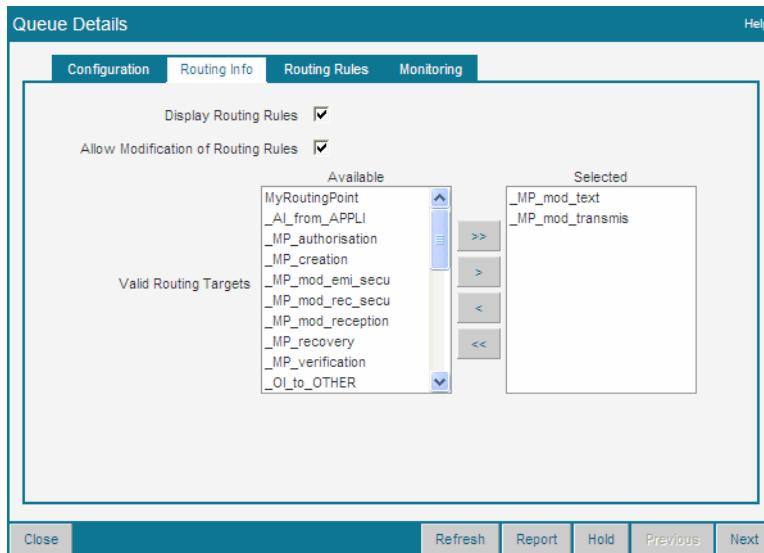
13.4.4.2 Queue Details Window: Routing Info Tab

Content

The **Routing Info** tab contains these elements:

- Details that relate to the routing information of the queues
See "Details" on page 468
- Functions that enable you to manage the queues
See "Functions" on page 465

Display



Details

Field	Description
Display Routing Rules	Determines whether the routing rules of the routing points are visible or not
Allow Modification of Routing Rules	Determines whether modification of the routing rules of the routing points is allowed or not Modification of routing rules is subject to specific permissions
Valid Routing Targets	Specifies the valid routing targets for the queue that the window currently displays The Available list contains a list of all the routing points reachable from the queue except for exit points, which the system already considers as valid routing targets. The values that you include in the Selected list become valid routing targets for the queue.

13.4.4.3 Queue Details Window: Routing Rules Tab

Content

The **Routing Rules** tab contains these elements:

- A filtering criterion that enables you to filter the list entities on the **Routing Rules** tab
See "Details" on page 469
- Details that relate to the routing rules of the queues
See "Details" on page 469

The **Routing Rules** tab shows only a subset of the details for the queue. The other tabs of the **Queues Details** window collectively contain the remainder of the queue details. See "Queue Details Window" on page 465.

- Functions that enable you to manage the queues
See "Functions" on page 465

For more information, see "Queues" on page 446.

Display

Queue Details - _SI_from_SWIFTNet

Help

Configuration Routing Info **Routing Rules** Monitoring

Filter on Schema: All

Default Action: Dispose To: MXToBeInvestigated

Routing Rules (Rows in list: 7, in selection: 0)

Change View	Add	Delete	Report	Previous	Next
Sequence Number	Description		Schemas		
80	System messages to TR_REC		A		
90	FileAct messages to FileActRec		A		
100	MX messages to MXReceived		A		
200	route deliv. notif. to MXSyste		A		
300	No authorisation		A		
400	Not authorised		A		
500	Signature error		A		

Close Refresh Report Hold Previous Next

Details

Field / Column	Description	Filtering criteria
Filter on Schema	Filters the list of routing rules according to schema assignment. If you select a value from the drop-down list, then the system returns only the routing rules that are assigned to the corresponding schema.	✓
Sequence Number	Indicates the order of activation of the routing rule relative to the other routing rules for the routing point.	
Description	The description of the rule.	
Schemas	The routing schemas that the routing rule is assigned to.	
Default Action	Specifies the default routing action.	

13.4.4.4 Routing Rules Details Window

Overview

The **Routing Rules Details** window uses tabs to group related information together.

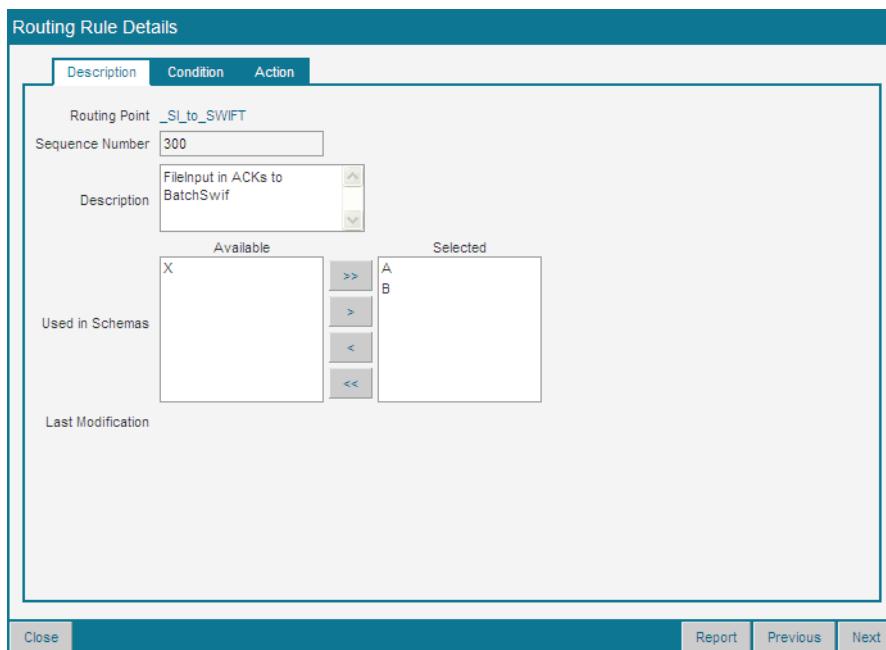
13.4.4.4.1 Routing Rules Details Window: Description Tab

Content

The **Description** tab contains these elements:

- Details that relate to the description of the routing rules for a queue
See "Details" on page 470
- Functions that enable you to manage the routing rules for a queue
See "Functions" on page 465

Display



Details

Field	Description
Routing Point	The name of the queue for which the routing rule is active
Sequence Number	Specifies the order of activation of the routing rule relative to the other routing rules for the routing point By default, the system gives the first routing rule the number 100. Then the system increments the number by 100 for each subsequent rule.
Description	The description of the rule
Used in Schemas	The routing schemas that the system assigns the routing rule to The Available list contains a list of all the routing schemas in Alliance Access. The system assigns the routing rule to the values that you include in the Selected list.

Field	Description
Last Modification	The time of the last modification to the routing rule

13.4.4.4.2 Routing Rules Details Window: Condition Tab

Content

The **Condition** tab contains these elements:

- Details that relate to the conditions of the routing rules for a queue
See "Details" on page 472
- Functions that enable you to manage the routing rules for a queue
See "Functions" on page 465
- Functions that enable you to create conditional statements
See "Functions" on page 472

Display

The screenshot shows the 'Routing Rule Details' window with the 'Condition' tab selected. The window is divided into several sections:

- Top Bar:** 'Routing Rule Details' with tabs for 'Description', 'Condition' (selected), and 'Action'.
- Condition on:** A dropdown set to 'Message and Function'.
- Available Function Results:** A list box containing 'Authorisation not present', 'Failure', 'Inactive correspondent', 'Nacked', and 'Not Authorised by RMA'.
- Selected Success:** An empty list box.
- Message Criteria Editor:** A panel containing the query '(Src_entity = 'FileInput')' and a toolbar with buttons for 'Add Criteria', 'AND', 'OR', 'NOT', '(', ')', and 'Validate'.
- Bottom Buttons:** 'Close', 'Report', 'Previous', and 'Next'.

Details

Field	Description
Condition on	<p>Specifies the condition type that triggers the routing rule</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Always: the system always performs the routing action, even when the trigger conditions are not matched • Message: the system performs the routing action if the message attributes match the conditional statements specified in the trigger condition • Function: the system performs the routing action if the processing result that the MPF returns matches one of the processing results specified in the trigger condition • Message and Function: the system performs the routing action if either the message or the function result trigger conditions are matched
Function Result	<p>Specifies the routing results that are a trigger condition for the routing rule</p> <p>The Available list contains a list of all processing results the assigned MPF can return for a message instance.</p> <p>The values that you include in the Selected list become trigger conditions for the routing rule.</p> <p>Present only when Condition on is set to Function OR Message and Function.</p>
Message	<p>The conditional statements</p> <p>A conditional statement is a rule criterion based upon a list of approved message attributes called keywords.</p> <p>Each conditional statement that you construct in this field must conform to the predefined syntax which uses keywords and boolean operators.</p> <p>For the functions associated with this field, see "Functions" on page 472</p> <p>Present only when Condition on is set to Message OR Message and Function.</p>

Functions

Function	Description
Add Criteria	<p>Enables you to add conditional statements to message instances</p> <p>Available when the Condition on field is set to Message OR Message and Function.</p> <p>Procedure: "Define Trigger Conditions (Condition Tab)" on page 504</p>
AND	Appends an and boolean (logical "and" function) to the content of the Message field
OR	Appends an or boolean (logical "or" function) to the content of the Message field
NOT	Appends a not boolean (does not equal) to the content of the Message field
(Appends a ((establish precedence open parenthesis) to the content of the Message field
)	Appends a) (establish precedence close parenthesis) to the content of the Message field

Function	Description
lower	When defining a message or message and function condition, if you precede the message field with <code>lower</code> , all case variations of the field text will satisfy the criteria (such as "Text", "text", "TEXT", "texT", and so on). For example, the condition <code>(lower(Src_entity) like 'mpin%')</code> is satisfied for messages input by the message partners <code>MPInput</code> , <code>MplnputMx</code> , <code>mpIN</code> , and so on. If you do not precede the message field with <code>lower</code> , only the specified case will satisfy the criteria (case-sensitive).

13.4.4.4.3 Routing Rules Details Window: Action Tab

Content

The **Action** tab contains these elements:

- Details that relate to the actions of the routing rules for a queue
See "Details" on page 474
- Functions that enable you to manage the routing rules for a queue
See "Functions" on page 465

Display

Details

Field	Description
Action on	<p>Specifies the type of message instance that is the target of the rule action</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Source: specifies the source instance as the target and displays the fields of the Source Instance area • New Instance: specifies new instances as the target and displays the fields of the New Instance area • Source and New Instance: specifies both source and new instances as the target and displays the fields of the Source Instance and the New Instance areas

Source Instance and New Instance

Field	Description
Type ⁽¹⁾	<p>Determines whether the system routes a copy instance or a notification with details about the instance to another routing point or to an addressee</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Copy: routes a copy instance • Notification/Transmission: routes a notification with transmission information • Notification/Information: routes a notification with information about a particular action • Notification/History: routes a notification with intervention details
Action	<p>Specifies the action to perform on an instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • None ⁽²⁾: the system performs no action • Complete ⁽²⁾: the life cycle of the message is finished, so it requires no further processing • Dispose To: the system routes instances to the routing point selected from the drop-down list of valid targets <p>The drop-down list appears below the Action field when Dispose To is selected.</p> <ul style="list-style-type: none"> • To Addressee: the system routes message instances to the message receiver (or to the message sender ⁽¹⁾)

Field	Description
Addressee ⁽¹⁾	<p>Specifies the addressee destination</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Sender: the system routes message instances to the message sender • Receiver: the system routes message instances to the message receiver <p>Present only when Action is set to To Addressee.</p>
Intervention	<p>Determines whether the system appends an intervention to the instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • No Intervention: does not append an intervention • Copy Text Intervention: includes a copy of the message text as an intervention • Free Formatted Intervention: appends the text that you input in the Intervention Text field <p>Not present when Action is set to None.</p>
Intervention Text	<p>The free formatted intervention text</p> <p>Present only when Intervention is set to Free Formatted Intervention.</p>
Unit	<p>Determines whether the system assigns units to an instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Keep Current: applies the current unit assignment • None: does not assign units <p>Not applicable when Type is set to Notification/<value>. It is not possible to change the unit assignment that a notification inherits from the original or copy instance.</p>
Routing Code	<p>Specifies the routing code that the Routing application adds to a message instance, when the routing rule is applied</p> <p>The system transmits this code to a back-office application (that is, a message partner) for routing purposes within that application.</p>

Field	Description
Priority	<p>Specifies the instance priority</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Keep Current: keeps the current instance priority value • 1-Highest • 2 • 3-System • 4 • 5-Urgent • 6 • 7-Normal • 8 • 9-Lowest

(1) Valid only for **New Instance**

(2) Valid only for **Source Instance**

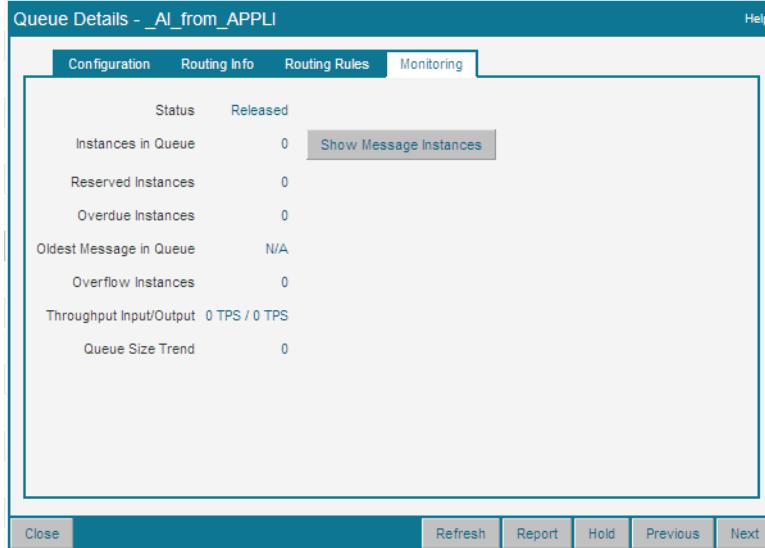
13.4.4.5 Queue Details Window: Monitoring Tab

Content

The **Monitoring** tab contains these elements:

- Details that relate to the monitoring of the queues
See "Details" on page 477
- Functions that enable you to manage the queues
See "Functions" on page 465
- A function that enables you to view the message instances for a queue
See "Functions" on page 477

Display



Details

Field	Description
Status	Indicates if the queue is currently either <code>Released</code> or <code>Held</code>
Instances in Queue	The number of live message instances currently in the queue
Reserved Instances	The number of reserved message instances currently in the queue
Overdue Instances	The number of overdue message instances currently in the queue
Oldest Message in Queue	The time and date of the oldest message instance currently in the queue
Overflow Instances	The number of message instances that are above the queue threshold
Throughput Input/Output	The input and output throughput (in TPS) of the queue, that is, the number of message instances that are routed to (input) or from (output) the queue in 1 second.
Queue Size Trend	The difference between the current queue size and the previous queue size brought back to 1 second. A positive trend indicates that build-up is increasing. A negative trend indicates that build-up is decreasing.

Functions

Function	Description
Show Message Instances	Opens the Message Instances in Queue window See "Message Instances in Queue" on page 478

13.4.5 Message Instances in Queue

Overview

Every message stored in Alliance Access can be uniquely identified based on information contained within parts of the header and text.

A Unique Message Identifier (UMID) consists of a User Unique Message Identifier (UUMID) plus a suffix, which makes it unique in the scope of Alliance Access. A UUMID, which is unique from the point of view of a single Alliance Access user, consists of the following:

I/O + Correspondent + ID (type of message) + Reference

where Reference is either TRN or MUR (MUR can be empty). However, note that the UUMID will not always be unique to a user, for example, if the user puts the same Reference twice in a single message.

For more information on these elements and other instance information, see "Details" on page 479.

Content

The **Message Instances in Queue** window contains these elements:

- Details of the messages instances in the queue
See "Details" on page 479
 - Functions that enable you to manage the message instances
See "Functions" on page 480

Display

Message Instances in Queue _SI_to_SWIFT								Rows in list: 1, in selection: 1			
Instances								Rows in list: 1, in selection: 1			
Change View		Refresh	Change Priority		Re-assign	Complete	Move to	Cancel Emission	Report	< Previous Next >	
<input checked="" type="checkbox"/>	I/O	Correspondent		Identifier		Reference		Suffix		Inst #	In Queue
<input checked="" type="checkbox"/>	I	AENTBEEAXXX		fin.199		test		140324		0	_SI_to_SWIFT

Details

Column	Description
I/O	<p>Indicates the direction of flow for the message instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • I: The message is input to a network, such as SWIFT (Alliance Access sends the message) • o: The message is output from a network (Alliance Access receives the message)
Correspondent	<p>The BIC address (11 alphanumeric characters long) of the sender, or receiver of the message instance</p> <p>If no specific branch code is given, then the last 3 characters of the BIC-11 address default to XXX.</p> <p>The direction of flow for the message instance determines which party the BIC address identifies:</p> <ul style="list-style-type: none"> • If the value for I/O is I, then the value for Correspondent is the BIC-11 address of the receiver of the message instance. • If the value for I/O is o, then the value for Correspondent is the BIC-11 address of the sender of the message instance.
Identifier	<p>Identifies the type of message</p> <p>For SWIFT format, this is always a 3-character number and refers to the message type. Example: 100 for a customer transfer.</p>
Reference	<p>The message reference</p> <p>The value depends on the message format:</p> <ul style="list-style-type: none"> • MT: <ul style="list-style-type: none"> – Either the Transaction Reference Number (TRN), which is located in Field 20 of the message – Or the Message User Reference (MUR), which is located in the SWIFT User Header of the message • MX: a user reference • Other formats: the number from the header or message text
Suffix	<p>A system-generated value to make the UMID unique</p> <p>The first part is the creation date of the message in YYMMDD format. The second part is a 5-digit number that the system generates at random and is unique for all messages for each day.</p>
Inst #	<p>The sequence number of the message instance</p> <p>The original message instance has the sequence number 0.</p>
In Queue	<p>The queue that the message instance is in</p> <p>The system does not display this column by default.</p>
In Queue Since	<p>The date and time of the message instance entering the queue</p> <p>The system does not display this column by default.</p>

Column	Description
Type	<p>The message instance type</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Original • Copy • Notification
Priority	The current internal priority of the message instance
Date/Time	<p>The creation date and time of the message instance</p> <p>The system does not display this column by default.</p>
Creating Function	<p>The function that created the message instance</p> <p>The system does not display this column by default.</p>
Related Instance	<p>The number of related message instances that are not complete</p> <p>The system cannot complete a message until all the related message instances are completed.</p> <p>The system does not display this column by default.</p>
Unit	The unit that the message instance is assigned to
Service Name	<p>The SWIFTNet service for the message instance</p> <p>The system does not display this column by default.</p>
Application	<p>The application in which the message instance was created</p> <p>The system does not display this column by default.</p>
Function	<p>The last function to have processed the message instance</p> <p>The system does not display this column by default.</p>
Message Description	<p>The description of the message</p> <p>The system does not display this column by default.</p>
Status	<p>The status of the message instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Live • Completed • Reserved <p>The system does not display this column by default.</p>

Functions

Function	Description	Message Instances in Queue window	Message Details Area	
			Instances Tab	All other tabs
Change Priority	<p>Enables you to change the priority of message instances</p> <p>Procedure: "Change the Priority of Message Instances" on page 509</p>	✓	✓	x

Function	Description	Message Instances in Queue window	Message Details Area	
			Instances Tab	All other tabs
Re-assign	Enables you to re-assign message instances Procedure: "Re-assign Message Instances to a Unit" on page 510	✓	✓	x
Complete	Completes the message instance	✓	✓	x
Move to	Enables you to move message instances Procedure: "Move Message Instances" on page 512	✓	✓	x
Re-activate	Enables you to reactivate message instances Procedure: "Re-activate Completed Message Instances" on page 513	x	✓	x
Report	Enables you to generate a report of instance-specific information of a message Procedure: "Generate an Instance Report" on page 514	✓	✓	x
Cancel Emission	Enables you to cancel message instance emissions for FIN, InterAct, and FileAct messages. To use this function, the Message File, Cancel msg emission permission is required. For more information, see the section on cancelling message instance emissions in Message Management Guide .	✓	✓	x
Search Results	Returns you to the Message Instances in Queue window view	x	✓	✓
Instance Description & Comments	Shows the Instance Description & Comments view for the current instance	x	✓	x
Interventions	Shows the Interventions List view for the current instance	x	✓	x
Instances List	Returns you to the Instances List view for the current instance	x	✓	x
Interventions List	Returns you to the Interventions List view for the current instance	x	✓	x

13.4.6 Message Details Area

Overview

The **Message Details** area uses tabs to group related information together.

13.4.6.1 Message Details Area: Header Tab

Content

The **Header** tab contains these elements:

- Details that relate to the header information of a message instance

See "Details" on page 483

- Functions that enable you to navigate the **Message Details** area

See "Functions" on page 480

Display

Message Details - IAENTBEDAXXX103RACHELLE WOO Help

Header Sender/Receiver Text History Instances Other

Status	Possible duplicate indicator set locally Duplicate detected by interface Deletable		
Format	Swift	Sub-Format	Input
Identifier	fin.103		
Nature	Financial		
Sender	AENTBEDAXXX	LT	A
Receiver	AENTBEDAXXX	LT	X
Transaction Reference	RACHELLE WOO		
Priority	Normal		
Banking Priority			
MUR	RACHELLEFC		
Amount	1000,	Currency	EUR
		Value Date	15/07/13

Close Previous Next

Close

Details

Field	Description	Message format		
		MT	MX	File
Status	<p>The status indicators that are applicable to the message instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Message Modified: indicates that the message instance text has been modified after sending • Possible Duplicate Emission: indicates that the message instance may have been sent before • Possible Duplicate Reception: indicates that the message instance may have been received before • Partial Message: indicates that the message instance is incomplete • Read-only: indicates that the SWIFT Interface sets the incoming message instance to read only <p>This status cannot be reset.</p> <ul style="list-style-type: none"> • Retrieved: indicates that the message instance has been retrieved from the network and extracted from an MT 021 • Sanctions screening - Message blocked: indicates that Sanctions Screening has reported the MT message instance as a true hit. <p>For more information about this warning, see "Configuration for Sanctions Screening" on page 58.</p> <ul style="list-style-type: none"> • Template <name>: indicates that the message instance is the template used as the basis for other messages • Test Message: indicates that a Test and Training destination sent the message instance 	✓	✓	✓
Format	<p>The format of the message instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Swift: MT message format • MX: MX message format • File 	✓	✓	✓
Sub-Format	<p>Indicates the direction of flow for the message instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Input: Alliance Access sends the message instance to a network. • Output: Alliance Access receives the message instance from a network. 	✓	✓	✓

Field	Description	Message format		
		MT	MX	File
Identifier	Identifies the message type of the message instance The system uses a code to identify the message type. For MT messages, the system prefixes the code with <code>fin</code> for financial messages and <code>apc</code> for system messages	✓	✓	✓
Nature	The business nature of the message instance These are the possible values: <ul style="list-style-type: none">• Financial: a financial message• Network: a system message	✓	x	x
Sender	The BIC-11 address of the sender of the message instance The direction of flow for the message instance determines which party the BIC-11 address identifies: <ul style="list-style-type: none">• If the value for Sub-Format is <code>Input</code>, then the value for Sender is your BIC-11 address.• If the value for Sub-Format is <code>Output</code>, then the value for Sender is the BIC-11 address of the party that sends you the message instance.	✓	x	x
Receiver	The BIC-11 address of the receiver of the message instance The direction of flow for the message instance determines which party the BIC-11 address identifies: <ul style="list-style-type: none">• If the value for Sub-Format is <code>Input</code>, then the value for Receiver is the BIC-11 address of the party to which you send the message instance.• If the value for Sub-Format is <code>Output</code>, then the value for Receiver is your BIC-11 address.	✓	x	x
LT	The logical terminal that sent or received the message at your side	✓	x	x
Transaction Reference	The transaction reference number This value is found in field 20 of the message.	✓	x	x
Priority	The priority of the message, either: <ul style="list-style-type: none">• Normal: the standard priority for a message• System: the priority for SWIFT user-to-system messages (MT0nn)• Urgent: lets the sender communicate the urgency of a message and lets the recipient select the message as a priority when it arrives	✓	✓	✓
Banking Priority	Same as User Priority	✓	x	x
MUR	The Message User Reference	✓	✓	✓

Field	Description	Message format		
		MT	MX	File
Amount ⁽¹⁾	The amount as it occurs in the first Amount sub-field of the message	✓	x	x
Currency ⁽¹⁾	The three-character ISO (International Standards Organisation) currency code format for the currency of the Amount	✓	x	x
Value Date ⁽¹⁾	The date on which the Amount is credited to or debited from the account of the receiver	✓	x	x
Requestor DN	The sender of the message	x	✓	✓
Responder DN	The receiver of the message	x	✓	✓
Service Name	The SWIFTNet service for which the message is sent or received	x	✓	✓
Non-repudiation	<p>The result of the request for non-repudiation of the message</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • TRUE • FALSE • Empty, if non-repudiation is not requested 	x	✓	✓
Sign Message	<p>The result of the request to sign the message</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • TRUE • FALSE • Empty, if it is not requested to sign the message 	x	✓	✓
Delivery notif. request	Indicates whether notification of delivery is required	x	✓	✓
Overdue Warning Time	The date and time (in UTC) after which store-and-forward generates an overdue warning if the message or the file remains undelivered	x	✓	✓
Overdue Warning Delay	<p>The number of minutes after which store-and-forward generates an overdue warning if the message or the file remains undelivered</p> <p>The minimum value is 5, the maximum value is 1440.</p>	x	✓	✓
MX Keyword 1	The first MX keyword, if found	x	✓	x
MX Keyword 2	The second MX keyword, if found	x	✓	x
MX Keyword 3	The third MX keyword, if found	x	✓	x

(1) The system shows a value in this field for financial messages only. The value is found in field 32A of the message.

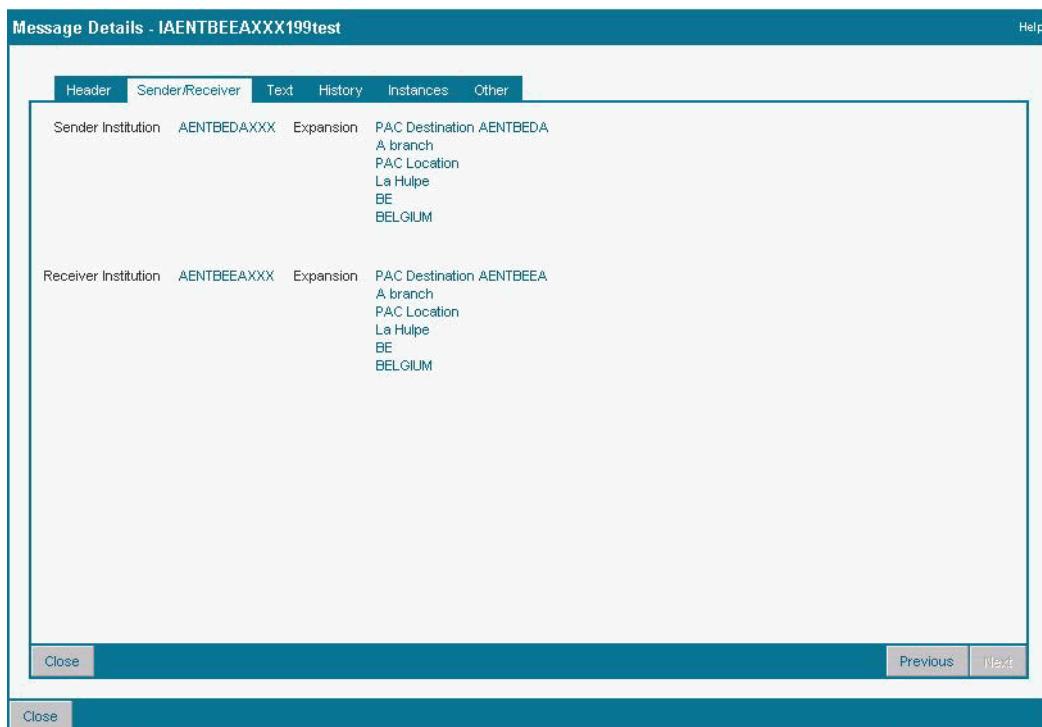
13.4.6.2 Message Details Area: Sender / Receiver Tab

Content

The **Sender / Receiver** tab contains these elements:

- Details that relate to the sender and receiver information of a message instance
See "Details" on page 486
- Functions that enable you to navigate the **Message Details** area
See "Functions" on page 480

Display



Details

Field	Description
Sender Institution	The BIC-11 address of the institution that sends the message instance
Receiver Institution	The BIC-11 address of the institution that receives the message instance
Expansion	The expansion of the BIC-11 address of the institution
Recipients for Distribution⁽¹⁾	Contains the list of the recipient DNs to which the message or file is distributed
Public⁽¹⁾	Indicates whether the list of the recipient DNs is made public to all recipients

(1) Present only when SWIFTNet Copy is requested for the current message.

13.4.6.3 Message Details Area: Text Tab

Content

The **Text** tab contains these elements:

- The message text of a message instance

See "Message text" on page 487

The other tabs of the **Message Details** area collectively contain the complete set of details for the messages instance. See "Message Details Area" on page 481.

- Functions that enable you to navigate the **Message Details** area

See "Functions" on page 480

Message text

The **Text** tab displays the contents of the body of the message. You can display this tab and the information within it only if you are a member of a unit to which at least one of the message instances is assigned.

The text of a message can appear in either normal or expanded format. Normal format displays the message text using standard SWIFT syntax. The expanded format provides descriptive names for each field and a more readable field layout.

For SWIFT messages, the display shows blocks 4 and 5. Optionally, the message text can also contain the U-blocks and the S-blocks. These blocks are reserved for local use and are never transmitted over the SWIFT network.

Depending on the value of the configuration parameter **FIN User Header**, the **Text** tab may also show the contents of the FIN User Header (block 3) of the message.

13.4.6.4 Message Details Area: Response Text Tab

Content

For real-time MX AnyXML or other XML messages sent only.

For MX messages sent using real-time delivery, the **Response Text** tab contains a business response from the message receiver. The **Display expanded text** option is also available on this tab. This option is only shown when Alliance Access Configuration was able to retrieve the message definition of the response (deployment package installed) and the response is valid according to its schema definition.

13.4.6.5 Message Details Area: Related Messages Tab

Content

For MX messages; relevant only for store-and-forward delivery.

Appears in the message details if the message that you open is related to at least one other message.

13.4.6.6 Message Details Area: File Tab

Content

The **File** tab contains these elements:

- The message details of File messages

The other tabs of the **Message Details** area collectively contain the complete set of details for the messages instance. See "Message Details Area" on page 481.

- Functions that enable you to navigate the **Message Details** area

See "Functions" on page 480

13.4.6.7 Message Details Area: History Tab

Content

The **History** tab contains these elements:

- The message history of a message instance

The other tabs of the **Message Details** area collectively contain the complete set of details for the messages instance. See "Message Details Area" on page 481.

- Functions that enable you to navigate the **Message Details** area

See "Functions" on page 480

Note

The Message History Tab shows only the final routing rule that was applied to the source instance, that is, the instance that is being routed.

For example, if two routing rules are applied to an original instance, and if the first routing rule *does not* perform an action on the original instance but the second rule *does* perform an action, then the history of the message includes only the details of the second routing rule. The history does not include details of the first routing rule.

13.4.6.8 Message Details Area: Instances Tab

Content

The **Instances** tab contains these elements:

- Details that relate to the instances of a message instance

See "Details" on page 489

- Functions that enable you to navigate the **Message Details** area

See "Functions" on page 480

Display

Message Details - IAENTBEDAXXX103RACHELLE WOO

Header Sender/Receiver Text History Instances Other Help

Instances List Rows in list: 1, in selection: 1

Instances List								
Change View		Complete	Move to	Re-assign	Re-activate	Cancel Emission	Instance Report	Change Priority
<input checked="" type="checkbox"/>	Inst #	In Queue	Status	Type	Instance Priority	Application	Date/Time	
<input checked="" type="checkbox"/>	0	_SI_to_SWIFT	Live	Original	7	Messenger Adapter	2014/03/24 11:37:46	

Details

Field	Description
Inst #	The sequence number of the message instance The value is always 0 for the original instance.
In Queue	The routing queue where the message instance is currently being processed or waiting to be processed
Status	Indicates the status of the message instance These are the possible values: <ul style="list-style-type: none"> • Live: The instance is queued at a routing point. • Completed: The instance is not queued at a routing point.

Field	Description
Type	<p>Indicates what type of instance the message instance is</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Original <p>These are the events that generate original message instances:</p> <ul style="list-style-type: none"> – Reception of a message from the SWIFT network – Reception of a message from a message partner through the Application Interface – Manual creation of a message • Copy <p>Copy instances make it possible to process message instances in parallel within the system. This enables the same message to be sent to various internal and external locations.</p> <p>A copy instance exists independently from its original instance. Copy instances are created at routing points by routing rules and are usually generated for information.</p> • Notification <p>A notification provides information on the processing of a message and is usually sent to the originator of the message. A notification reports that the status of a message has changed in some way. For example: when the message has been positively acknowledged by the SWIFT network.</p>
Instance Priority	<p>The current internal priority of the message instance</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Keep Current: keeps the current instance priority value • 1-Highest • 2 • 3-System • 4 • 5-Urgent • 6 • 7-Normal • 8 • 9-Lowest
Application	The application that created the message instance
Date/Time	The creation date and time of the message instance
Creating Function	The Message Processing Function (MPF) that created the message instance

Field	Description
Function	The name of the last MPF that processed the message instance If the message instance is reserved, then this is the function which is currently processing the instance.
Related Instance	The related instance
Unit	The name of the unit that the message instance is assigned to
In Queue Since	The date and time of the message instance entering the queue

13.4.6.9 Instances Tab: Instance Details

Overview

The **Instances** tab can also show the details for an instance that you select from the **Instances List**.

13.4.6.9.1 Instance Description & Comments

Content

The **Instances** tab contains these elements:

- Details that relate to the instances of a message instance
See "Details" on page 489
- Functions that enable you to navigate the **Message Details** area
See "Functions" on page 480

Display

Message Details - IAENTBEDAXXX103RACHELLE WOO

Header Sender/Receiver Text History Instances Other

Instance Description & Comments Interventions

Description Comments

Message UUMID: IAENTBEDAXXX103RACHELLE WOO
Instance No.: 0
Instance Type: Original
Assigned Unit: None
Status: Instance in rp (_SI_to_SWIFT) previously processed by (mpc) with a return status=Success
Instance Priority: 7
In Queue Since: 2014/03/24 11:37:46

Addressee

Institution: AENTBEDAXXX PAC Destination AENTBEDA
A branch
La Hulpe
BE

Close Previous Next

Details

Description

Field	Description
Message UUMID	The Unique Message Identifier that the system creates from information in the header and text of the message
Instance No.	See Inst # in "Details" on page 489
Instance Type	See Type in "Details" on page 489
Assigned Unit	See Unit in "Details" on page 489
Status	<p>The current processing state of the message instance</p> <p>Includes this information:</p> <ul style="list-style-type: none"> • The name of the routing point • The name of the last MPF • The result of the process
Instance Priority	See Instance Priority in "Details" on page 489
In Queue Since	The date and time of the message instance entering the queue

Addressee

Field	Description
Institution	<p>The details for the Receiver of the message instance</p> <p>These are the possible details:</p> <ul style="list-style-type: none"> • The BIC-11 address of the Receiver Institution • The name of the Department within the Institution <p>Present only if the Receiver is a department, or an individual within a department</p> <ul style="list-style-type: none"> • The last and first names of the Individual <p>Present only if the Receiver is an individual</p> <ul style="list-style-type: none"> • The details for the Receiver correspondent <p>Present only if available and of the appropriate type</p> <p>These are the possible details:</p> <ul style="list-style-type: none"> – The full name of the Receiver correspondent – The full name of the branch for the Receiver correspondent – The name of the city where the Receiver correspondent is located
Deferred until ⁽¹⁾	The deferred delivery date of a telex message
at ⁽¹⁾	The deferred delivery time of the telex message that the instance is for
Network	The name of the network

Field	Description
Routing code	Free-format text that influences the routing of the message instance For more information, see the System Management Guide .
Disposition address code	The name of the queue that the message instance is transferred to

(1) Applicable only for instances of telex messages restored from archive.

Creation

Field	Description
Appl/Serv	The Alliance application or service that created the message instance
RP & Ft	The Routing Point (RP) and the associated Message Processing Function (Ft) that created the message instance
Date	The creation date of the message instance
Time	The creation time of the message instance

13.4.6.10 Instances Tab: Interventions

Overview

The **Instances** tab can also show the **Interventions List** for an instance that you select from the **Instances List**.

13.4.6.10.1 Interventions List

Content

The **Instances** tab contains these elements:

- Details that relate to the interventions of a message instance
See "Details" on page 489
- Functions that enable you to navigate the **Message Details** area
See "Functions" on page 480

Display

Message Details - IAENTBEDAXXX103RACHELLE WOO

Header Sender/Receiver Text History Instances Other

Instance Description & Comments Interventions

Instance No. 0 - Interventions List Rows in list: 3

Change View

Date/Time	Text
2014/03/24 11:37:46	Routing Instance created, Pacman
2014/03/24 11:37:46	Message Modified Possible Duplicate Message, SYSTEM
2014/03/24 11:37:46	Routing Instance routed, Pacman

Close Previous Next

Close Previous Next

Close

Details

Column	Description
Date/Time	The creation date and time of the intervention

Column	Description
Text	<p>For transmission interventions</p> <p>Includes this information:</p> <ul style="list-style-type: none"> • Network name: for example, SWIFT or APPLI • Session Holder: for example, the logical terminal or message partner profile that established the session during which the message was exchanged with Alliance Access <p>For MX messages, it is one of these:</p> <ul style="list-style-type: none"> – the name of the emission profile (in case of emission) except if the emission profile uses an input channel – the name of the input channel for store-and-forward emission profiles using an input channel – the SWIFTNet Link endpoint (in case of reception) <ul style="list-style-type: none"> • Type: either <code>Emission</code> or <code>Reception</code> • Session Number: the number of the session during which the message was exchanged between Alliance Access and the external network or the message partner • Sequence Number: the sequence number within the communications session specified in the previous field <p>For user interventions</p> <p>Includes this information:</p> <ul style="list-style-type: none"> • Category: always has the value <code>Normal</code> • User intervention name: includes the name of the application, or server which added the user intervention, and the name of the operator that created it

13.4.6.10.2 Instances Tab: Intervention Details

Overview

The **Instances** tab can also show the **Interventions List** for an instance that you select from the **Instances List**.

13.4.6.10.2.1 Intervention Details

Content

The **Instances** tab contains these elements:

- Details that relate to the interventions of a message instance

See "Details" on page 489
- Functions that enable you to navigate the **Message Details** area

See "Functions" on page 480

Display

Details

Intervention Description

Field	Description
Message UUMID	The Unique Message Identifier that the system creates from information in the header and text of the message
Instance No.	The sequence number of the message instance The value is always 0 for the original instance.

Text

Description
Optional information that an application or a user provides when adding a user intervention to a message

Intervention

Field	Description
Name	The name that the system gives to a system or user intervention

Field	Description
Category	<p>The category of the intervention</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Routing • Message as transmitted • Delivery
Operator	<p>The name of the operator that creates and routes the message</p> <p>Operators cannot add interventions directly to a message instance.</p>
Unit	The name of the unit that the message instance is assigned to

Creation

Field	Description
Appl/Serv	The Alliance application or service that created the system or user intervention
RP & Ft	The Routing Point (RP) and the associated Message Processing Function (Ft) that created the system or user intervention
Date	The creation date of the system or user intervention
Time	The creation time of the system or user intervention

13.4.6.11 Message Details Area: Other Tab

Content

The **Other** tab contains these elements:

- Details that relate to the miscellaneous information for a message instance

See "Details" on page 498
- Functions that enable you to navigate the **Message Details** area

See "Functions" on page 480

Display

Message Details - IAENTBEDAXXX103RACHELLE WOO

Header Sender/Receiver Text History Instances Other

Sender to Network Instructions

Priority	Normal	Delivery overdue warning request	No
FIN copy Service	VBB	Network delivery notif. request	No

Sender to Receiver Instructions

Banking Priority
Warning Status

Server to Receiver Instructions

Message Creation

Appl/Server	Messenger Adapter	Routing Point & Function	mpc
Date	2014/03/24	Time	11:37:46
Expiry Date Time	2014/04/13 12:37:46		

Format & Validation

Version	2013	Validation Checked	Minimum
Network Application	FIN	Validation Passed	Maximum

Buttons

Close Previous Next

Details

Sender to Network Instructions / Sender to SWIFTNet Instructions

Field	Description	Sender to Network Instructions	Sender to SWIFTNet Instructions
Priority	<p>The priority of the message</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Normal: the standard priority for a message • System: the priority for SWIFT user-to-system messages (MT0nn) • Urgent: lets the sender communicate the urgency of a message and lets the recipient select the message as a priority when it arrives (MT messages only) 	✓ (1)	✓
Delivery mode	<p>The delivery mode of the message</p> <p>The system extracts the value is from the corresponding MX Message Standard.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Real-time • Store-and-Forward • Empty 	x	✓

Field	Description	Sender to Network Instructions	Sender to SWIFTNet Instructions
Delivery overdue warning request	Indicates whether the sender of the message requests the issue of a non-delivery warning if the message is not delivered at the end of the obsolescence period The SWIFT network uses an MT 010 message to issue this warning. The value of this field is either TRUE or FALSE.	✓ ⁽¹⁾	x
Network delivery notif. request	Indicates whether the sender of the message requests an automatic delivery notification when the message is delivered The SWIFT network uses an MT 011 message to generate this notification. The value of this field is either TRUE or FALSE.	✓ ⁽¹⁾	x
FIN copy Service	The 3-character identifier of the central or clearing institution that Alliance Access sends a copy of the message to, if applicable	✓ ⁽¹⁾	x
User reference	The user-defined reference text	✓ ⁽²⁾	x
Warning status	The warning status, if applicable	✓ ⁽²⁾	x

(1) Present only for MT messages

(2) Present only for MX messages

Sender to Receiver Instructions

Field	Description
User Priority	For MT messages: corresponds to the Banking Priority field in the message header of a message
User Reference	For MT messages: <ul style="list-style-type: none">The 16-character Message User Reference found in the User Header (Block 3) For MX messages: <ul style="list-style-type: none">The RequestRef value
Warning Status	Warning information, if applicable
Server to Receiver Instructions	For MT messages (FINCopy): information added by the central institution for the receiver
Possible Duplicate	For MT messages: used to add a PDE trailer to the message

Message Creation

Field	Description
Appl/Server	The Alliance application or service that created the original message instance
Routing Point & Function	The Routing Point and the associated Message Processing Function that created the original message instance

Field	Description
Date	The creation date of the original message instance
Time	The creation time of the original message instance

Format & Validation

Field	Description
Version	The version number of the Message Syntax Table (MST) that the system uses to validate the message
Network Application	<p>The SWIFT network application</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • LTC: Logical Terminal Control application • APC: Application Control application • FIN: User-to-user Message Control application • SWIFTNet: For MX messages
Validation Checked	<p>The level of validation that the message is checked with</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Minimum • Medium • Maximum
Validation Passed	<p>The level of validation that the message has successfully passed</p> <p>It is possible that the validation process lowers the level of validation for a message. The system still records the message in the Alliance database because it meets the minimum quality grade.</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Minimum • Medium • Maximum • No validation: For invalid MX messages only

SWIFTNet Copy

Field	Description
Copy Requested	Indicates whether a copy was requested (input message)
Authorisation delivery notification request	Indicates whether an authorisation delivery notification is required (input message)

13.4.7 Routing Rule Process

Overview

By default, the first routing rule added is given the number 100, and each subsequent rule added is given a number incremented by 100. For example, if there are three routing rules already created, then these will have the numbers 100, 200 and 300. When you manually create a routing rule, this is given the number 400. The routing rules are applied to the message instances in order of their sequence numbers, from lowest to highest. If you have to activate the routing rules in a different order, then you must duplicate the routing rules in the order required (each can be given a new sequence number), and then delete the originals.

The default routing rule is only applied if no routing rules are assigned to the routing point, or none of the assigned rules are applicable.

When designing new rules, consider all the processing that must be performed at the selected routing point. If an action is performed too early, then it can prevent important processing from occurring later. For example, if the first rule in the sequence is "complete the instance", then none of the other rules in the list are applied. You can also leave gaps in the rule sequence numbering so that other rules can be inserted in the correct order at a later date. For example, instead of numbering the rules 101, 102, 103, and so on, number them with gaps of 100, that is 100, 200, 300, and so on.

Routing rules

Each routing point has a set of routing rules which determine the movement of instances. A routing rule defines the way in which message instances are transformed and moved between routing points.

On top of the routing rules that you can define, each routing point contains a number of system routing rules which are applied before the user routing rules to ensure the proper behaviour of the system. These rules are not visible, not modifiable and only specify non-sensitive actions. Default rules only specify sensitive actions. User rules can specify both.

Each routing point has one default action. This specifies the action which processes the message if none of the user rules is applied.

Overview

Routing rules in one routing point have a sequence number and are executed one after the other (cascading).

Routing rules are triggered by:

- the processing result of the message processing function
- keywords

The routing algorithm ends when a sensitive action is taken on the routed message instance.

There is always one action associated with a routing point, the default action. Hence, each routing point has at least one routing rule. The objective of this default action is to guarantee the consistency in the routing process so that, if none of the defined criteria (attached to the active schema) have been positively evaluated, a consistent action will always be performed. If no rule is evaluated to TRUE and the default action cannot be executed (the instance cannot be routed as specified in the default action) the message will be routed to a routing point named ToBeInvestigated.

From a user point of view it means that a rule is valid if and only if:

- the rule condition is evaluated to TRUE

and

- the instance can enter the routing point specified in the action part if any

A list of allowed targets is defined for each routing point. This list defines the routing points to which routing is allowed or disallowed while routing from this routing point.

A notification or copy instance will not be created if it cannot enter the target routing point.

13.4.8 Add a Queue

Purpose

This procedure enables you to add an exit point or a user-defined queue.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To add or modify an exit point, your operator profile must have the following additional actions:

- **Applic. Interface / Add Exit Point**
- **Applic. Interface / Mod Exit Point**

To add or modify a user-defined queue or modify any type of queue, your operator profile must have the following additional actions:

- **System Management / Add Queue**
- **System Management / Mod Queue**

Procedure

1. From the list of queues, click **Add**.
The **Queue Details** window opens.
2. From the **Configuration** tab, type the name of the exit point or user-defined queue in the **Name** field.
3. In the **Type** drop-down list, select one of the following values:
 - **Exit Point**
 - **User-defined**

4. If you selected **Exit Point** in the **Type** drop-down list, then indicate the following:
 - In the **Processing Order** drop-down list, select **FIFO** or **Priority**.
 - In the **Queue Threshold** field, indicate the number of messages that may be present in the queue before an alarm is generated.
 - In the **Maximum Message Age** field, indicate a maximum message age limit in **Days, Hours, or Minutes**.
 5. From the **Routing Info** tab, select the **Display Routing Rules** and **Allow Modification of Routing Rules** check boxes if you want to display the **Routing Rules** tab and be able to modify routing rules.
 6. Select routing targets from the **Valid Routing Targets/Available** list.
 7. Click **Save**.

A status popup message appears.

If you selected **Display Routing Rules**, the **Routing Rules** tab appears.
 8. Click **Close**.
- You can now modify the default routing and define routing rules.

13.4.9 Define Routing Rules

Purpose

This procedure enables you to define routing rules.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To add, modify, or delete a routing rule, your operator profile must have the following additional actions:

- **Routing / Add Rule**
- **Routing / Def Rule** (to modify the default routing rule of a queue)
- **Routing / Mod Rule** (to modify the routing rules of a queue except the default rule)
- **Routing / Rem Rule**

Prerequisites

If you are defining routing rules attached to the "active" routing schema, then sign on in housekeeping mode. If you are working on a duplicate of the "active" schema, then you can sign on in operational mode.

Procedure

1. From the **Routing Rules** tab of the **Queue Details** window, click **Add**.
The **Routing Rule Details** window opens.
2. Choose carefully the sequence number of the routing rule. For more information, see "How message routing works" on page 443.
3. Make modifications to the **Description**, **Condition**, and **Action** tabs, as required.

See "Specify an Order of Activation and Assign Routing Rules to a Schema (Description Tab)" on page 504, "Define Trigger Conditions (Condition Tab)" on page 504, "Define Routing Actions (Action Tab)" on page 508.

13.4.10 Specify an Order of Activation and Assign Routing Rules to a Schema (Description Tab)

Purpose

In the **Description** tab, you have to specify the "order of activation" of the routing rules for the routing point and assign the rules to routing schemas.

Procedure

1. From the **Description** tab of the **Routing Rule Details** window, specify the following:
 - In the **Sequence Number** field, enter the sequence number of the rule in the routing table.
 - In the **Description** field, enter a description for the rule.
 - In the **Used in Schemas** selection list, select the schemas to which the routing rule is assigned.
2. Click **Save**.
A status popup message appears.
3. You can now fill in the **Condition** tab. "Define Trigger Conditions (Condition Tab)" on page 504

13.4.11 Define Trigger Conditions (Condition Tab)

Purpose

In the **Condition** tab, you can specify conditional criteria that determine whether the rule actions defined in the **Action** tab are to be applied to a message instance.

A conditional statement is a rule criterion based upon a list of approved message attributes called keywords.

Procedure

1. Select one of the following options from the **Condition** tab of the **Routing Rule Details** window, to specify when to perform the routing action:

Option	Result	Next Step
Always	perform the routing action even when the trigger conditions are not matched	Step 4 on page 506
Message	perform the routing action if the message attributes match the conditional statements that are specified in the trigger condition	Step 2 on page 505
Function	perform the routing action if the processing result that the Message Processing Function (MPF) returns matches one of the processing results that is specified in the trigger condition	Step 3 on page 506
Message and Function	perform the routing action if the trigger conditions are matched in either the message or in the function results	Step 2 on page 505

2. If you select **Message** or **Message and Function**, then create one or several conditional statements, as follows:

- a. Click **Add Criteria**.

The **Add Criteria** window opens.

- b. Select the keyword that you require from the **Keyword** drop-down list. For a description of the keywords, see "List of Message Keywords" on page 517.

The keyword that you select controls which operator values are available in the next drop-down list. The keyword also controls whether the value field contains a drop-down list or is a free-text field.

- c. Select the operator that you require from the list of values available in the next drop-down list. See "Relational operators" on page 506.

- d. Select or type the value that you require.

Tip Alliance Access normalises the value of the **Requestor DN** and the **Responder DN** before saving the message in the database.

If you use the **Requestor DN** and the **Responder DN**, then you must also use the normalised values for these DNs when you specify the value of the keyword. To normalise a DN, remove spaces and use only lowercase characters.

- e. Click **OK**.

- f. Use the **AND**, **OR**, **NOT**, **(**, and **)** buttons, if needed for complex conditional statements.

You can also use the "Arithmetic operators" on page 506.

See also "Special characters" on page 506.

The system adds the new criteria in the **Message** field. For example: (Currency = 'EUR') and (Authentication = Invalid_SignDN)

3. If you select Function or Message and Function, then select the routing results from the **Function Result** selection. The Message Processing Function can returns these routing results for a message instance.

A function result of Success means that the transmission was successful (not authentication).

The selected results become trigger conditions for the rule. The routing action is performed if one of the processing results specified in the trigger condition matches the processing result returned by the MPF.

4. Click **Save**.

A status popup message appears.

5. Next, complete the **Action** tab. See "Define Routing Actions (Action Tab)" on page 508

Relational operators

Conditional statements may include the following relational operators:

Relational operator	Purpose
<:	The term to the left of the operator is less than the term to the right
!=	The terms either side of the expression are not equal
>	The term to the left of the operator is greater than the term to the right
<=	The term to the left of the operator is less than or equal to the term to the right
=	The terms either side of the expression are equal
>=	The term to the left of the operator is greater than or equal to the term on the right
like	Find a match between one character string and another. Permitted wildcards are % and _ For example, the statement (Sender like SMBKBEBB%) checks the Sender field of each routed message for a string matching the BIC-12 address "SMBKBEBB%".

Arithmetic operators

Conditional statements may include the following arithmetic operators:

Arithmetic operator	Purpose
+	Add terms either side of the operator
-	Subtract term to the right of the operator from the term on the left
/	Divide the term on the left of the operator by the term on the right
*	Multiply the term on the left of the operator by the term on the right

Special characters

Conditional statements may include the following special characters:

Special characters	Purpose
\n	New line
\r	Carriage return

Special characters	Purpose
\t	Tab
\'	Single quote
\\	Single backslash

13.4.12 Example: Create a Simple Conditional Statement (Condition Tab)

Purpose

In the following example, a conditional statement is created based on the currency and amount attributes of a typical source message.

Procedure

1. From the **Condition** tab of the **Routing Rule Details** window, select one of the following conditions:

- Message
- Message and Function

2. Click **Add Criteria**.

The **Add Criteria** window opens.

3. From the **Keyword** drop-down list, select **Currency**.

4. Select the **=** operator.

5. In the next field, type **GBP**

6. Click **OK**.

The **Add Criteria** window closes.

This part of the expression appears in the **Message** field with quotes automatically inserted.

7. Click **AND**.

The operator appears in the **Message** field.

8. Click **Add Criteria** again.

The **Add Criteria** window opens.

9. Follow steps 3 to 6 to insert an amount this time.

10. Click **OK**.

The **Add Criteria** window closes.

11. Click **Save**.

12. Click **Close**.

13.4.13 Example: Set Precedence in a Statement (Condition Tab)

Overview

By the careful use of parenthesis you can define the precedence in a statement. For instance in the following example:

A OR (B AND C)

will be interpreted by checking first if B AND C is true, after which the result is used in the A OR part.

Changing the location of the parenthesis changes the result entirely, by "forcing" precedence so that A OR B is processed first:

(A OR B) AND C

This gives different results as A OR B is checked first, after which result AND C is checked.

The following example is a little more complex.

(Mesg_type = '530') OR (Mesg_type = '532') OR (Mesg_type = '599')

AND (Sender = 'IRVTBEBEXXX') OR (Sender = 'PARBBEBZXXX')

Here the parenthesis individually force each value assignment to be verified TRUE or FALSE before the OR and AND operators are processed into a result. Can you see the difference between this example and the one below:

((Mesg_type = '530') OR (Mesg_type = '532') OR (Mesg_type = '599')) AND ((Sender = 'IRVTBEBEXXX') OR (Sender = 'PARBBEBZXXX'))

Yes, the double parenthesis - parenthesis can also be nested. In the case of nested parenthesis, the innermost set of parenthesis have precedence. In this example, each '=' assignment in parenthesis is verified to be TRUE or FALSE. The outer set of parenthesis are then evaluated either side of the AND operator. Finally, the two results are then subjected to the AND.

13.4.14 Define Routing Actions (Action Tab)

Purpose

In the **Action** tab, you can specify what actions are triggered when conditional criteria defined in the **Condition** tab are satisfied. An action can be directed towards the source instance or a new instance or both.

Procedure

1. From the **Action** tab of the **Routing Rule Details** window, select one of the following targets:
 - Source
 - New Instance
 - Source and New Instance
2. For actions directed towards the source instance, specify the following:
 - In the **Action** drop-down list, specify the action to be taken on the instance.

- In the **Intervention** drop-down list, specify the type of intervention that you want to append to the instance. If you select **Free Formatted Intervention**, then you can add text in the **Intervention Text** field.
 - In the **Unit** drop-down list, change the unit assignment of the instance.
 - In the **Routing Code** field, specify a routing code. The Routing application adds this routing code to a message instance, when the routing rule is applied.
 - In the **Priority** drop-down list, specify the instance priority.
3. For actions directed towards the new instance, specify the following:
- In the **Type** and **Action** drop-down lists, determine whether the system routes a copy instance or a notification with details about the instance to another routing point or to an addressee.
 - Select a routing point or addressee in the next drop-down list.
 - In the **Intervention** drop-down list, specify the type of intervention that you want to append to the instance. If you select **Free Formatted Intervention**, then you can add text in the **Intervention Text** field.
 - For a copy instance, you can change the unit assignment of the instance in the **Unit** drop-down list.
 - In the **Routing Code** field, specify a routing code.
 - In the **Priority** drop-down list, specify the instance priority.
4. Click **Save**.
- A status popup message appears.
5. Click **Close**.
- The **Routing Rule Details** window closes.

13.4.15 Change the Priority of Message Instances

Purpose

This procedure enables you to change the priority of message instances.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To change the priority of message instances, your operator profile must have the following additional action:

- **Message File / Change priority**

Procedure

1. From the **Monitoring** tab of the **Queue Details** window, click **Show Message Instances**.
The **Message Instances in Queue** window opens.
2. From the **Message Instances in Queue** window, select the check boxes of the instance list entities for which you want to change the priority.
3. Click **Change Priority**.
The **Change Priority** window opens.
4. Select the value that you require from the **Available Priorities** drop-down list.
5. Click **Change**.
A status popup message appears.
The **Change Priority** window closes.
6. Click **Close**.
The **Message Instances in Queue** window closes.
7. Click **Close**.
The **Queue Details** window closes.

The system changes the priority of the selected message instances.

13.4.16 Re-assign Message Instances to a Unit

Purpose

This procedure enables you to re-assign message instances.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To re-assign message instances, your operator profile must have the following additional action:

- **Message File / Re-assign instance**

Procedure

1. From the **Monitoring** tab of the **Queue Details** window, click **Show Message Instances**.

- The **Message Instances in Queue** window opens.
2. From the **Message Instances in Queue** window, select the check boxes of the instance list entities that you want to re-assign.
 3. Click **Re-assign**.
- The **Re-assign Unit** window opens.
4. Select the value that you require from the **Available Units** drop-down list.
 5. Click **Re-assign**.
- A status popup message appears.
- The **Re-assign Unit** window closes.
6. Click **Close**.
- The **Message Instances in Queue** window closes.
7. Click **Close**.
- The **Queue Details** window closes.

The system assigns the selected message instances to the selected unit.

13.4.17 Complete Message Instances

Purpose

This procedure enables you to complete message instances.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To complete message instances, your operator profile must have the following additional action:

- **Message File / Complete instance**

Procedure

1. From the **Monitoring** tab of the **Queue Details** window, click **Show Message Instances**.
- The **Message Instances in Queue** window opens.
2. From the **Message Instances in Queue** window, select the check boxes of the instance list entities that you want to complete.
 3. Click **Complete**.
- The **Complete Confirmation** window opens.

4. Click **OK**.
A status popup message appears.
 5. Click **Close**.
The **Message Instances in Queue** window closes.
 6. Click **Close**.
The **Queue Details** window closes.
- The system completes the selected message instances.

13.4.18 Move Message Instances

Purpose

This procedure enables you to move message instances.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To move message instances, your operator profile must have the following additional action:

- **Message File / Move Instance**

Procedure

1. From the **Monitoring** tab of the **Queue Details** window, click **Show Message Instances**.
The **Message Instances in Queue** window opens.
 2. From the **Message Instances in Queue** window, select the check boxes of the instance list entities that you want to move.
 3. Click **Move to**.
The **Move Instance** window opens.
 4. Select the value that you require from the **Available Routing Point** list.
 5. Click **Move**.
A status popup message appears.
- The **Move Instance** window closes.
6. Click **Close**.
The **Message Instances in Queue** window closes.

7. Click **Close**.

The **Queue Details** window closes.

The system moves the selected message instances to the selected routing point.

13.4.19 Re-activate Completed Message Instances

Purpose

This procedure enables you to reactivate a completed message instances.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To reactivate message instances, your operator profile must have the following additional action:

- **Message File / Re-activate Instance**

Procedure

1. From the **Monitoring** tab of the **Queue Details** window, click **Show Message Instances**.
The **Message Instances in Queue** window opens.
2. From the **Message Instances in Queue** window, click a message instance.
The **Message Details** window opens.
3. From the **Instances** tab of the **Message Details** window, select the check boxes of the instance list entities that you want to reactivate.
4. Click **Re-activate**.
The **Re-activate Instance** window opens.
5. Select the value that you require from the **Target Routing Point** drop-down list.
6. Type a comment in the **Re-activation Comment** field, as required.
7. Click **Re-activate**.
A status popup message appears.
The **Re-activate Instance** window closes.
8. Click **Close**.
The **Message Details** window closes.
9. Click **Close**.

The **Queue Details** window closes.

The system reactivates the selected message instances in the selected routing point.

13.4.20 Generate an Instance Report

Purpose

Alliance Access Configuration allows you to generate a report of instance-specific information of a message retrieved through searching.

Procedure

1. From the **Monitoring** tab of the **Queue Details** window, click **Show Message Instances**.
The **Message Instances in Queue** window opens.
2. From the **Message Instances in Queue** window, click a message instance.
The **Message Details** window opens.
3. Use the check box to select the instance for which you want to generate a report.
4. Click **Instance Report**
5. Select a format from the **Output Format** drop-down list. The formats available are: PDF, XLS, and HTML.

Note **Page Orientation** and **Page Format** are not available in HTML format

6. Select the orientation of the report from the **Page Orientation** drop-down list.
7. Select the page size of the report from the **Page Format** drop-down list.
8. Click **OK**.
If you selected HTML format, then the report is displayed in a new browser window.
If you selected a different format, then a **File Download** window appears. You can then click **Open** to view or **Save** to save the report.
If you click **Open**, then the report automatically opens assuming that you have a tool installed to read PDF, or XLS files.
9. Click **Close** to return to the list of messages.

13.4.21 Hold or Release a Queue

Purpose

This procedure enables you to hold or release a queue.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)

- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To hold or release queues, your operator profile must have one of the following additional actions:

- **Monitoring / Hold Queue**
- **System Management / Hold Queue**

Procedure

1. From the list of queues, select the check boxes for one or several queues in the left column. You can select all the queues by selecting the check box in the column heading line.
2. Depending on the status of the queues, click **Hold** or **Release**.
A status popup message appears.

Note The Hold/Release procedure is only possible for the queues or type of queues specified below.

Exit points:

- FIN traffic sent to the back-office
- MX traffic sent to the back-office
- FileAct traffic sent to the back-office

Message preparation queues:

- _MP_mod_text
- _MP_mod_transmis
- _MP_verification
- _MP_authorisation
- _MP_mod_emi_secu
- _MP_mod_rec_secu
- _MP_mod_reception
- _MP_recovery
- SI_to_SWIFT
- SI_to_SWIFTNet

13.4.22 Delete a Queue

Purpose

This procedure enables you to delete a queue.

Users and permissions

To display the list or the details of queues, or filter the list, your operator profile must have one of these entities or actions:

- **Routing / Open Routing Point** (list)
- **System Management** (list and details in the **Configuration** and **Routing Info** tabs)
- **Applic. Interface / Open/Print Exit Point** (list and details in the **Configuration** tab)
- **Routing / Open Routing Rules** (details in the **Routing Rules** tab)
- **Monitoring** (list and details in the **Monitoring** tab)

To delete an exit point, your operator profile must have the following additional action:

- **Application Interface / Rem Exit Point**

To delete a user-defined queue, your operator profile must have the following additional action:

- **System Management / Rem Queue**

Prerequisites

User-defined queues and exit points can only be deleted if they do not contain any instances and if they are not used by any routing rule.

System queues and ADK queues cannot be deleted.

Procedure

1. From the list of queues, select the check boxes for one or several exit points or queues in the left column.

The **Queue Details** window opens.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

The queue or queues selected are deleted.

13.5 Routing Keywords

Description

Alliance Access provides predefined keywords that operators can use in rules for routing messages. See "List of Message Keywords" on page 517.

You can also define new routing keywords and assign them to fields, or to sub-fields, of specific message types.

13.5.1 List of Message Keywords

Overview

This section contains a list of all default message keywords that can be used to form a conditional statement when creating a routing rule.

Addressee_information

This keyword represents the Server-to-Receiver instructions and allows Alliance Access to route on field 115 of block 3.

The content and the usage of this field depend on the FINCopy service provider.

Addressee_integrated_appl

This keyword represents the name of the network that receives the instance. For example, SWIFT or APPLI.

Warning Do not use this keyword in the routing conditions of the _AI_from_APPLI queue.

Amount

This keyword represents the amount of currency.

The format for representing the amount is: 16 positions to the left of the decimal point (without the thousand separators) and 6 positions to the right of the decimal point:

<16 digits> , <6 digits>

For example, 100000,000

Alliance Access may extract the value of **Amount** from the following fields of the message text: 32A:, 32B:, 32P:, 32R:, 32K:, 34A:, 34B:, or 19. Only the first occurrence of each of these fields is taken into account.

Note When you enter an amount, Alliance Access does not validate the value that you enter.

ack_nack_text

This keyword can be used to filter messages based on the text of the positive or negative acknowledgement.

Note This keyword cannot be used for the _SI_to_SWIFT or _SI_to_SWIFTNet routing points. The message must first be routed to a user-defined queue, or an exit point.

Authentication

When Alliance Access receives a message, it authenticates the message. This keyword represents the result of the authentication and it applies to incoming messages only.

The values are:

- Auth_Failure
- Bypassed
- Invalid_CertID

- Invalid_Digest
- Invalid_SignDN
- Not_Needed
- Sig_Failure
- Success

This keyword can be used for routing FileAct messages.

Authorisation_result

When Alliance Access receives a message, it checks that the message is authorised (if authorisation is required for that message). This keyword represents the result of the authentication and it applies to incoming messages only.

The values are:

- Autho_NotInValidPeriod
- Authorisation_Bypassed
- Authorisation_Failure
- Authorisation_NotEnabled
- Authorisation_NotNeeded
- Authorisation_Success
- No_Authorisation
- Not_authorised

This keyword can be used for routing FileAct messages.

Authorising_operator_name

This keyword represents the username of the operator that authorised the instance.

This keyword can be used for routing FileAct messages.

Banking_priority

This routing keyword allows Alliance Access to route a message on field 113 in block 3.

Business_area

This keyword represents the business area code of an MX or FileAct message.

Checksum

This keyword represents the result of the checksum algorithm for a message that Alliance Access receives. This keyword applies to incoming messages only.

The value is: Chck_Failure.

Class

This keyword represents the class of the message.

The values are:

- Broadcast
- Message
- Template

This keyword can be used for routing FileAct messages.

Copy_recipient_DN

This keyword represents the recipient DN of the SWIFTNet Copy message or file.

This keyword can be used for routing FileAct messages.

Note The value of the DN is not normalised before it is saved in the database.

Copy_state

This keyword represents the state of the SWIFTNet Copy service.

The values are:

- Active
- Bypass
- TCopyFallback

Copy_type

This keyword represents the type of the SWIFTNet Copy.

The values are:

- Full
- Header (only for FileAct)

This keyword can be used for routing FileAct messages.

Creating_application

This keyword represents the application that created the message instance.

This keyword can be used for routing FileAct messages.

Creating_mpfn

This keyword represents the message processing function that created the message instance.

This keyword can be used for routing FileAct messages.

Creating_operator_name

This keyword represents username of the operator that created the message.

This keyword can be used for routing FileAct messages.

Creation_date

This keyword represents the date on which the message instance was created.

The format is DD/MM/YYYY. For example, 22/02/2011.

This format is specific to the Routing and has no relationship with the date format that is defined in System.

This keyword can be used for routing FileAct messages.

Creation_queue

This keyword represents the name of the queue where the message or message instance was created.

This keyword can be used for routing FileAct messages.

Creation_time

This keyword represents the time the message was created.

The format is `HH:MM:SS`. For example, `08:15:30`.

This format is specific to the Routing and has no relationship with the time format that is defined in System.

This keyword can be used for routing FileAct messages.

Currency

This keyword represents the currency that is specified in the message. The ISO currency format is used, for example, `USD`, `GBP`, `EUR`.

Note Alliance Access may extract the **Currency** value from the following fields of the message text: `32A:`, `32B:`, `32P:`, `32R:`, `32K:`, `33A:`, `33K:`, `34A:`, `34B:` and `F68A`

Delivery_requested

This keyword indicates whether a delivery notification was requested. The value of the keyword is either `true` or `false`.

This keyword can be used for routing FileAct messages.

Disposition_address_code

This keyword represents a disposition address code and allows Alliance Access to route messages based on the content of the routing code.

If the configuration parameter **RTV Routing** is set to **ON**, then this keyword automatically takes the value **RTV** for retrieved messages.

Duplicate

This keyword indicates whether a message was received from SWIFT or from a back-office application as a possible duplicate. The possible duplicate information was set externally and received by Alliance Access. This applies to incoming messages only.

The values are:

- **PDE:** Possible Duplicate Emission.

The correspondent adds this trailer to the message.

- **PDR:** Possible Duplicate Reception.

SWIFT adds a Possible Duplicate Message trailer to a message when SWIFT believes that a message delivery has failed. When Alliance Access receives the message, it converts a Possible Duplicate Message to a Possible Duplicate Reception

- **PDE_and_PDR:** Possible duplicate (a combination of PDE/PDR).

Note The keyword is applied only for RJE/DOS formatted messages and not for XML. The keyword "User_duplicate" can be used to route the XML messages.

File_description

This keyword is a string that describes the contents of the payload file. This is a free-text field.

File_info

This keyword is a string that customers can use to provide information about a file. Routing rules can be defined to route FileAct messages based on the content of this field.

File_logical_name

This keyword represents the logical name of the file.

This keyword can be used for routing FileAct messages.

File_size

This keyword represents the size of the file in bytes.

This keyword can be used for routing FileAct messages.

FIN_user_header

This keyword represents the complete FIN User Header (block 3) of an MT message.

You can use this keyword to route messages that are validated through the Sanctions service.

For example, you can configure a routing rule that routes the messages which Sanctions Screening over SWIFT reports as true hits. In this case, the condition must check whether the value of the field 433 contains a true hit, as follows, "%{433:/NOK/%".

Format

This keyword represents the format of the message, for example, Swift.

This keyword can be used for routing FileAct messages.

Full_text

This keyword represents the Message Text (Block 4 for SWIFT format) of a message. This allows Alliance Access to route a message based on the content and the values in a message.

Warning Using this keyword dramatically reduces the overall performance of Alliance Access.

Instance_type

This keyword represents the type of message instance.

The values are:

- Copy
- Notification
- Original

This keyword can be used for routing FileAct messages.

Is_MessageRetrieved

This keyword supports Interact message retrievals by Alliance Access and can be used for FIN and InterAct messages. It exposes the Mesg_is_retrieved message field.

Note The **Disposition_address_code** routing keyword is used for FIN messages only.

Is_verifiable

When set by the Message Management application, this keyword indicates that a deployment package contains one or more verifiable fields.

The value of the keyword is either `true` or `false`.

This keyword can be used for both MX and MT message routing. It exposes the Mesg_needs_verification message field.

Last_operator_name

This keyword represents the username of the operator that last worked with the instance.

This keyword can be used for routing FileAct messages.

LAU_result

When the **Continue on LAU failure** global security configuration parameter is set to **On**, this keyword indicates if a message received from the back office has failed the LAU check.

It is applicable to all types of messages (FIN, InterAct, and FileAct) and configured with the WebSphere MQ connection method.

Live_msg

This keyword represents the distinction between "live" or "test" messages. The value of the keyword is either `true` or `false`.

This keyword can be used for routing FileAct messages.

Mesg_type

This keyword represents the FIN or System message type. Format is `nnn`.

Note No prefix is required, only the message type number must be entered. For example, for an MT 103, enter 103, or for a QUIT message (APDU 05), enter 05.

This keyword can be used for routing FileAct messages.

Message_identifier

This keyword represents the message identifier.

This keyword can be used for routing FileAct messages.

Modifying_operator_name

This keyword represents the username of the last operator that modified the message text.

MUR

This keyword represents the Message User Reference.

MX_keyword_1

This keyword represents the first keyword for an MX message.

MX_keyword_2

This keyword represents the second keyword for an MX message.

MX_keyword_3

This keyword represents the third keyword for an MX message.

NAK_reason

This keyword represents a NAK reason code, which explains why the message was not acknowledged. Alliance Access can perform additional routing based on this keyword, which is applicable to messages sent over the SWIFT network.

Nature

This keyword represents the nature of the message.

The values are:

- Finance: MT 101 to MT 998, MX messages, and FileAct messages
- Network: All System MTs (except MT 05)
- Secure
- Service: MT 05 (QUIT)
- Text: MT 999 messages

Network_application

This keyword represents the SWIFT application that handles the message, for example, FIN, APC, LTC.

This keyword can be used for routing FileAct messages.

Network_delivery_status

This keyword represents delivery status of the message to the network.

For explanations of these codes, see "Structure of the DataPDU" on page 640.

The values are:

- Network_Aborted
- Network_Acked
- Network_N_A
- Network_Nacked

- Network_RejectedLocally
- Network_TimedOut
- Network_WaitingAck

This keyword can be used for routing FileAct messages.

Network_priority

This keyword represents the priority of the message over the network.

The values are:

- System
- Urgent
- Normal

This keyword can be used for routing FileAct messages.

Non_delivery_requested

This keyword indicates whether a Non-Delivery Warning was requested. The value of the keyword is either `true` or `false`.

Pac

This keyword represents the result of the secondary authentication that Alliance Access performs on a message that it receives. This keyword applies to incoming messages only.

The values are:

- Auth_Failure
- Bypassed
- Invalid_CertID
- Invalid_Digest
- Invalid_SignDN
- Not_Needed
- Sig_Failure
- Success

Partial

This keyword indicates whether the message is a partial message. The value of the keyword is either `true` or `false`.

Possible_duplicate

This keyword indicates whether the message has been detected by Alliance Access as a duplicate of another message in the database.

Priority

This keyword represents the priority of the message instance within Alliance Access. The values are 9 (lowest priority) through 0 (highest priority).

This keyword can be used for routing FileAct messages.

Receiver

This keyword represents the full 11-character BIC address (Institution Identifier) of the receiver of the message.

If the message was input to SWIFTNet (Sub-format I), then the receiver is the correspondent to whom the message is being sent. The field contains the correspondent's address.

If the message was output from the SWIFTNet (Sub-format O), then you are the receiver of the message, which was sent by your correspondent to one of your own destinations.

This keyword can be used for routing FileAct messages.

Related_TRN

This keyword represents the related Transaction Reference Number. For SWIFT messages, this is located in field 21 of the message text.

Requestor_DN

This keyword represents the normalised value of the Requestor DN of an MX or FileAct message.

Note Alliance Access normalises the value of the DN before saving it in the database. To normalise the DN, Alliance Access removes spaces and converts all uppercase letters to lowercase.

Responder_DN

This keyword represents the normalised value of the Responder DN of an MX or a FileAct message.

Note Alliance Access normalises the value of the DN before saving it in the database. To normalise the DN, Alliance Access removes spaces and converts all uppercase letters to lowercase.

Routing_code

This keyword represents free-format text to influence routing. The field can be manually filled for a message in the Reception Modification Queue. When the configuration parameter **RTV Routing** is set to OFF, the routing code is automatically set to RTV for a retrieved message.

The routing code has a maximum length of six characters.

This keyword can be used for routing FileAct messages.

RT_SNLL_endpoint

This keyword represents the real-time SWIFTNet Link endpoint. It applies to incoming MX or FileAct messages only.

Sender

This keyword represents the 11-character BIC address (Institution Identifier) of the sender of the message.

If the message was input to the network (Sub-format = "I"), then you are the sender of the message and your own address appears in the field.

If the message was output from the network (Sub-format = "O"), then the sender is the correspondent who sent you the message and the sender address appears in the field.

This keyword can be used for routing FileAct messages.

Sender_reference

This keyword represents the message reference for messages that are entered by APPLI.

This keyword can be used for routing FileAct messages.

Service_name

This keyword represents the SWIFTNet Service to which an MX or FileAct message belongs.

SnF_queue

This keyword represents the name of the store-and-forward queue. This keyword applies to incoming MX or FileAct messages only.

Src_entity

This keyword represents the name of the entity through which Alliance Access received a message from a message partner.

Entity	Value
APPLI network	name of message partner profile
SWIFT network	BIC9 + "XXX" + F (in) or A (apc)

This keyword can be used for routing FileAct messages.

Status

The keyword indicates whether the message is live or completed.

This keyword can be used for routing FileAct messages.

Sub_format

This keyword indicates whether the message was input or output to SWIFTNet after it was created.

The values are:

- Input
- Output

This keyword can be used for routing FileAct messages.

SWIFT_copy_service

This keyword represents the SWIFT copy service identifier (3 characters in length).

SWIFT_receiver_address

This keyword represents the SWIFT address of the receiver (12 characters in length).

SWIFT_sender_address

This keyword represents the SWIFT address of the sender (12 characters in length).

Time

This keyword represents the time of routing.

The format is: HH:MM:SS. For example, 08:15:45.

This format is specific to Routing and has no relationship with the time format specified by the **Display Format** system parameter.

This keyword can be used for routing FileAct messages.

Today

This keyword represents the date of routing.

The format is: DD/MM/YYYY. For example, 20/01/2011.

This format is specific to Routing and has no relationship with the date format specified by the **Display Format** system parameter.

This keyword can be used for routing FileAct messages.

Transfer_description

This keyword is a string that describes the file transfer. This is a free-text field.

Transfer_info

This keyword is a string that customers can use to provide information about a file transfer. Routing rules can be defined to route FileAct messages based on the content of this field.

TRN

This keyword represents the Transaction Reference Number. For SWIFT messages, this is located in field 20 of the message text.

UMID

This keyword represents the Unique Message Identifier.

This keyword can be used for routing FileAct messages.

Unit_name

This keyword represents the name of the unit that owns the message instance.

This keyword can be used for routing FileAct messages.

User_duplicate

This keyword indicates whether a message was locally marked (within Alliance Access, either by means of a manual operation or by the interface) as a possible duplicate. It can be used for routing XML messages. Messages that have been identified as duplicate by Alliance Access are also automatically marked as having been flagged locally as duplicate by the user.

Validation

This keyword represents the validation level that the message passed successfully.

The values are:

- Intermediate
- Maximum

- Minimum

This keyword can be used for routing FileAct messages.

Validation_flag

This keyword represents the Message User Group.

This routing keyword allows Alliance Access to route a message on field 119 in block 3.

For example, it allows Alliance Access to route MT 103, MT 103.STP and MT 103.REMIT in different ways. In this case, the condition on a message can be set to:

```
((Msg_type = '103') and (Validation_flag = 'STP'))
```

Note STP must be entered capital letters for the routing rule to be applied.

This keyword can be used for routing FileAct messages.

Value_date

This keyword represents the date (as a string) on which funds are at the disposal of the receiver.

Note Alliance Access may extract the **Value_date** from fields 32A: or 32B: of the message text.

Value_date2

This keyword represents a date on which funds are at the disposal of the receiver. The format is: DD/MM/YYYY.

This keyword can be used with the variables "yesterday", "today", or "tomorrow" to route messages based on whether the value date in the message is less than, equal to or greater than the date of yesterday, today, or tomorrow.

This format is specific to Routing and has no relationship with the date format specified by the **Display Format** system parameter.

Note Alliance Access may extract the **Value_date2** from fields 32A: or 32B: of the message text.

Verifying_operator_name

This keyword represents the username of the last operator that verified the message.

13.5.2 Routing Keywords Page

Content

The **Routing Keywords** page contains these elements:

- A filtering criterion and filtering functionality that enable you to filter the list entities on the **Routing Keywords** page:
 - See "Details" on page 529
 - See "Functions" on page 22
- Details of the routing keywords defined for the current Alliance Access instance

See "Details" on page 529

- Functions that enable you to manage the routing keywords
- See "Functions" on page 530

Display

Routing Keywords					
Filtering Criteria					
Routing Keywords					
	Change	View	Add	Update	Report
<input type="checkbox"/>	RK1	String	String	1405	
<input type="checkbox"/>	RK2	Amount	Amount	1405	
<input type="checkbox"/>	RK3	Date	Date	1405	
<input type="checkbox"/>	RK4	Integer	Integer		

Details

Column	Description	Filtering criteria
Name	The name of the routing keyword	✓
Description	The description of the routing keyword	
Type	<p>The type of routing keyword</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Amount: format <16 digits>, <6 digits> • Date: format DD/MM/YYYY • Integer: represents any number (without ",") • String: represents any character (ASCII set including CrLf) 	
Syntax Versions	The message syntax table versions that the routing keyword is assigned to	

13.5.3 Routing Keyword Functions

Overview

These functions enable you to manage the routing keywords.

Functions

Function	Description	Routing Keywords page	Routing Keywords Details window
Add	<p>Routing Keywords page:</p> <ul style="list-style-type: none"> Enables you to add a routing keyword <p>Procedure: "Add a Routing Keyword" on page 533</p> <p>Routing Keyword Details window:</p> <ul style="list-style-type: none"> Enables you to add message mapping to the routing keyword that the window currently displays <p>Procedure: "Add a Message Mapping" on page 534</p>	✓	-
Delete	<p>Routing Keywords page:</p> <ul style="list-style-type: none"> Deletes the routing keyword entities currently selected <p>Routing Keyword Details window:</p> <ul style="list-style-type: none"> Deletes the message mapping entities currently selected 	✓	-

13.5.4 Routing Keyword Details Window

Content

The **Routing Keyword Details** window contains these elements:

- Details of the routing keywords
See "Details: General" on page 531
- Details for the message mapping entities
See "Details: Message Mapping" on page 531
- Functions that enable you to manage the routing keywords
See "Routing Keyword Functions" on page 529

Display

Routing Keyword Details

Name: keyword

Description:

Type: String

Mapping to Message

Mapping to Message

Rows in list: 1, in selection: 0

	Syntax Version	Field Tag	Scope
<input type="checkbox"/>	1005	11A	Complete Field

Close **Report** **Previous** **Next**

Details: General

Field	Description
Name	The name of the routing keyword
Description	The description of the routing keyword
Type	See Type in "Details" on page 529

Details: Message Mapping

Routing Keyword Details Window: Message Mapping List

Column	Description
Syntax Version	The message syntax table version
Field Tag	Specifies the field to map to the keyword
Scope	<p>Indicates whether the system maps the keyword to the complete field or to a sub-field of the selected field</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Complete Field • Sub-Field

13.5.5 Message Mapping Details Window

Content

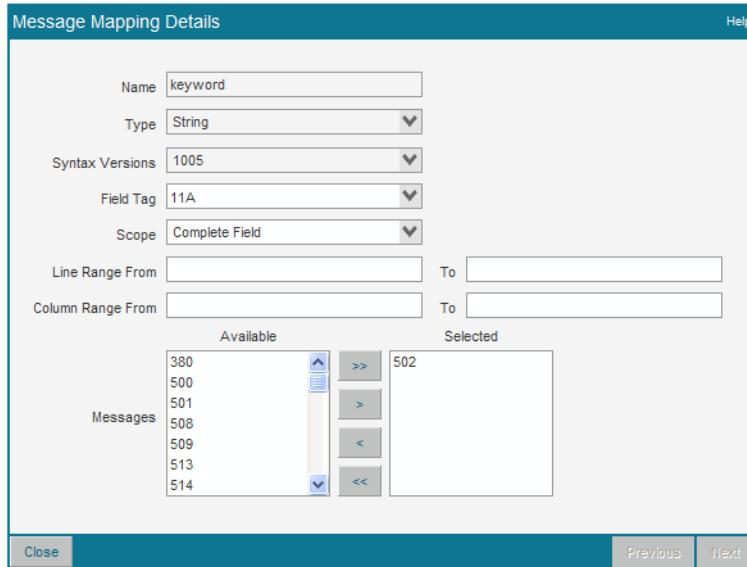
The **Message Mapping Details** window contains these elements:

- Details for the configuration of the message mapping

See "Details" on page 532

- Functions that enable you to manage the routing keyword details

Display



Details

Field	Description
Name	The name of the routing keyword
Type	See Type in "Details" on page 529
Syntax Versions	See Syntax Version in "Details: Message Mapping" on page 531
Field Tag	Specifies the field to map to the keyword
Scope	<p>Determines whether the system maps the keyword to the complete field or to a sub-field of the selected field</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Complete Field: Maps the complete field to the keyword • Sub-Field: If the SWIFT message field has a sub-field, then it is possible to select this value. If you select this value, then an additional field appears that enables you to select a specific sub-field value to map to the keyword.
Line Range From / To	Specifies the line position of where to place the keyword within a field
Column Range From / To	Specifies the column position of where to place the keyword within a field
Messages	<p>In the Available list:</p> <ul style="list-style-type: none"> • The list of SWIFT message types that contain the SWIFT message field and that the keyword is valid for <p>In the Selected list:</p> <ul style="list-style-type: none"> • The SWIFT message types to assign the keyword to

13.5.6 Add a Routing Keyword

Purpose

This procedure enables you to add routing keywords that you can assign (map) to specific field or sub-fields of message types.

Note Routing keywords are dependent on the message syntax table. Each time a new version of the message syntax table is released, you must re-define your routing keywords according to the new version, to map the routing keywords included in the routing rules.

Users and permissions

To display the list or the details of routing keywords, or filter the list, your operator profile must have this entity:

- **Routing**

To add routing keywords, your operator profile must have the following additional action:

- **Routing / Add Keyword**

If you have the **Routing / Mod active schema** action and have initiated a change using Web Platform, any changes you make in operational mode are effective immediately. Otherwise, the changes are effective only at the next Alliance Access restart in operational mode.

Procedure

1. From the list of routing keywords, click **Add**.

You can also add routing keywords using the characteristics of existing routing keywords. Select the check box of a routing keyword and click **Add As**.

The **Routing Keyword Details** window opens.

2. In the **Name** field, type the name of the keyword.
 3. In the **Description** field, type a description. For example, you can describe how the keyword will be used.
 4. In the **Type** drop-down list, select one of the following:
 - **Amount**: with the format <16 digits>, <6 digits>
 - **Date**: with the format DD/MM/YYYY
 - **Integer**: which represents any number (without ",")
 - **String**: which represents any character (ASCII set including CrLf)
 5. Click **Save**.
- A status popup message appears.
6. Click **Close**.
- The **Routing Keyword Details** window closes.

After defining a new routing keyword, the keyword must be assigned to a message syntax table, a message type, a message field, or even a message sub-field.

13.5.7 Add a Message Mapping

Purpose

The routing keywords must be assigned to a specific message syntax table and can also be assigned to fields in specified message types.

This procedure enables you to assign keywords to fields in FIN messages.

Users and permissions

To display the list or the details of routing keywords, or filter the list, your operator profile must have this entity:

- **Routing**

To add a message mapping, your operator profile must have the following additional action:

- **SWIFT Support / Add Keyword**

If you have the **Routing / Mod active schema** action and have initiated a change using Web Platform, any changes you make in operational mode are effective immediately. Otherwise, the changes are effective only at the next Alliance Access restart in operational mode.

Procedure

1. From the list of routing keywords, click the row of a routing keyword.

The **Routing Keyword Details** window opens.

2. Click **Add**.

You can also add mapping using the characteristics of an existing message mapping. Select the check box of a message mapping and click **Add As**.

The **Message Mapping Details** window opens.

3. In the **Syntax Versions** drop-down list, select the required message syntax table version.
4. In the **Field Tag** drop-down list, select the SWIFT message field that is to be mapped to the keyword.

Note You cannot assign a keyword of type **Amount** to a free format text field.

5. To select a sub-field to map to the keyword, select **Sub-Field** in the **Scope** drop-down list. then, select the sub-field in the drop-down list to the right of the **Scope** field.
6. It is also possible to place the keyword in the middle of a field or sub-field by entering the line and column range in the **Line Range From** and **Column Range From** fields.
7. In the **Messages** selection list, select the SWIFT message types which contain the SWIFT message field and for which the keyword is valid.
8. Click **Save**.
A status popup message appears.
9. Click **Close**.
The **Message Mapping Details** window closes.
10. Click **Close**.

The **Routing Keyword Details** window closes.

The routing keyword is not used for routing until the servers have been restarted in operational mode.

13.5.8 Delete a Message Mapping

Purpose

This procedure enables you to delete a message mapping.

Users and permissions

To display the list or the details of routing keywords, or filter the list, your operator profile must have this entity:

- **Routing**

To delete message mappings, your operator profile must have the following additional action:

- **SWIFT Support / Rem Keyword**

Procedure

1. From the list of routing keywords, click the row of a routing keyword.

The **Routing Keyword Details** window opens.

2. Select one or several message mappings.

3. Click **Delete**.

The **Delete Confirmation** window opens.

4. Click **OK**.

A status popup message appears.

5. Click **Close**.

13.5.9 Delete a Routing Keyword

Purpose

This procedure enables you to delete routing keywords.

Users and permissions

To display the list or the details of routing keywords, or filter the list, your operator profile must have this entity:

- **Routing**

To delete routing keywords, your operator profile must have the following additional action:

- **Routing / Rem Keyword**

Procedure

1. From the list of routing keywords, select the check boxes for one or several routing keywords in the left column.

You can select all the routing keywords by selecting the check box in the column heading line.

2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

A status popup message appears.

The routing keyword or routing keywords are deleted.

13.6 Routing Schemas

13.6.1 Routing Schemas Page

Content

The **Routing Schemas** page contains these elements:

- Details of the routing schemas defined for the current Alliance Access instance
See "Details" on page 537
- Functions that enable you to manage the routing schemas
See "Functions" on page 537

Display

Routing Schemas				Rows in list: 1, in selection: 1					
Change View		Add	Clone	Approve	Activate	Delete	Report	Previous	Next
✓	Name	Description			Status				
✓	A	Default schema for basic routing			Active				

Details

Column	Description
Name	The name of the routing schema
Description	The description of the routing schema
Status	<p>The status of the routing schema</p> <p>These are the possible values:</p> <ul style="list-style-type: none"> • Active • Approved • Unapproved

13.6.2 Routing Schema Functions

Overview

These functions enable you to manage the routing schemas.

Functions

Function	Description	Routing Schemas page	Routing Schema Details window
Add	Enables you to add a routing schema Procedure: "Add a Routing Schema" on page 538	✓	x
Clone	Enables you to clone a routing schema Procedure: "Clone a Routing Schema" on page 538	✓	✓
Approve	Approves the unapproved routing schemas currently selected	✓	✓
Activate	Activates the approved routing schema currently selected Sets the previously active routing schema to approved	✓	✓
Delete	Deletes the routing schemas currently selected	✓	x

13.6.3 Routing Schemas Details Window

Content

The **Routing Schemas Details** window contains these elements:

- Details that relate to the routing schemas
See "Details" on page 538
- Functions that enable you to manage the routing schemas
See "Functions" on page 537

Display

The screenshot shows a modal window titled "Routing Schema Details". It contains the following fields and buttons:

- Name:** A text input field containing the character "A".
- Description:** A text input field containing the text "Default schema for basic routing".
- Status:** A dropdown menu showing "Active".
- Buttons:** "Close", "Report", "Clone", "Previous", and "Next".

Details

Field	Description
Name	The name of the routing schema
Description	The description of the routing schema
Status	The status of the routing schema

13.6.4 Add a Routing Schema

Purpose

This procedure enables you to add routing schemas.

Users and permissions

To display the list or the details of routing schemas, your operator profile must have this entity:

- **Routing**

To add routing schemas, your operator profile must have the following additional action:

- **Routing / Add Schema**

Procedure

1. Click **Add**.

The **Routing Schema Details** window opens.

2. In the **Name** field, type a character with a value of A to Z.
3. In the **Description** field, type a description of the routing schema.
4. Click **Save**.

A status popup message appears.

5. Click **Close**.

The **Routing Schema Details** window closes.

You can now assign routing rules to the routing schema.

13.6.5 Clone a Routing Schema

Purpose

This procedure enables you to clone routing schemas.

By "cloning" an existing routing schema, you can modify "active" routing rules without having to restart the servers in housekeeping mode.

Users and permissions

To display the list or the details of routing schemas, your operator profile must have this entity:

- **Routing**

To clone routing schemas, your operator profile must have the following additional action:

- **Routing / Add Schema**

Procedure

1. From the list of routing schemas, select the check box of the routing schema that you want to clone.

2. Click **Clone**.

The **Clone Routing Schema** window opens.

3. In the **Name** field, type a character with a value of A to Z.

4. In the **Description** field, type a description of the routing schema.

5. Click **Clone**.

A status popup message appears.

The **Clone Routing Schema** window closes.

All rules that are used by the source schema are added to the cloned schema.

13.6.6 Approve and Activate a Routing Schema

Purpose

Once the routing rules have been assigned, the routing schema must be approved and then activated. Only routing rules in the "active" routing schema are used to route messages in Alliance Access.

Users and permissions

To display the list or the details of routing schemas, your operator profile must have this entity:

- **Routing**

To approve and activate routing schemas, your operator profile must have these actions:

- **Routing / Approve Schema**
- **Routing / Activate Schema**

Procedure

1. From the list of routing schemas, select the check box for the routing schema that you want to approve in the left column.

2. Click **Approve**.

A status popup message appears.

- The routing schema status changes to **Approved**.
3. Select the check box for the routing schema again.
 4. Click **Activate**.

A status popup message appears.

The routing schema status changes to **Active**.

13.6.7 Delete a Routing Schema

Purpose

This procedure enables you to delete routing schemas.

Users and permissions

To display the list or the details of routing schemas, your operator profile must have this entity:

- **Routing**

To delete routing schemas, your operator profile must have this action:

- **Routing / Rem Schema**

Procedure

1. From the list of routing schemas, select the check boxes for one or several routing schemas in the left column. The active schema cannot be deleted.
2. Click **Delete**.

The **Delete Confirmation** window opens.

3. Click **OK**.

The **Delete Confirmation** window closes.

A status popup message appears.

Appendix A

Integrating Back-office Applications with Alliance Access

A.1 Connection Methods

Introduction

Connection methods define how messages are exchanged between Alliance Access and message partners.

A.1.1 Session Sequence Number

Description

Within each active session that uses one of the following connection methods, Alliance Access assigns a sequence number to each message that it exchanges with the message partner:

- File Transfer
- Interactive
- Print
- SOAP
- WebSphere MQ

Increment the output sequence number across sessions

The operator can specify whether the output sequence number of each transmitted message is reset to 1 at the start of each new sessions, or to continue the sequence over several sessions

For the Print connection method, this helps to verify whether gaps exist in printed output (for example, if the printer has been reset before the message was printed).

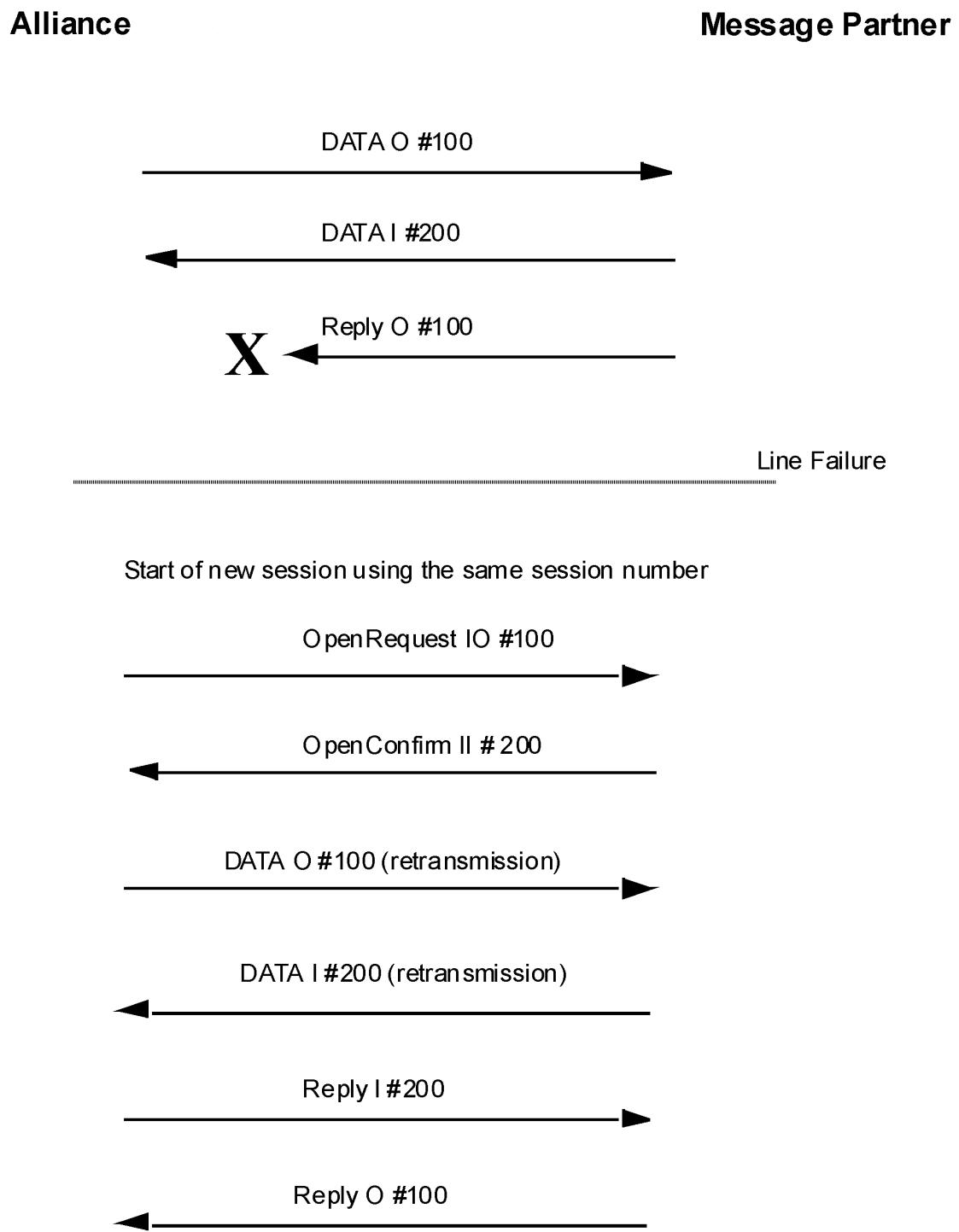
To continue the sequence number across several sessions, select the option **Increment Sequence Number across Sessions** in the in the **Emission** area.

You can only select when **Allowed direction** is set to **To Message Partner** or **To & From Message Partner**.

For Interactive, the sequence number of messages is maintained across sessions. For example, if a session is stopped and restarted the sequence number is not reset to 1.

Example

An example of session sequence number allocation and the recovery process in the Interactive connection method is illustrated in the following diagram:



I # input sequence number
O # output sequence number
II # initial input sequence number
IO # initial output sequence number

A.1.2 Direct FileAct

Overview

This section provides information about the Direct FileAct connection method that you can use to transfer a payload file between Alliance Access and a back-office application.

The core design of the Direct FileAct adapter is a mapping between a directory with a correspondent for a given service. This configuration is primarily suited to handle a limited number of correspondents with a few services, to keep the number of directories to manage under control.

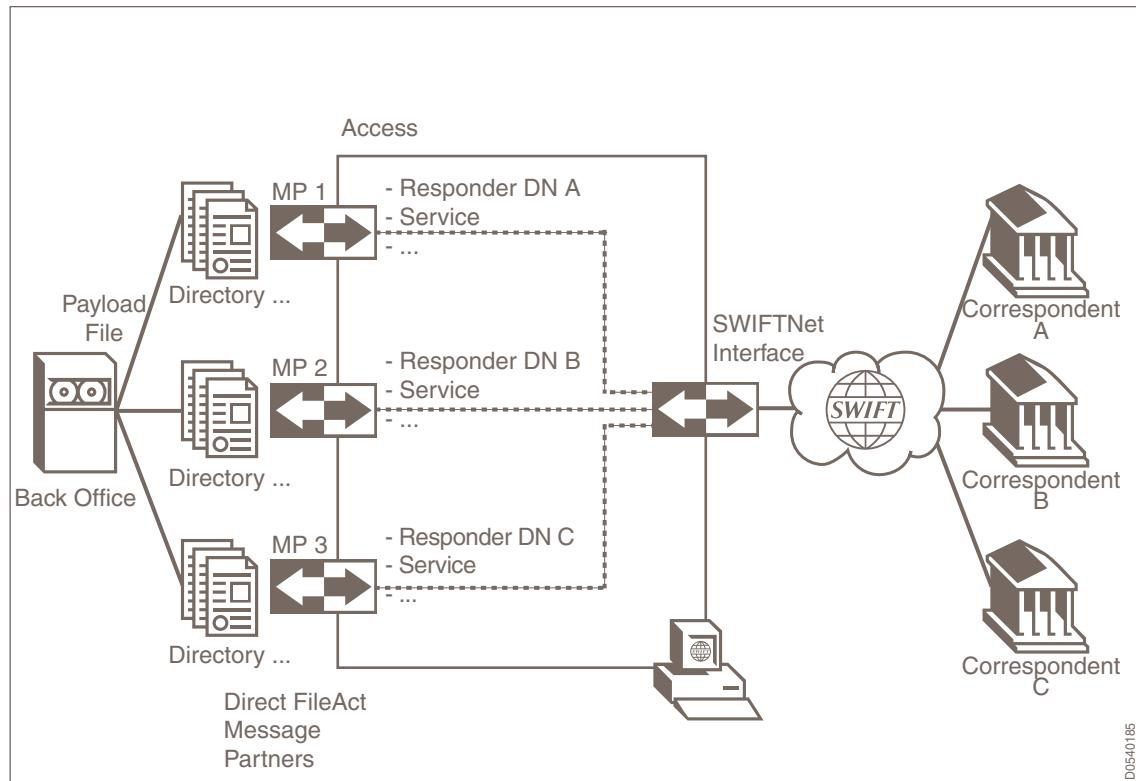
A.1.2.1 Description of Direct FileAct

Direct FileAct

Direct FileAct is an adapter on Alliance Access that enables the transfer of a payload file between Alliance Access and a back-office application. No XML version 2 message or parameter file with FileAct settings accompanies the payload file.

Direct FileAct makes it easy to integrate back-office applications which already produce payload files with Alliance Access because no specific development effort is required to define the transmission parameters in an XML version 2 message. It is intended for use when files are transferred to a limited number of pre-defined correspondents.

Direct FileAct connection method



Configuration of Direct FileAct

A message partner profile with the Direct FileAct connection method must exist for each back-office application and correspondent that will use Direct FileAct to transmit files between each other.

For example, if the back-office application stores a payload file in a pre-configured input directory, then the presence of the file in the directory can automatically start a Direct FileAct session. In this case, Alliance Access determines the FileAct transmission parameters from the message partner that is associate with the directory.

You can define and view a message partner profile for Direct FileAct only through the Alliance Access Configuration package on the Alliance Web Platform.

A Direct FileAct transfer session can be started automatically or manually. For a manual transfer, an operator can manually select the payload file to send to SWIFTNet.

License option on Alliance Access

Use of the Direct FileAct connection method requires the licence package, **22:DIRECT FILEACT**.

A.1.2.2 Features of Direct FileAct

Directory Mapping

The Direct FileAct adapter establishes an association between a set of directories and a FileAct correspondent.

Digest Calculation

Alliance Access calculates the digest of each payload file that it receives from a back-office application and store the digest value in the database.

The configuration parameter, **File: File Digest Algorithm**, specifies the Secure Hash Algorithm (SHA-1 or SHA-256) to use for calculating the digest value.

Duplicate detection

Alliance Access does not verify whether the payload file that a Back Office sends is a duplicate.

However, Alliance Access can detect duplicate FileAct messages based on the file-digest calculation that it applies to an internal File message. The SWIFTNet Interface Component (SNIS) creates an internal message of type File for every Direct FileAct transfer, to help manage the file transfer to and from the back-office application.

Polling Timer

The configuration parameter **Automatic - Polling Timer** controls the frequency at which Alliance Access automatically scans the Direct FileAct Input directories to find files sent from a back-office application.

Notifications of transmission and delivery

For files that are sent from a back-office application to SWIFTNet, Alliance Access provides an empty file of the same name and with an additional extension that indicates the status of a file transmission.

The response file is empty and the back-office application does not need to parse it. Only the extension of the file is relevant. For more information about Direct FileAct response files, see "Direct FileAct Transmission Status" on page 551.

Alliance Access sends delivery notifications only in store-and-forward mode and if specifically requested in the Emission profile associated with the Requestor DN.

No Local Authentication support

The Direct FileAct adapter does not support the configuration of Local Authentication settings to secure payload files that are sent to or received from a back-office application.

If a back-office application requires the payload files to be secured by Local Authentication, then you can use the File Transfer connection method instead.

No File Compression

The Direct FileAct adapter does not compress the payload files.

Maximum file Size

The maximum file size that a back-office application can exchange with Alliance Access is controlled by a configuration parameter, **Message: Maximum File Size**. For more information, see "Message" on page 118.

No T-Copy or Y-Copy support

The Direct FileAct adapter does not support Y-Copy and T-Copy modes. Therefore, you cannot use Direct FileAct for a service for which Y-Copy or T-Copy are defined as mandatory in their Application Service Profiles.

At the start of every Direct FileAct message partner session, Alliance Access checks the associated FileAct service configuration, and stops the session if the service is configured for T-Copy or Y-Copy mode.

Direct FileAct versus File Transfer

The following table gives a summary the difference between Direct FileAct and File Transfer connection methods:

Feature	Direct FileAct	File Transfer
Configuration of bi-directional exchange: Allowed direction parameter set to To & From Message Partner	No	Yes
Manual and automatic start of transfer sessions	Yes	Yes
One directory per correspondent on Alliance Access to hold payload files that the back-office application sends and receives	Yes	Yes
Limited number of correspondents	Yes	No
FileAct transmission settings provided through:		
XML version 2 message that accompanies the payload file	No	Yes
Message partner profile, specific to each correspondent	Yes	No
Selection of the payload file during a manual start of a transfer session	Yes	No
Requires a specific licence package	Yes	No
Requires specification of data formats used to transfer information	No	Yes
Local Authentication setting to secure the payload files	No	Yes
Support of the <code>HeaderInfo</code> element for services that mandate its usage	No	Yes

A.1.2.3 Direct FileAct from the Back Office

Before a file can be transmitted to SWIFTNet

The description of "Emission of a file to SWIFTNet" on page 548 assumes that:

- A "From" message partner with the Direct FileAct connection method has been defined for the back-office application.
 - The data directory where the back-office application will store files for sending to SWIFTNet has been defined and with correct access permissions.
 - The Requestor DN in the SWIFTNet Emission Profile is a valid licensed BIC.
 - The service does not mandate T-Copy or Y-Copy in its Application Service Profiles.

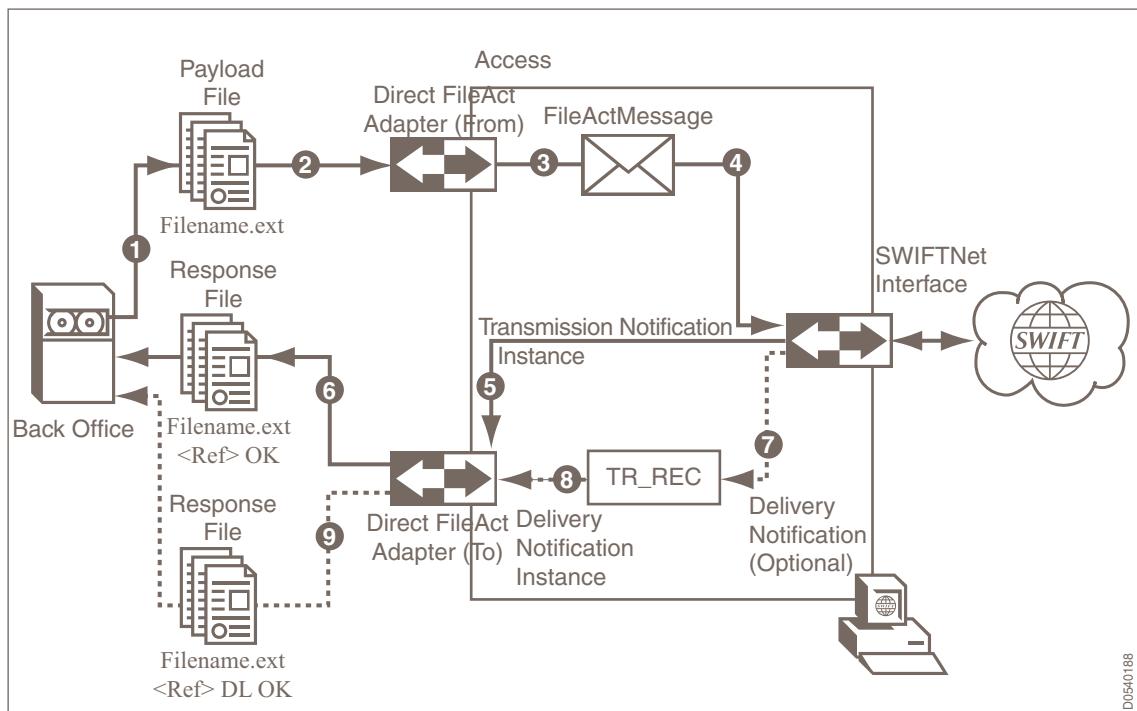
At the start of every Direct FileAct message partner session, Alliance Access checks the associated FileAct service configuration, and stops the session if the service is configured for T-Copy or Y-Copy mode, or if the T-Copy or Y-Copy is mandatory for the Request Type.

- The message partner session for the back-office application is enabled and open.

Direct FileAct - Emission to SWIFTNet

Alliance Access receives a file from a back-office application and sends it to SWIFTNet as follows:

Direct FileAct - Emission to SWIFTNet



Emission of a file to SWIFTNet

Alliance Access receives a file from a back-office application and sends it to SWIFTNet as follows:

1. The back-office application prepares a payload file and stores it in the data directory associated to a Direct FileAct message partner. This directory location is specified in the **Direct FileAct Input Directory** field.

In this example, the file is named **filename.ext**. (See "Direct FileAct - Emission to SWIFTNet" on page 547).

2. The Direct FileAct input Message Partner (Application Interface) automatically detects the file and stores it in the database.

Alliance Access automatically calculates the digest value of the payload file.

The configuration parameter **File Digest Algorithm** specifies which Secure Hash Algorithm (SHA-1 or SHA-256) to use to calculate the digest value.

3. **Creation of the FileAct message**

The Application Interface creates a FileAct-based message for sending over FileAct with the payload file. The File message contains a pointer to the payload file.

The Direct FileAct message partner that is associated with the back-office application provides the following values for the FileAct message:

- **Requestor DN**
- **Responder DN**
- **Service**
- **Request Type**
- **Priority**

The FileAct message is a message of type File, and is the original instance of the FileAct message. As with any other FileAct message, you can view the message in the Message File, print it, route it, and so on.

Tip

You can view the message through the Configuration and Monitoring package on the Alliance Web Platform, but you cannot view the content of the payload file from the web platform.

4. The SWIFTNet emission profile that is associated with the Requestor DN and the Service determines the FileAct transmission parameters:

- **Delivery Mode** (real-time or store-and-forward)
- **Delivery Notification** settings (with corresponding Responder DN, Request Type or Delivery Notification Queue)
- **Non Repudiation Required**
- **Signing Required**
- **Windows Size and Retry Limit**

Alliance Access routes the message according to routing schema that is defined for **_SI_to_SWIFTNet**, and the SWIFTNet Interface application transmits the file to SWIFTNet.

5. After the file is transferred successfully to the SWIFTNet Link (real-time mode) or to the store-and-forward queue of the back office's correspondent, the SWIFTNet Interface application generates a Transmission Notification Instance, which it routes to an exit point in the Application Interface.

This instance is routed to a 'To' message partner that is associated with the back-office application and that does not use the Direct FileAct connection method.

6. The Direct FileAct adapter creates a response file with a file extension that indicates whether the file was transferred successfully to the correspondent.
7. **Store-and-forward mode only:**

If the emission profile requested a delivery notification, then the following also occurs:

- a. The SWIFTNet Interface component receives the Delivery Notification message from SWIFTNet and routes it to the TR_REC module for reconciliation with the original message instance. (Step 7 in "Direct FileAct - Emission to SWIFTNet" on page 547)

TR_REC processes the message and creates a Delivery Notification Instance for the original message. This instance is routed to a 'To' message partner that is associated with the back-office application and that does not use the Direct FileAct connection method. (Step 8 in "Direct FileAct - Emission to SWIFTNet" on page 547)

- b. In addition, the Direct FileAct adapter creates a response file with a file extension that indicates a successful delivery notification. (Step 9 in "Direct FileAct - Emission to SWIFTNet" on page 547)

Tip The response file is empty and the back office does not need to parse it. Only the extension of the file is relevant. For more information about Direct FileAct response files, see "Direct FileAct Transmission Status" on page 551.

A.1.2.4 Direct FileAct to the Back Office

Before a file can be transmitted to Back Office

The description of how Alliance Access handles the emission of a file from a back-office application to SWIFTNet assumes that:

- A "To" message partner with the Direct FileAct connection method has been defined for the back-office application. An exit point is associated with this message partner.
- The data directory where the back-office application will receive files from SWIFTNet has been defined and with correct access permissions.
- The service does not mandate T-Copy or Y-Copy in its Application Service Profiles.

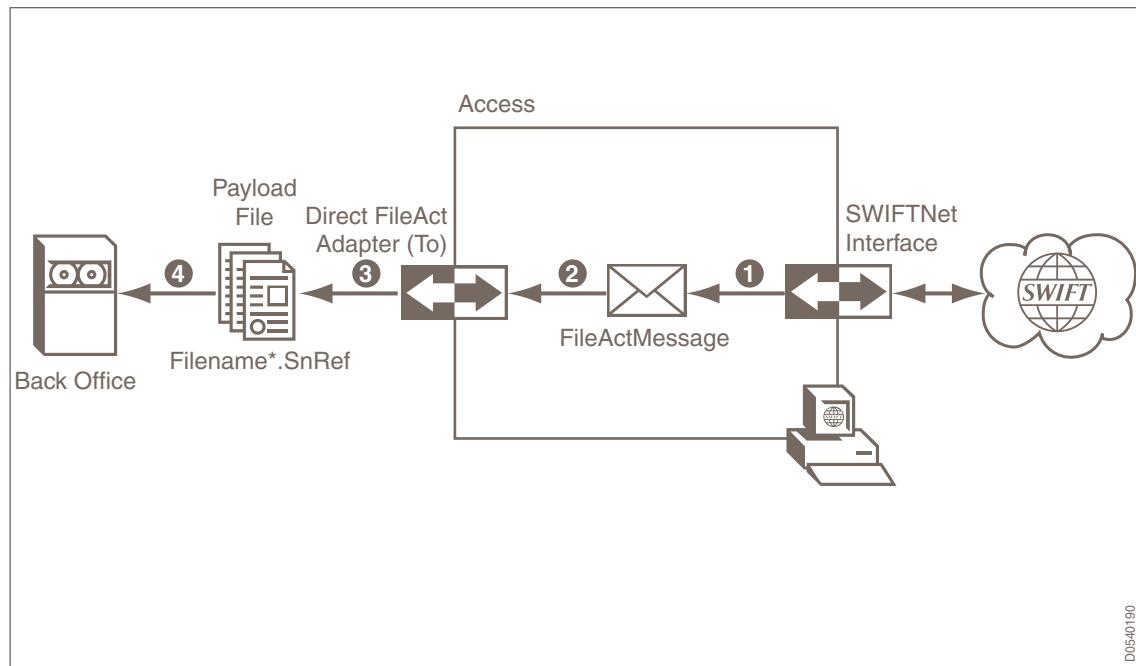
At the start of every Direct FileAct message partner session, Alliance Access checks the associated FileAct service configuration, and stops the session if the service is configured for T-Copy or Y-Copy mode, or if the T-Copy or Y-Copy is mandatory for the Request Type.

- The message partner session for the back-office application is enabled and open.

Direct FileAct - Reception from SWIFTNet

Alliance Access receives a file from SWIFTNet and sends it to a back-office application as follows:

Direct FileAct - Reception from SWIFTNet



D0540190

Reception of a file from SWIFTNet

Alliance Access receives a file from SWIFTNet and sends it to a back-office application as follows:

1. The SWIFTNet Interface in Alliance Access receives a FileAct file-transfer notification from a SWIFTNet Reception profile. The delivery mode for the file transfer is either real-time or store-and-forward.
2. After Alliance Access receives the file successfully, it creates a message of type File, 'File MsgA-0', and routes the message instance to a 'To' Message partner that is associated with the back-office application and has a Direct FileAct connection method.

The FileAct message, File MsgA-0', represents the original instance of the FileAct message. As with any other FileAct message, you can view the message in the Message File, print it, route it, and so on.

3. The Direct FileAct message partner generates a payload file, and stores it in the data directory **Direct FileAct Output Directory**, which is specified in the message partner.
4. The back-office application processes the payload file present in the data directory.

Note No response files are created when files are being sent from SWIFTNet to a back-office application.

Payload filenames

Alliance Access creates a unique filename for a payload file using the logical name of the incoming file from SWIFTNet and the SWIFTNet transfer reference.

The FileAct logical names can contain only the characters **A-Za-z0-9_**. Alliance Access replaces other characters in the logical name of the incoming file with an underscore character, _.

A.1.2.5 Direct FileAct Transmission Status

Direct FileAct response file

For every file that a back-office application sends to SWIFTNet, Alliance Access provides a response file to indicate the status to the file transfer.

The Direct FileAct response file is an empty file of the same name as the original file and only the extension of the response file **.<status>** is relevant. The back-office application does not parse the response files, which makes it easy to integrate the back-office application with Alliance Access.

The information returned by a response file is limited to the network status. It does not contain any additional information (such as detailed authentication information or reason for rejection or delivery notification).

Alliance Access sends delivery notifications only in store-and-forward mode and if specifically requested in the Emission profile associated with the Requestor DN.

In the following table, the original file that a back-office application sent to SWIFTNet is **<filename.ext>**. The name of the response file contains only the characters **A-Za-z0-9_**, and any other character in original filename is replaced by the _ character. Therefore, **<filename.ext*>.<status>** is the resulting file name.

Transmission status

The following table describes the transmission status of a file sent by Direct FileAct:

.<status>	Transmission Status
TransferRef.ok	TransferRef is the reference that SWIFTNet assigned to the initial FileAct Input message from the message partner to SWIFTNet. It is communicated to Alliance Access in the network acknowledgement. .ok indicates a positive network acknowledgement
[TransferRef.]err	TransferRef is the reference that SWIFTNet assigned to the initial FileAct Input message from the message partner to SWIFTNet. .err indicates that it was communicated to Alliance Access in a network negative acknowledgement (NAK). If the transfer fails due to a CUG error, there is no retry and the .err contains the TransferRef. If the transfer fails due to an MRR error, there is a retry and the .err does not contain a TransferRef
SnFRef.dlok	SnFRef is the reference that SWIFTNet assigns to the initial FileAct Input message sent by the sender to SWIFTNet. .dlok indicates that the message was delivered successfully.
SnFRef.dlnok	SnFRef is the reference that SWIFTNet assigns to the initial FileAct Input message sent by the sender to SWIFTNet. .dlnok indicates that the message was not delivered.

Examples

You can view examples of some transmission statuses in the following sections:

- "Direct FileAct from the Back Office" on page 547
- "Direct FileAct to the Back Office" on page 549

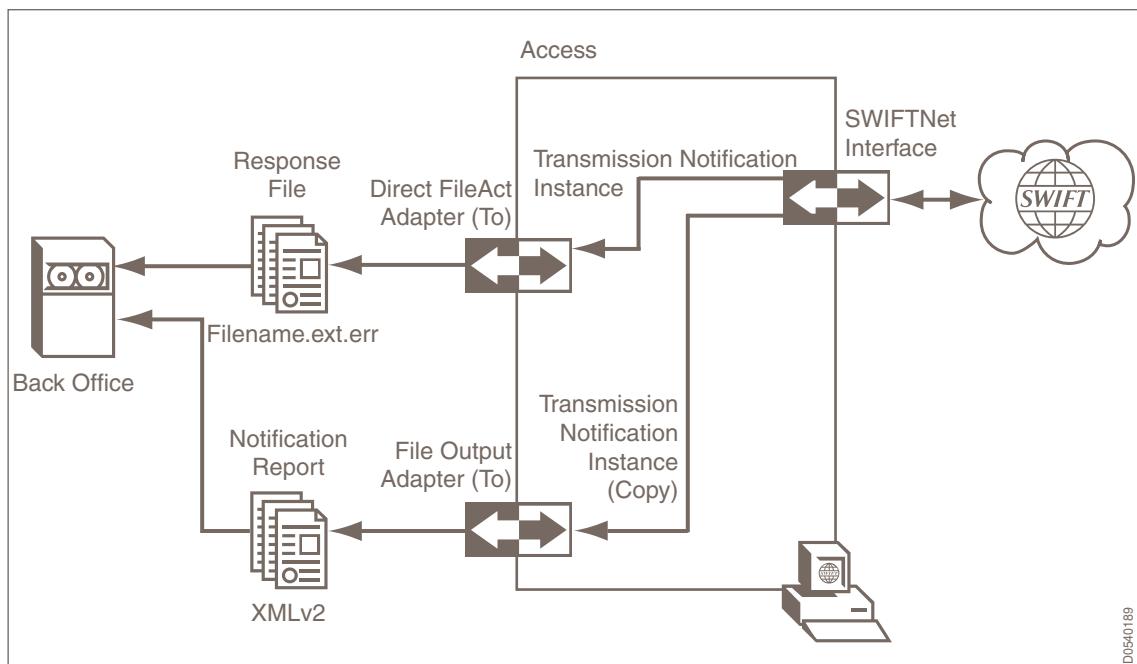
Enhanced transmission status

If a back-office application can support more sophisticated integration logic, it is still possible to generate more detailed notification information.

As shown in "Enhanced transmission status for Direct FileAct" on page 552, it is possible to create an additional copy of the transmission notification instance using the Routing application. To achieve this, you must define routing rules that send the notification copy to a message partner profile that uses the Transfer connection method to the back-office application. When the copy is routed to an exit point associated with the File Transfer message partner, then the Application Interface generates an XML version 2 based notification report that contains the details of the transmission notification.

The same logic can be applied to network delivery notifications.

Enhanced transmission status for Direct FileAct



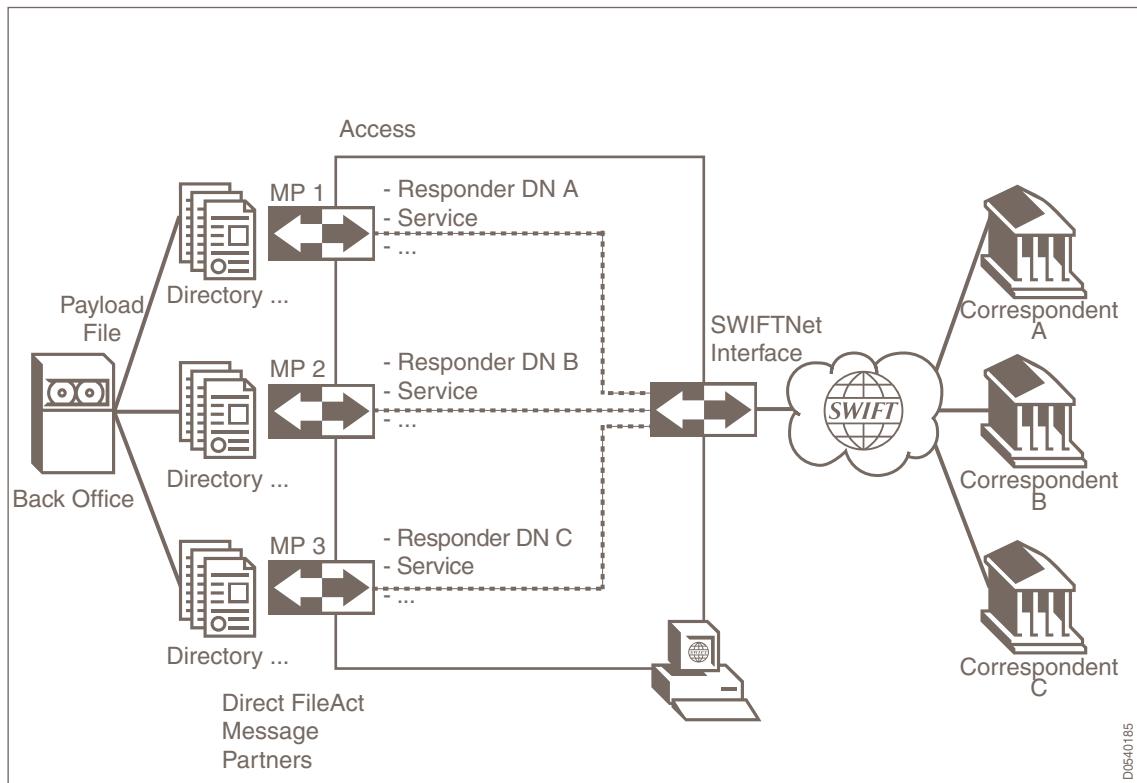
A.1.2.6 Prepare to Use Direct FileAct

Purpose

Use the instructions in this section to prepare Alliance Access to communicate with a back-office application using Direct FileAct.

Directories for Direct FileAct

The Direct FileAct adapter establishes an association between a set of directories and a FileAct correspondent.



T-Copy and Y-Copy

Direct FileAct does not support SWIFTNet T-Copy or Y-Copy services.

Do not set up Direct FileAct for a service for which Y-Copy or T-Copy are defined as mandatory in their Application Service Profiles.

Prepare to use Direct FileAct

On Alliance Access, do the following:

1. Create the directories that Alliance Access will use for transferring files with each back-office correspondent.

Ensure that the directories have correct permissions:

- **Emission from Back Office**

It must be possible to open the **Direct FileAct Input Directory**.

- **Reception at the Back Office**

It must be possible to write to the **Direct FileAct Output Directory**.

2. Configure a message partner profile for each service and for each correspondent that the back-office application will communicate with.

Note that:

- **Emission from Back Office**

For **From Message Partners**, the directory is specified in **Direct FileAct Input Directory**

- **Reception at the Back Office**

For **To Message Partners**, the directory is specified in **Direct FileAct Output Directory** field.

The message partner profile will provide the FileAct transmission parameters for file transfers between the back-office application and the correspondent.

3. Use only valid and licensed BICs as values for **Requestor DN**.

Validate that only Message Partner profiles that have the same **Requestor DN** use the same **Direct FileAct Input Directory**.

4. Verify the settings of the following configuration parameters suit the requirements of the back-office application:

- **File: File Digest Algorithm**

- **Message: Maximum File Size**

5. Transmission Notification and Delivery Notification message instances cannot be routed to a message partner with a Direct FileAct connection method.

If the back-office application expects to receive them, then ensure that a message partner with a connection method that is not Direct FileAct is defined and enabled, to handle notification message instances.

6. Ensure that payload files do not exceed the maximum file size. For more information, see "Message" on page 118.

A.1.3 File Transfer

Overview

This section provides information about the File Transfer Connection method.

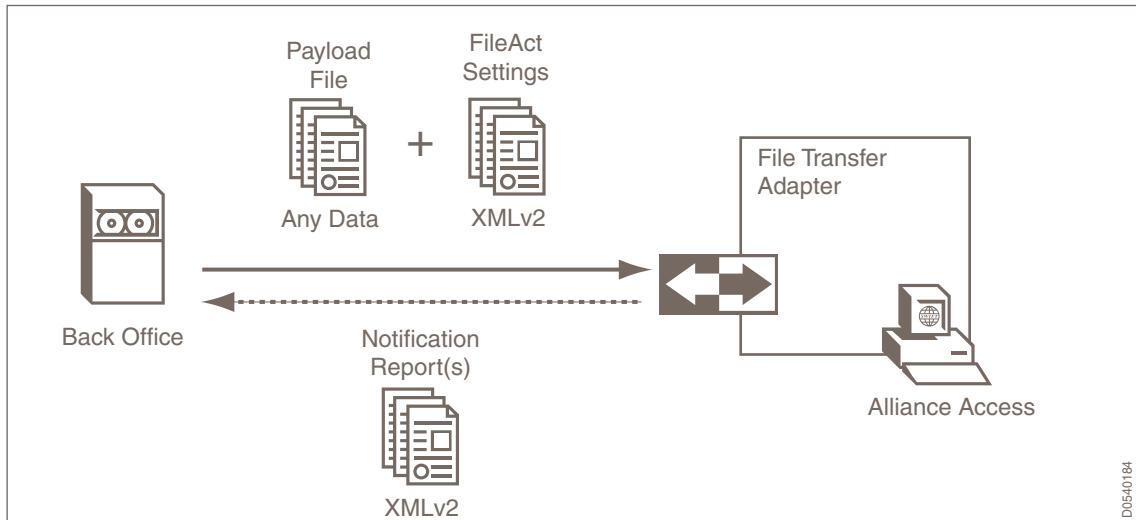
This method differs from the Direct FileAct connection method because this method allows a back-office application to send files to several counterparties without specifying a message partner profile for each counterparty.

For more information about Direct FileAct, see "Direct FileAct" on page 544.

A.1.3.1 Transferring Files using the File Transfer Connection Method

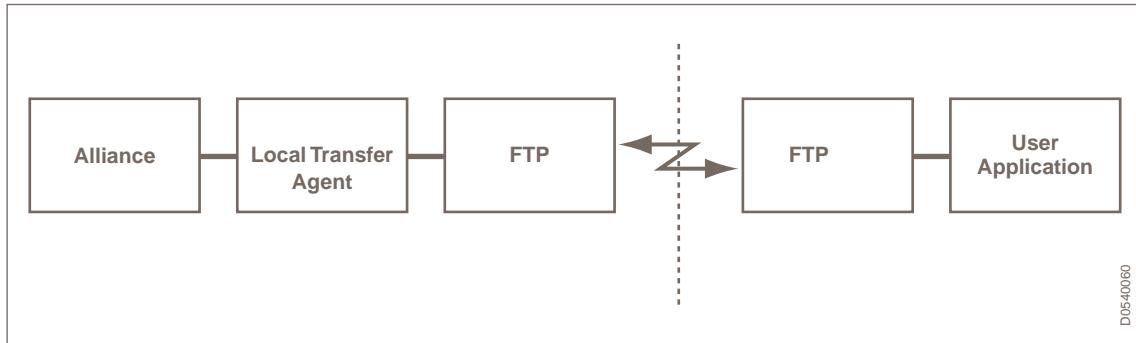
Overview

The File Transfer connection method enables a back-office application to use Alliance Access to exchange files with SWIFTNet. The back-office application provides the transmission parameters for exchanging the file in an XML version 2 message, and in an optional parameter file.



Alliance Access provides to the back-office application the notifications that are related to the file transfer. These notifications are reports in XML version 2, which the back-office application must parse to determine the exact transmission status.

Alliance Access is not responsible for the physical exchange of messages with the message partner. A program known to Alliance Access as the Local Transfer Agent handles this task externally.



The File Transfer connection method supports automated batch input and output sessions.

FileAct headers

The payload of the XML version 2 message specifies the name of the original file to be transferred. It also specifies other elements to manage the transfer, and for some services, these elements may be mandatory. For example, a delivery notification may be mandatory for a particular service or Solution.

The Application Service Profile defines the mandatory elements for a service. You can specify these key mandatory elements for a particular service in the FileAct header which allows the SWIFTNet central systems and the back-office applications that receive these messages to process these elements. For more information about specifying these elements, see the `HeaderInfo` element in "SWIFTNetNetworkInfo" on page 699.

Data Formats for File Transfer

Physically, the connection medium can be either a DOS formatted disk, or a system directory. The File Transfer connection method supports the optional use of parameter files to provide the processing information necessary to each communication session.

The following table lists the available data formats, connection points, and protocols that you can use with the File Transfer connection method:

Data Format	Connection Point	Protocol
DOS PCC (ST200 PCC)	Directory	Batch
RJE (ST200 RJE)	Directory	Batch
CAS 1/2 (NDF/NIF)	Directory	CAS Batch
MERVA/2	Directory	Batch
XML version 1 or 2	Directory	Batch

Manual sessions

When launching a manual File Transfer session, the operator must select the XML v2 file, not the payload file to be transferred.

Tip The Direct FileAct connection method allows you to select a payload file directly, to send to a counterparty.

Automated batch input and output sessions

1. Input from back-office application

A back-office application stores the message file and parameter files in an input directory.

Alliance Access scans the input directory periodically to detect the files. The way the operating system organises the directory structure determines the order in which files are processed.

After Alliance Access detects a suitable file, it starts a communication session to exchange the file.

Tip If files are placed in the input directory at a faster rate than Alliance Access can poll and process them, then a problem may occur. You can avoid this by creating fewer files but each file can contain a larger number of messages and be sent at greater time intervals.

2. Output to a back-office application

For output sessions, the responsibility of Alliance Access ends when the parameter or message file is placed in the output directory.

Alliance Access can launch the Local Transfer Agent automatically if specified. However, what the Local Transfer Agent does with the file lies outside the domain of Alliance Access because it is a user-defined utility.

For more information, see:

- "File Transfer Sessions Without Parameter Files" on page 557
- "File Transfer Sessions with Parameter Files" on page 558

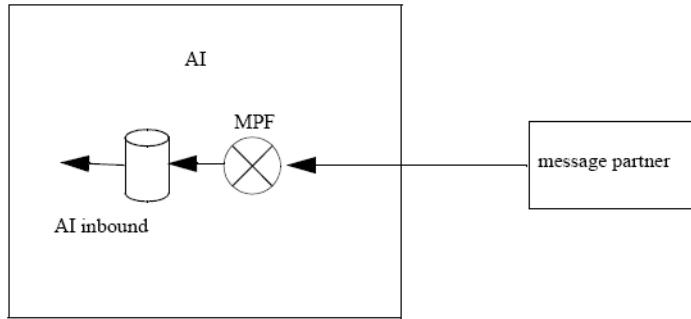
A.1.3.2 File Transfer Sessions Without Parameter Files

Overview

This section describes what happens during batch input sessions to Alliance Access and batch output sessions from Alliance Access when parameter files are not used.

This section relates to the File Transfer connection method.

What Happens During a Batch Input?



From time to time, errors occur during the input of a batch file.

To prepare for such events you can use the **Batch File Validation** button to determine whether the session must be aborted, or whether the session can continue (if the error is not a security issue) when these errors occur.

When **Continue on rejection** is selected, and the message is flagged as modifiable, erroneous messages are passed to the MP_mod_text queue for manual recovery. If the message is flagged as non-modifiable, then the message is completed and a record is made in the Event Journal. When all messages in a batch input session are successfully processed, the session closes normally and the messages are routed.

For information on the procedure followed when messages have input errors, see "Message Validation for RJE, DOS-PCC, and MERVA/2 Messages" on page 761.

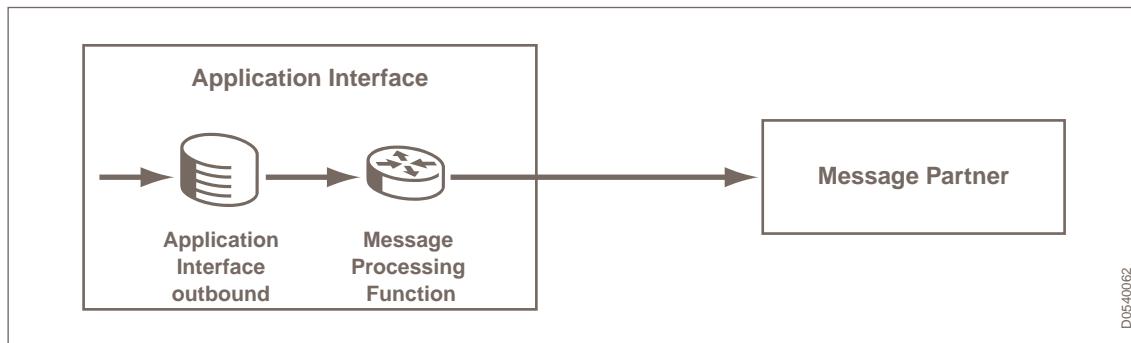
Manual Input Sessions

For manual input sessions, the session is started using the **Start Session** command. The message file is read from the specified directory. From this file, the messages are processed one by one and placed on the AI inbound queue. These messages are held in a reserved state and the session stays open until all messages in the file have been processed.

Automated Input Sessions

The automatic initiation of input sessions is based upon a polling mechanism which scans the input directory for a suitable batch file. If the message partner is currently involved in a session, then the scanning process moves to the next connected message partner, and so on. The duty cycle of the polling mechanism is set using a configuration parameter called "Polling Timer" managed by the System Management application (SMA). For automated file transfer to take place, the software package **16:FILE AUTOMATED** must be licensed on the system.

What Happens During a Batch Output?



D0540062

When started, the batch output process for automated and manual sessions is basically the same in operation. It ensures that each message at the exit point is placed in a reserved state and then copied to an output message file. If all goes well then the messages are removed from the exit point when the file is successfully transferred to the disk. In normal operation, the session remains open and the messages in the exit point remain reserved until the file transfer has been completed.

For automated sessions, the naming convention of the file transfer output file is <internal 4-digit Message partner ID><4-digit Session ID>.<Output file extension, if any>. The session ID will be reset to 0001 automatically only after reaching 9999.

Note For the CAS 1 and 2 formats, messages are taken from any assigned exit points and are encoded according to the network format specified by the message partner profile. They are then sequentially appended to the message file.

Regardless of how the output session was started, the session is closed when the file is transferred to the disk.

If specified in the Message Partner Profile, then the Local Transfer Agent is invoked automatically and the user-defined script is run.

A.1.3.3 File Transfer Sessions with Parameter Files

Overview

This section describes what happens during batch input sessions to Alliance Access and batch output sessions from Alliance Access when parameter files are used.

This section relates to the File Transfer connection method.

Manual Batch Input Session Using a Parameter File

After a manual input session has been activated using the **Start Session** command, File Transfer checks the parameter file specified by the connection point to establish the location of the message data file. The message file is then read. A cyclic redundancy check (CRC) is made and the result stored in the batch history file. The result of the cyclic redundancy check is then checked against a pre-recorded value which was placed in the parameter file when the message file was created. If the check is correct then the session is started.

The decoding is based on the format of the input message. This is established by either an auto-recognition process, or explicitly, depending on the setting for Format Recognition in the message partner profile. From this decoding process, Alliance messages are created and placed on the AI inbound queue.

The stored result of the cyclic redundancy check is also used to check for file duplication. With manual input sessions, you are warned of file duplication errors.

Automated Batch Input Session Using a Parameter File

For automated input sessions started by the input polling mechanism, the **Input path name** field specifies the directory where parameter files can be found. The polling mechanism checks the directory specified in the **Input path name** field at regular intervals. If a file is present and no session is currently active, then the auto-start process starts an input session.

The parameter file is scanned. From information present in this file, the identity of message partner is validated and the message data file is located and checked using the result of the cyclic redundancy check, just as described for manual sessions. If the cyclic redundancy check is successful then the session is started. Each message in the file is read and decoded by the MPF resident at AI inbound queue.

The decoding is based on the format of the input message. This is established by either an auto-recognition process, or explicitly, depending upon the setting for Format Recognition in the message partner profile. From this decoding process, Alliance messages are created and placed on the AI inbound queue.

Following a successful input session the messages are routed and the message and parameter file is moved into the **FTBackup** directory. This directory is specified in the configuration parameter **Batch Input - Automatic Input Backup Directory**.

Manual Batch Output Session Using a Parameter File

Output sessions are invoked manually using the **Start Session** or **Run Session** command. First, the message partner profile is read to obtain the configuration details for the session, this includes the pathname of the parameter file. This pathname dictates where in the file system the message file (and automatically generated parameter file, in the case that no parameter file is specified), is placed after the batch session is complete.

Messages are then taken from any assigned exit points and are encoded according to the network format specified in the message partner profile. They are then sequentially appended to the message file.

When an output batch session is completed, a cyclic redundancy check is generated for the message file and the result is placed in the parameter file.

For all output sessions, the Application Interface provides an interface whereby the Local Transfer Agent can be invoked through user-defined executables. These executables can be programs or scripts which handle the transfer of the parameter and message file (to the remote application) created by File Transfer.

There is a "watchdog" configuration parameter called **LTA_Timeout** which is set in motion after the Local Transfer Agent command is run. If the Local Transfer Agent program has not finished its task at the end of the period set by this parameter, then an event is generated and placed in the Event Journal.

When the Local Transfer Agent has finished its task an event is generated. This happens whether the Local Transfer Agent program was successful or not.

Automated Batch Output Session Using a Parameter File

Automated output sessions can be invoked in two ways:

- By specifying an activation time in 5-minute slots (current date by default)
- By specifying a common queue threshold for the message partner. When this threshold is reached the output session is started.

For automated output sessions, the parameter file and message data file are generated automatically.

When a session is started, messages are taken from any assigned exit points and are encoded according to the network format specified in the message partner profile. They are then sequentially appended to the message file.

The messages are automatically appended with a three character extension specified by the user in the message partner profile. If no extension is given, then the extension **.out** is applied by default.

When an output batch session is completed, a cyclic redundancy check is generated for the message file and the result is placed in the parameter file. The File Transfer application then calls the Local Transfer Agent program to start processing the parameter file and the encoded message file.

For all output sessions, AI provides an interface whereby the Local Transfer Agent can be invoked by means of user-defined executables. The executables can be programs or scripts which handle the transfer of the parameter and message file (to the remote application) created by File Transfer.

There is a "watchdog" configuration parameter called `LTA_Timeout` which is set in motion after the Local Transfer Agent command is run. If the Local Transfer Agent program has not finished its task at the end of the period set by this parameter, then an event is generated and placed in the Event Journal. This feature is activated by setting the configuration parameter `LTA_waiting mode`. When the Local Transfer Agent has finished its task an event is generated. This happens whether the Local Transfer Agent program was successful or not.

A.1.3.4 Summary of Profile Settings

Overview

This section provides an overview of the options that you can set in a message partner profile for the File Transfer connection method.

Note **If you connect to a UNIX or Linux server**

When allowed session direction is set to **To & From Message Partner** and Input file format recognition is set to **Forced**, the Input and Output file format field are combined into a single button labelled **Input & Output File Format**. The restriction to the CAS2 input file format for automated format recognition remains the same.

A.1.3.4.1 From Message Partner

Profile settings

Session Initiation	Parameter File	Format Recognition	Input Path Name	Input File Formats Recognized
Manual	Not required	Forced	Specifies a pathname to an input message file	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN1, Text), XML
Manual	Required	Forced	Specifies a pathname to an input parameter file	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN1), Text, XML
Manual	Not required	Auto-recognition	Specifies a pathname to an input message file	DOS, RJE, MERVA/2, CAS2* (ASN.1), XML

Session Initiation	Parameter File	Format Recognition	Input Path Name	Input File Formats Recognized
Manual	Required	Auto-recognition	Specifies a pathname to an input parameter file	DOS, RJE, MERVA/2, CAS2* (ASN.1), XML
Automatic	Not required	Forced	Specifies a directory where input message files may be found	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN.1, Text), XML
Automatic	Required	Forced	Specifies a directory where input parameter files may be found	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN.1, Text), XML
Automatic	Not required	Auto-recognition	Specifies a directory where input message files may be found	DOS, RJE, MERVA/2, CAS2* (ASN.1), XML
Automatic	Required	Auto-recognition	Specifies a directory where input parameter files may be found	DOS, RJE, MERVA/2, CAS2* (ASN.1), XML

*	CAS1 protocol versions are only recognised when the Format Recognition is set to Forced
---	--

A.1.3.4.2 To Message Partner

Profile settings

Session Initiation	Parameter File	Output Pathname	Data Formats Available	Output File Extension
Manual	Not required	Specifies a pathname where the output message file is placed	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN1, Text), XML	Not required. File pattern in the Output path name is used.
Manual	Required	Specifies a pathname to where the message file and parameter file is placed. If the parameter file is not named explicitly, then it is automatically generated with a proprietary format.	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN1, Text), XML	Not required. The message file takes the file extension, .out , automatically
Automatic	Required	Specifies the directory where the automatically generated parameter and message files are placed	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN1, Text), XML	Specify the extension of the message file. If not specified, then the default extension .out is taken. Any pattern specified in the Output path name is ignored.
Automatic	Not required	Specifies a directory where the generated message file is placed	DOS, RJE, MERVA/2, CAS1, CAS2 (ASN1, Text), XML	Specify the extension of the message file. If not specified, then the default extension .out is taken. Any pattern specified in the Output path name is ignored.

A.1.3.5 Checking for Message File Duplication

On input message files

The result of the Cyclic Redundancy Check on each input message file received by Alliance Access is kept in a batch history file. The Cyclic Redundancy Check value is the result of a mathematical function applied to the sum of the file contents and, with the file name, uniquely identifies the file to the input session.

Each time the system processes an incoming message file, a check is made between the Cyclic Redundancy Check of the message file and the batch history file. If a match is found, then the system alerts the operator of a possible duplication, thus preventing processing and routing the same set of messages more than once.

If a match in the Cyclic Redundancy Check of a batch file is found, then a prompt is issued:

"This batch file has already been used. Do you want to re-use it?"

If the operator decides to proceed with the session in spite of a duplication warning, then a Possible Duplicate Emission is added automatically.

In addition to a record of Cyclic Redundancy Check calculations, the system also keeps a record of message file names. If no Cyclic Redundancy Check match is found, then a secondary check on used message file names is carried out. If a match on file name is found, then the same warning prompt "This batch file has already been used. Do you want to re-use it?" is issued.

The length of time that a record is kept of message file names is set by the configuration parameter **Batch Input - History Period**. For more information about this configuration parameter, see "Batch Input" on page 113.

On output message files

For output message files, a check is made to see whether the message file exists on the target directory.

If a match on file name is found, then the warning prompt "File <filename> already exists, do you want to overwrite" is issued.

If the operator decides to proceed with the session in spite of a duplication warning, then any matching file in the target directory is overwritten.

A.1.3.6 Recovery of Batch Sessions

Batch output

An output message partner configured with connection method set to File Transfer writes the messages to a file. If anything goes wrong with the session, then the recovery mechanism unreserves and requeues the messages at the exit point. An event concerning the session failure is recorded in the Event Journal.

Batch input

An input message partner configured with connection method set to File Transfer reads the messages from a file.

With batch input sessions, the session operation and recovery principle is very similar. If anything goes wrong with the session, then the recovery mechanism unreserves, removes, and discards the messages in the AI inbound queue.

Automatic sessions

If an error occurs, then the batch input message file is moved into a storage location known as the Automatic Input Error Directory (set by the system parameter **Automatic - Error Dir**).

If a parameter file is being used, then the parameter file is moved into this Error Directory. If the message file and parameter file are located in the same connection point directory, then both are moved into the Error Directory.

To avoid filename clashes, each file placed in the Error Directory is given a file extension **YYMMDDHHMMSS**.

An event concerning the reason for the session failure is recorded in the Event Log.

A.1.4 Interactive

Overview

The Interactive connection method is used to transfer messages of a specified format between Alliance Access and a message partner. This transfer is carried out according to Common Application Server (CAS) standards. For more information about CAS, see "CAS Protocol" on page 563.

The Interactive connection method permits message transfer in the following directions:

- To message partner
- From message partner
- To and from message partner

Depending upon a setting of the message partner profile, permission to start a session can be granted specifically to Alliance Access or to the message partner, or to both parties.

Sessions can be stopped or aborted at any time by either party.

Protocol for Interactive connection method

The protocol for the Interactive connection method currently supported in Alliance Access is:

- TCP/IP: Transmission Control Protocol/Internet Protocol

A.1.4.1 CAS Protocol

Overview

As part of the Application Interface (AI), Alliance Access supports CAS protocol standards 1 and 2.

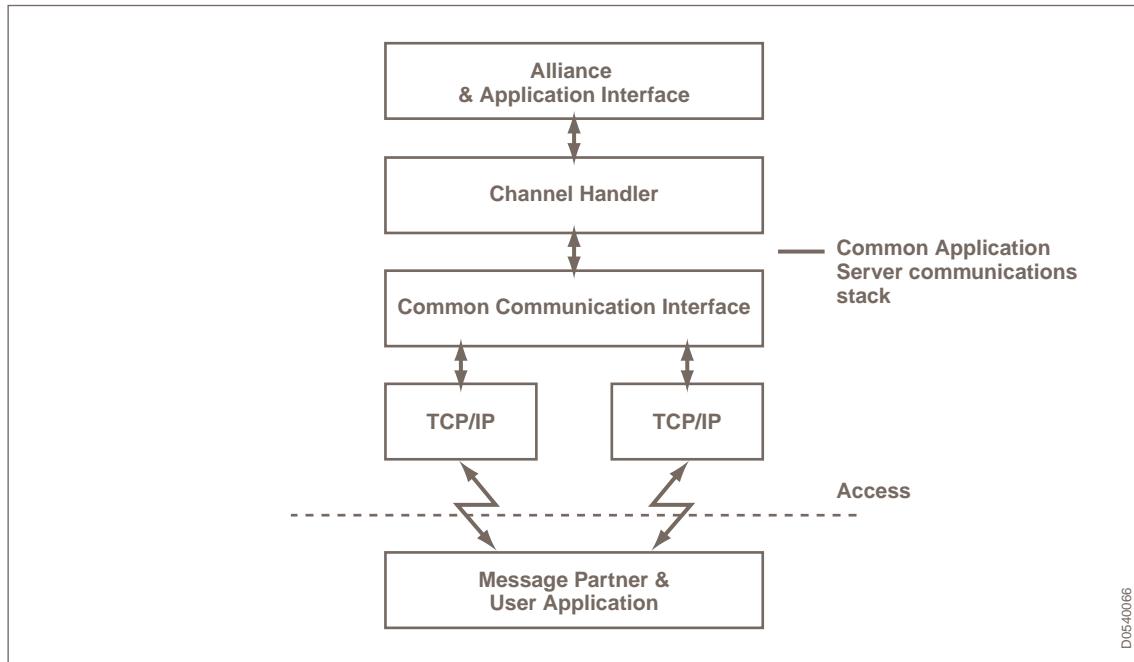
Both these CAS protocols provide a common form of access between SWIFT terminal products (CBTs) and back-office mainframe applications. In addition, use of the CAS protocol permits Alliance Access to store messages that it receives from networks other than SWIFT. Therefore, messages that use protocols other than SWIFT can be processed and "*switched*" through Alliance Access like calls through a telephone exchange.

CAS protocol

The Common Communication Interface (CCI) together with the channel handler and protocol units, are known as the CAS communications stack. Together they are responsible for providing transparent and reliable communications between AI and a message partner.

The channel handler is responsible for taking messages received from the network protocols by means of the CCI, and delivering them one at a time (in the correct format) to AI. It also provides a service in the reverse direction, that is, taking messages from AI and presenting them one at a time to the CCI.

The CCI is a software module which provides a "common transport interface". This interface handles messages to and from the underlying communication protocols. The communication protocols are the software programs which carry the messages across the network.



A relevant message partner profile defines which protocol is used for a communication session using CAS.

Message format

Alliance Access accepts a message that is transmitted using the CAS protocol if it has one of the following formats:

- **Network Dependent Format (NDF)**

This format matches the SWIFT network.

Using the NDF format, financial institutions currently communicating with ST400 systems can re-use much of their CAS application software when switching to Alliance Access.

- **Network Independent Format (NIF)**

With NIF, the body of the message is limited to the financial data, that is, block 4 of the SWIFT message format, while the network-related information is in a network independent format.

Using the NIF syntax permits financial institutions to use Alliance Access to exchange and process messages which are coming from SWIFT or non-SWIFT networks, for example, CHIPS, CHAPS, Fedwire, SIC, and so on.

Network Format	NDF	NIF
SWIFT	Message Syntax Table	Message Syntax Table
UNIX or Linux only:	-	UFS (User Format Services)

Network Format	NDF	NIF
Sic		
UNIX or Linux only: Other networks	-	UFS

Message encoding and decoding

The NDF/NIF formats are defined using the ISO standard Abstract Syntax Notation 1 (ASN.1). Its companion the Basic Encoding Rules (BER) Standard defines how data described using ASN.1 can be exchanged using a common transfer syntax.

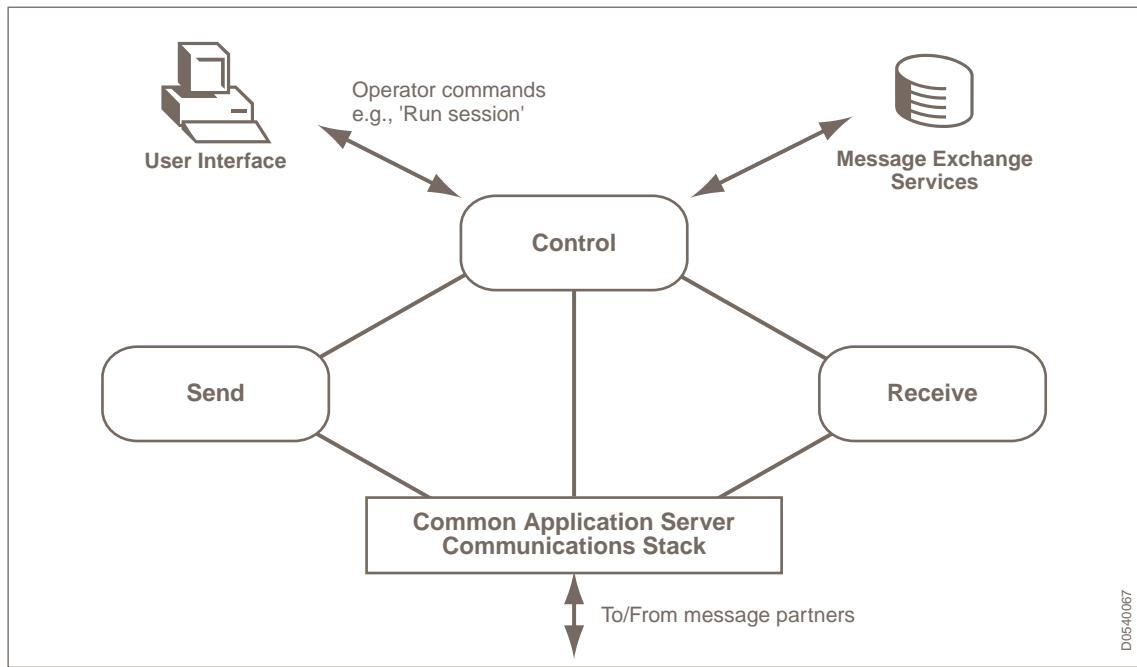
The messages exchanged between Alliance Access and message partners are encoded to the common transfer syntax for transmission, and from the common transfer syntax on reception.

In addition to the ASN.1 notation used by both CAS 1 and CAS 2 standards, the CAS 2 standard also supports a notation called Text Encoding. This notation has been developed to simplify the implementation of the CAS protocol. The structure and parameters of the CAS protocol remain unchanged, but the text encoding method uses special text characters to delimit the start and end of each structure block and field within the message.

A.1.4.2 What Happens During an Interactive Session?

Overview

For Interactive communications, there are three important transmission modules within the Application Interface: Control, Send, and Receive. These modules handle messages that are sent to and from the CAS communications stack.



- **Send:** assembles the message and passes the message to the channel handler.
- **Receive:** validates and routes the received message. The Receive module is also responsible for sending logical replies to the message partner.

- **Control:** is responsible for interaction with the operator by means of the GUI, and for the following operations:
 - for opening and closing the session
 - listening to the line after a message partner is enabled
 - managing a session abort.

Send Messages

During an interactive session with a message partner, messages are sent one at a time by the Send module to the message partner through the CAS communications stack. A logical reply is relayed to the sender, and another message can then be sent to the message partner.

If the message exchange session is using a messaging window value of greater than 1, then the message partner can transmit this number of messages before having to wait for a reply.

If the session was started with the **Start Session** command, then the session remains open and messages arriving at the exit point(s) are queued and transmitted straight away. The session stays open until:

- either Alliance Access or the message partner issues the **Stop Session** command
- the session fails
- either Alliance Access or the message partner aborts the session.

If the session was started with the **Run Session** command (to message partner only), the session remains open until:

- all messages present in the exit points at run time have been sent to the message partner
- either Alliance Access or the message partner issues the **Stop Session** command
- the session fails
- either Alliance Access or the message partner aborts the session.

Receive Messages

During an interactive session with a message partner, messages are received one at a time by the Receive module through the CAS communications stack. As the Receive module receives each message, a validation and a local authentication check can be made. If the message passes the required validation level, then Base Services accepts the message, and a positive reply is generated and sent to the message partner by the Receive module. The message partner can then send another message.

If the message fails the required validation level then it is rejected with a negative reply and a record of the event is written in the Event Journal. The message is either `routed to _MP_mod_text` or `completed`, depending on the parameter "Message Modification Allowed Yes/No". If the message fails the local authentication check, then the session is aborted.

The session is started with the **Start Session** command and remains open until:

- either Alliance Access or the message partner issues the **Stop Session** command
- the session fails
- either Alliance Access or the message partner aborts the session.

The session is terminated using the **Stop Session** command.

Note	During an interactive session, flow in either direction may be handled.
-------------	---

A.1.4.3 How are Interactive Sessions Handled?

Overview

Interactive sessions are opened, closed, and aborted by means of requests from either the Alliance Access operator or the back-office application.

Example (for an Interactive Messaging Window Size = 1)

Take for example an Alliance Access operator issuing the **Run Session** command. In this example, two messages are sent to the message partner.

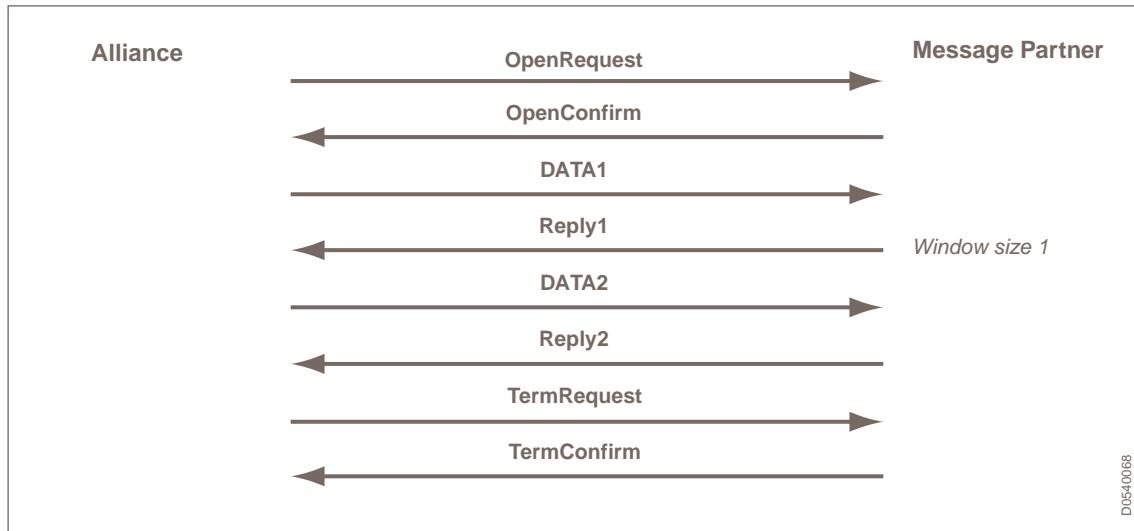
The operator selects the **Run Session** command and Alliance Access sends an event "Run Session" to the Control module. The Control module reads the message partner details from the Message Exchange Services (MXS) and then sends an event to the channel handler. The channel handler then attempts to open a session with the equivalent message partner session layer by communicating an **OpenRequest**.

If the message partner recognises the request, then it responds with an **OpenConfirm**. The session is now open.

When the session is open, the Send module examines all exit points assigned to the message partner and begins transmitting the first queued message to the message partner (DATA1).

Upon receipt of a positive reply (Reply1), the next message can be sent (DATA2).

When the last reply (Reply2) has been received, the channel handler issues a **TermRequest** across the connection to close the session. The message partner responds with a **TermConfirm** and the session is closed.



Interactive Messaging Window Size

By setting the field **Window Size**, the sender can transmit a set number of messages before receiving a reply. For example, if the window size is set to 5, then five messages may be sent sequentially to the receiver before a reply on the first message is required (if the operator opened the session).

The requested window size is given by the initiating message partner in the `OpenRequest` SPDU. The corresponding message partner confirms the window size (or a lower value in some cases) within the `OpenConfirm` SPDU.

Logical replies are relayed to the sender in the same sequence that they are received.

Recovery Mechanisms

For a description of the recovery mechanisms used by the Interactive method in case of failure, see "Interactive Sessions" on page 568.

If a session is aborted when a window size of more than 1 is implemented, then the receiver must discard any messages that the sender sent but which the receiver has not processed. This applies directly to messages which have not yet received a logical reply.

Message validation and disposition

For information about the disposition of CAS messages after arriving in Alliance Access, see "Message Validation and Disposition" on page 758. This section addresses various fields present in the Data APDU, and the entitlements that the message partner permission profile possesses.

A.1.4.4 Interactive Sessions

Description

Session recovery for interactive sessions involves restarting the session using the same session number as the failed session.

Session recovery begins by transmitting an `OpenRequest` SPDU. Either party can send the SPDU and it contains:

- The sequence number (incremented by one) of its last fully transmitted and acknowledged message
- The session number used for the recovered session. This is always the sequence number of the failed session
- A software flag **recoveryIndication = TRUE** indicating that this is a recovery request.

The other side replies with an `OpenConfirm` SPDU. This SPDU includes the input sequence number (incremented by one), of its last fully transmitted and acknowledged message from that side.

Scenario

During the transmission of a message to a message partner, the session is aborted before Alliance Access receives the logical reply. After the session is closed, the operator moves the message to a different exit point. Then, Alliance Access re-opens the session. In such cases, Alliance Access sends the message to the message partner even though the exit point to which the message has been "moved" is no longer assigned to the message partner.

Note for UNIX or Linux: connection problems arising when using TCP/IP protocol

The following error messages appear when a TCP/IP error occurs. Exactly which message depends on which of the following files is out of configuration:

- protocol file
- services file
- hosts file

problem in protocols file:

```
Message Partner <message partner name>
    - TCP connection error
```

Reason:

Could not obtain protocol number for protocol name TCP.

Failed to initiate communication.

problem in services file:

```
Message Partner <message partner name>
    - TCP connection error
```

Reason :

Unable to find service name MPconn...

Failed to initiate communication.

problem in hosts file :

```
Message Partner <message partner name>
    - TCP connection error
```

Reason : Unable to get host information for host name <host name>

Failed to initiate communication.

To get the relevant information about the error message, look into the Event Journal for the event.

TCP_connection error

reason: description of the problem.

reason can be :

-Could not obtain protocol number from protocol name: protocol name

-Unable to find service name : service name

-Unable to get host information for host name : hostname.

In all cases, use the help of the system administrator to resolve the problem.

A.1.5 Print

Overview

This section provides information about the Print connection method that you can use to print messages in batch to a printer or file.

A.1.5.1 Description of the Print Connection Method

Overview

The Print connection method permits the output of messages in batch to a specified printer or to a file in a user specified directory.

The definition of the paper size, font, font size, margins, and, optionally, paper orientation, for the selected printer can be made from the System entity. Additionally, to save paper usage, notifications can be printed to the output device without including interventions.

Output messages can also be printed in ST200-like format, which can also include warning indications, or eye-catchers, in the header of the output. For information about the format of the message report after the messages are printed, see "Printed Message Reports" on page 570.

Print Sessions

A print session can only have one allowed direction, To Message Partner.

An operator can start a print session either automatically or manually using the **Start Session** or **Run Session** command.

Messages are not printed until the operator stops the session because the printer spool job is not actually queued until the print session is closed.

On UNIX or Linux only: to recover from problems incurred during a Print session, for example, a paper jam, toner low, and so on, the system administrator may be required to resubmit the spool job manually.

A.1.5.2 Printed Message Reports

Introduction

Printed message reports are generated when a message is routed to a Print message partner, or when messages are printed on demand.

You can print messages on demand by selecting the **Print Instance** option in Message Management.

Report content

The report for a message instance consists of the following sections:

- Warning header
- Transmission section
- Message Header section
- Message Text section
- Message Trailer section
- Intervention section

Each message starts on a new page.

The page header includes date and time information, as well as the name of the message partner and its session and sequence number. The report indicates that the information is a reprint and thus the values for session and sequence number are all zero.

The configuration parameters of the classes **Print** and **Display/Print** influence the content of the printed report. For more information, see "Classes of Configuration Parameters" on page 111.

Eye-catcher text

When printing in ST200-like format, a warning identification, which is called eye-catcher text, indicates an exceptional condition.

Note Eye-catchers are not printed when the option for printing to a file is used.

The eye-catcher codes in the following table are shown in order of preference. This means that if more than one condition applies, then only the eye-catcher that is related to the first condition is printed:

Eye-catcher	Text	Condition
NAK	NAK'd message.	Message is an input message, the delivery status is Not Acknowledged (NAK).
SAI	Authentication and/or authorisation incorrect.	Message is an output message, the message authentication and/or authorisation verification failed.
SAB	Authentication and/or authorisation bypassed.	Message is an output message, the authentication and/or authorisation were bypassed.
FAI	FINCopy Authentication incorrect.	Message is a FINCopy output message, the FINCopy authentication verification failed.
FAB	FINCopy Authentication bypassed.	Message is a FINCopy output message, the FINCopy authentication code verification was bypassed.
FAN	FINCopy Authentication missing.	Message is a FINCopy output message, the FINCopy authentication is not present.
RTV	Retrieved message.	Message is an input or output message that has been retrieved.
***	Original	Message is an output message received from the SWIFT network and the instance is an original. Note: This means that only 1 instance contains the *** eye-catcher.

Warning headers - Alliance format

The default warning header is the Alliance format.

If Sanctions Screening flags a message as a true hit, then the warning header includes the warning, **Sanctions screening - Message blocked**. For more information about true hits, see "Configuration for Sanctions Screening" on page 58.

With this format, the warning header indicates that a message is a possible duplicate under any of the following conditions:

- The message was sent to the network with a Possible Duplicate Emission trailer
- The message was received with a Possible Duplicate Emission or Possible Duplicate Message trailer
- The message instance is a notification and an emission appendix exists before the related appendix

If a previous transmission attempt was made, then the warning header includes transmission-related details for the network, session holder, session number, sequence number, and delivery status.

Brief information prints in case authentication was successful or was not applicable for the message.

If the message being printed is a retrieved MT message, then the text prints accordingly.

Warning headers - ST200-like format

If Sanctions Screening flags a message as a true hit, then the warning header includes the warning, **Sanctions screening - Message blocked**. For more information about true hits, see "Configuration for Sanctions Screening" on page 58.

Text	Description
*** Naked Message ***	Prints only for an input message. Appears if the network delivery status of the related appendix indicates that the message was not acknowledged (NAK).
*** Authentication Result: <value> ***	<p>The following values are possible for the authentication result message, based on whether the message is MT, MX or a File message, and depending on the related appendix:</p> <ul style="list-style-type: none"> • Correct with current key • Incorrect • Correct with old key • Correct with future key • Authentication bypassed
*** Authentication/Authorisation Result: value> ***	<p>Printed only for an output MT message. The following value is possible:</p> <ul style="list-style-type: none"> • Incorrect
*** Authorisation Result: <value> ***	<p>Printed only for a message that requires authorisation. The following values are possible:</p> <ul style="list-style-type: none"> • No Record • Not Enabled • Invalid Period • Unauthorised
*** Authorisation key not present ***	Prints only for an output MT message that requires authorisation. Printed if no authorisation key is available.
*** FIN-Copy Authentication Result: <value> ***	<p>Prints only for an output MT message that requires proprietary authentication. The following values are possible for an MT message, based on the related appendix:</p> <ul style="list-style-type: none"> • Correct with current key • Incorrect • Correct with old key • Correct with future key

Text	Description
	<ul style="list-style-type: none"> Authentication bypassed Proprietary Authentication Code trailer missing
<code>*** FIN-Copy Authentication/Authorisation Result: <value> ***</code>	Prints only for an output MT message that requires proprietary authentication. The following values are possible for an MT message, based on the related appendix. The following value is possible: <ul style="list-style-type: none"> Incorrect
<code>*** Possible duplicate information received from network ***</code>	Prints if a message was received from SWIFT or from a back-office application as a possible duplicate. The possible duplicate information was set externally and received by Alliance Access.
<code>*** Possible duplicate indicator set locally ***</code>	Prints if a message was locally marked (within Alliance Access, either by means of a manual operation or otherwise) as a possible duplicate.
<code>*** Duplicate detected by interface ***</code>	Prints if Alliance Access has detected that a message is possibly a duplicate of another message in the database.
<code>*** Possible duplicate delivery ***</code>	If the original instance has one emission appendix, prints when printing/reprinting the original instance or when reprinting the transmission notification instance corresponding to the emission appendix. If the original instance has more than one emission appendix, prints when printing/reprinting the original instance or when reprinting any of the transmission notification instances corresponding to the emission appendices. ⁽¹⁾⁽²⁾
<code>*** Possible Duplicate Emission ***</code>	If the original instance has more than one emission appendix, prints when printing/reprinting the second, third, or later notification instances corresponding to the emission appendices. ⁽¹⁾⁽²⁾
<code>*** Possible Duplicate Reception ***</code>	Prints if the message is received from the network with a possible duplicate emission or Possible Duplicate Message trailer.
<code>*** Test and Training Mode ***</code>	Prints if the MT message sent or received is from/to a Test & Training destination.

(1) With status other than DLV_REJECTED_LOCALLY or DLV_NACKED.

(2) Applies to a 'Printing message to a Print MP' printout or a 'Printing with MXS layout from MMA' printout. A 'Printing message to a Print MP' printout creates an additional emission appendix (but no transmission notification instance), while a 'Printing with MXS layout from MMA' printout does not.

If a previous transmission attempt was made, the warning header includes transmission-related details for the network, session holder, session number, sequence number, and delivery status.

Instance type and transmission

The content of this section of the report varies, depending on the instance type and the type of transmission. The report always shows the network used to send the emission or reception appendix for a message. The following table explains additional content that can appear in the Instance Type and Transmission section:

Instance type / transmission	Content
Notification / emission	<p>Indicates the notification type, and includes the type of the related instance. Network acknowledgement information is printed. For notification type "Transmission", the report includes Network Delivery Status: <value>. For notification type "Delivery", the report includes User Delivery Status: <value>, possibly followed by NAK information.</p> <p>If the instance is for an MT message that is not an APC message, then the report includes Priority/Delivery : <value>. This information indicates the priority (System, Urgent, or Normal) and can be followed by the delivery status (Non-Deliv Warning or Deliv Notif).</p> <p>The message input reference prints in this part of the report.</p>
Notification / reception	<p>Indicates the notification type, and includes the type of the related instance. If the instance is for an MT message that is not an APC message, then the report includes Priority: <value>.</p> <p>The message output reference prints in this part of the report, along with the correspondent input reference.</p>
Original or Copy / emission	<p>Indicates the instance type and whether there is a related instance, and shows network acknowledgement information. If the instance is not for a FIN system message, then the report includes Priority/Delivery : <value>. This information indicates the priority (System, Urgent, or Normal) and can be followed by the delivery status (Non-Deliv Warning or Deliv Notif).</p> <p>The message input reference prints in this part of the report.</p>
Original or Copy / reception	<p>Indicates the instance type and whether there is a related instance. If the instance is for an MT message that is not an APC message, then the report includes Priority: <value>.</p> <p>The message output reference prints in this part of the report, along with the correspondent input reference.</p>

Message header

The content of this section of the report is relevant to the message itself, and not specific to the particular instance that has been printed.

Some content is common for both MT and MX messages:

- Message format
- Message direction (input or output)
- Transmission network
- Message type and message name

Details from the Correspondent Information File print for sender and receiver (MT message) or for the BIC8 that is part of the Requestor DN and Responder DN (MX message).

The following additional information prints for an MT message, if present:

- Message User Reference

- Banking Priority
- Server to Receiver Instructions
- FINCopy service
- Textblock Authentication, which includes User Code and MAC Result

For an MX message, the following information is included in the report:

- User Reference
- Service Name
- Non-repudiation Indicator
- Non-repudiation Type
- Non-repudiation Warning
- SWIFT reference
- SWIFT Request Reference
- CBT Reference
- Store-and-forward Input Time (if relevant)
- Signing DN

FIN User Header

The printed report contains the section, FIN User Header, in the following conditions:

- a. The value of the **Display/Print - FIN User Header** configuration parameter is set to Yes, and
- b. The message instance is printed through a Print message partner

Message text

The text of the message prints for any fields that contain values.

The FIN User Header (Block 3) is printed in the following conditions:

- a. The value of the **Display/Print - FIN User Header** configuration parameter is set to Yes, and
- b. The message instance is not printed through a Print message partner

Message trailer

The message trailer of an MT message prints after the message text.

Interventions

The interventions print for an instance if the **Print - Skip Interventions** parameter is set to No.

For an MX message sent using real-time delivery, intervention details of a Transmission Response (containing the Business Response) are preceded by the following information:

- SWIFT Reference
- Responder Reference

- Signing DN
- Signature Result
- Non-repudiation Type
- Non-repudiation Warning
- CBT-Reference
- Possible Duplicate Indication
- Responder DN

End of message trailer

When printing reports in ST200-like format, each message is terminated by an end-of-message trailer:

*End of Message

A.1.6 SOAP

Introduction

This section provides information about the SOAP connection method that you can use to transfer MT, XML-based, or FileAct messages between Alliance Access and a back-office application.

A.1.6.1 SOAP Host Adapter

Overview

The SOAP connection method enables the exchange of MT, XML-based, or FileAct messages between Alliance Access and back-office applications through the SOAP protocol. The SOAP connection method requires the licence package **14:SOAP ADAPTER** and supports the XML version 2 data format of revision 2 or higher.

The SOAP message carries the XMLv2 message. The parameters that control the file transfer include a pointer to the payload file, service, receiver of the file, header information, and notification options. These file-transmission parameters are carried in an XMLv2 message.

Note It is always the back-office application that starts a SOAP session with Alliance Access.

FileAct over SOAP

The SOAP Host Adapter supports the exchange of FileAct messages over HTTPS in two modes:

- Full FileAct mode, where file transmission parameters and the FileAct payload are transferred in XMLv2 format and the data exchange uses Web services over HTTPS.
- Mixed FileAct mode, where the file transmission parameters are carried in an XML version 2 message that is transferred using Web services over HTTPS, whereas the FileAct payload is transferred over the local file system.

SWIFT-defined SOAP Protocol

Alliance Access controls the interactive exchange of SOAP messages between the back-office applications and Alliance Access using an additional SWIFT-defined protocol on top of the SOAP protocol. This protocol provides a set of primitives to manage the message exchange sessions, to guarantee and ensure unique delivery of messages.

SOAP Primitives

The following SOAP primitives are used in SOAP messages:

- **Open**: open a session
- **Close**: close a session
- **Put**: send a message to Alliance Access
- **GetAck**: request Alliance Access to send a message that is waiting delivery to the back-office application, and optionally, acknowledge a message received from Alliance Access
- **Ack**: acknowledge a message received from Alliance Access

These primitives are implemented as operations of the SOAP host adapter Web service, which is described in "SOAP Host Adapter Web Service" on page 596. In this context, the request and response messages are SOAP messages exchanged over HTTPS.

For more information about the structure of SOAP messages, see "SOAP Message" on page 590.

Error Handling

When errors are encountered between the back-office applications and the SOAP host adapter, the standard SOAP fault error mechanism is used. When such SOAP fault errors are generated, the back-office can retry the requests except where the error refers to a session error (invalid token).

For more information, see "Recovery of a SOAP Session" on page 584.

A.1.6.2 SOAP Message Flow from Back-office Application

Types of information emitted to SWIFTNet

A back-office application can send the following information to Alliance Access in XMLv2 data format over SOAP:

1. MT message
2. XML-based message
3. A file (FileAct)

Before a message can be transmitted to SWIFTNet

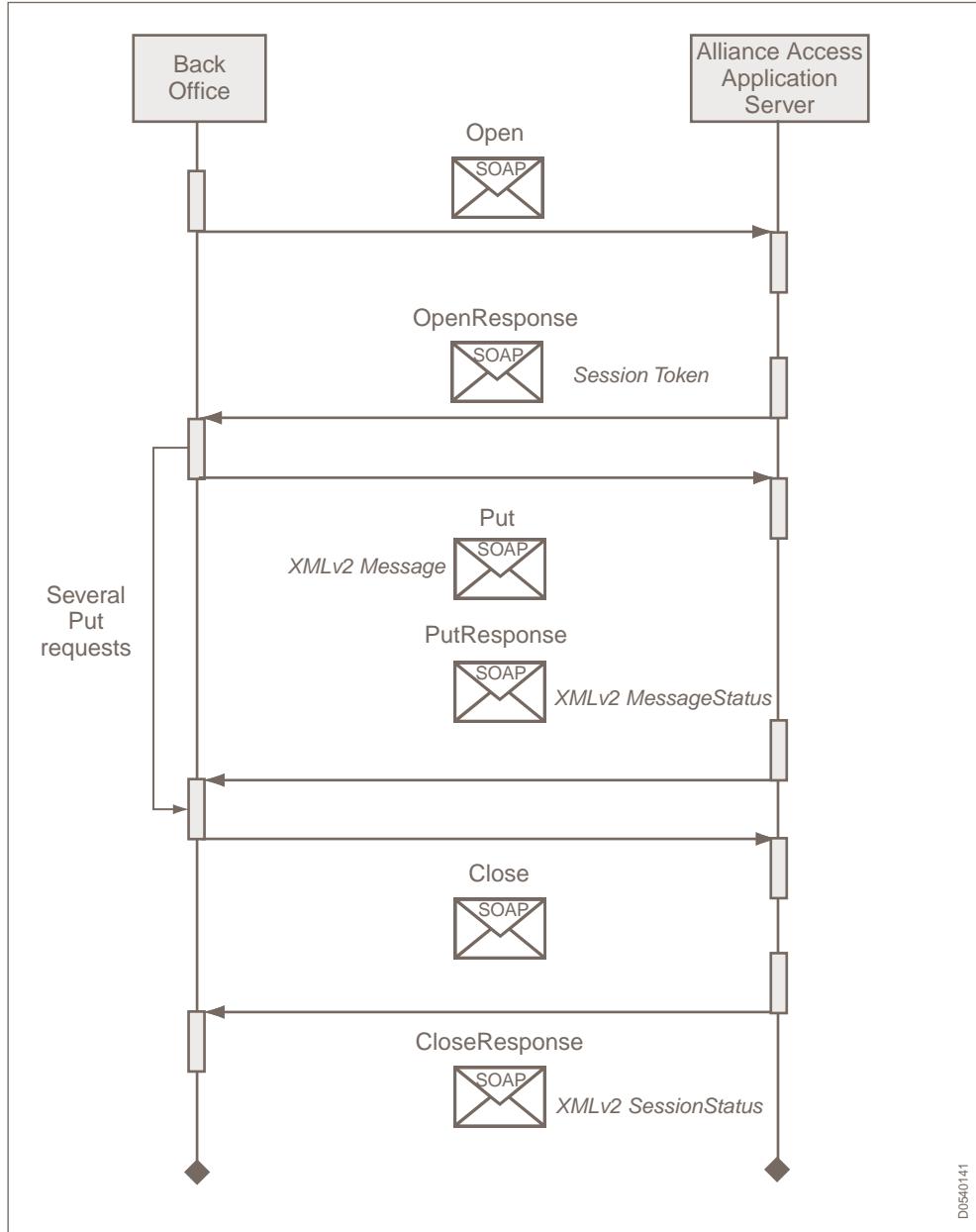
The description of the message flow assumes that:

- A **From** or **To&From** message partner that uses the **SOAP** connection method.
- **For mixed FileAct mode:**

The data directory that corresponds to the **Input Attachment Path** in the message partner profile has been defined and with correct access permissions. The back-office application will store files for sending to SWIFTNet in this directory.

SOAP - emission to SWIFTNet

Alliance Access receives an MT, XML-based, or FileAct message from a back-office application over SOAP and sends it to SWIFTNet as follows:



The back-office application can send **Put** request to Alliance Access if the SOAP message partner that is defined in Application Interface allows it. It can send several **Put** requests during one session.

Note

If the message partner is defined as **To&From** message partner, then messages are exchanged using the **Put** and **GetAck** messages while the session is open.

Emission of a file to SWIFTNet

Alliance Access receives a file from a back-office application and sends it to SWIFTNet as follows:

1. The back-office application prepares the SOAP message that contains the MT, MX, or FileAct message:

FileAct mode	Action taken by back-office application
Full	Adds the payload file as a SOAP attachment to the XML message, and optionally, signs the attachment. The body of the XML message is not required.
Mixed	Stores any payload files in the data directory that corresponds to the Input Attachment Path in the SOAP message partner profile. Places the name of the payload file in the body of the XML message.

2. The back-office application starts a session by sending an **Open** request.

Alliance Access confirms the session is open by sending an **OpenResponse**. This response contains the session token that identifies the session, and which must be used in each message that is exchanged as part of the session.

3. The back-office application sends a **Put** request, which has the XMLv2 message as its payload. This XMLv2 message contains the details of an MT, XML-based, or FileAct message.

4. On reception of the **Put** request, Alliance Access performs the following actions:

- a. Validates the session token in the **Put** message, to ensure that it matches the token returned in the **OpenResponse**.
- b. If the SOAP message partner that is associated with the session is configured for local authentication, then Alliance Access checks the local authentication of the message.

For more information, see "Local Authentication of SOAP Messages" on page 591.

- c. Checks that the sequence number of the received message is within the window size is defined for the session.

For more information about how the sliding window works in the SOAP host adapter, see "Window Size" on page 584.

- d. Processes the payload of the **Put** message, which contains the MT, XML-based or FileAct message. It may store the MT or XML-based message in the Alliance Access database.

For FileAct messages, the processing of the SOAP message varies depending on the FileAct mode, as follows:

FileAct mode	Actions
Full	Alliance Access checks that the XML message has a SOAP attachment that contains a payload file. If the SOAP attachment is signed, then Alliance Access also checks that the signature is correct.

FileAct mode	Actions
Mixed	<p>Alliance Access extracts the name of the payload file from the body of the XML message.</p> <p>Then, it checks that a file with that physical name exists in the Input Attachment Path, and has the permissions to be read and moved after processing.</p>

- For FileAct messages, Alliance Access automatically calculates the digest value of the payload file, and stores the file in the database.

The configuration parameter **File Digest Algorithm** specifies which Secure Hash Algorithm (SHA-1 or SHA-256) to use to calculate the digest value.

- If the processing of the **Put** message is successful, then Alliance Access replies to the back-office application with a **PutResponse**. If not, a SOAP fault message is sent to the back-office application.

For more information about SOAP faults, see "SOAP Fault - soapenv:Fault" on page 596.

The session remains open, and Alliance Access processes subsequent **Put** messages based on the window size.

- The back-office application ends an interactive SOAP message exchange session with Alliance Access by sending a **Close** message that specifies the session token of the session to be closed. Alliance Access sends a **CloseResponse** message to confirm that the session is closed.

Payload filenames

The file name can contain the characters, A-Za-z0-9 ._. Alliance Access replaces any other character with an underscore _.

Depending on the value of the **Extension** field in the message partner profile, an optional file name extension is added to the file name.

A.1.6.3 SOAP Message Flow to Back-office Application

Types of information received from SWIFTNet

Alliance Access can send the following information to a back-office application in XMLv2 data format over SOAP:

- Transmission Notification
- Delivery Notification
- History Notification or Information Notification
- A file (FileAct)

Before a message can be received from SWIFTNet

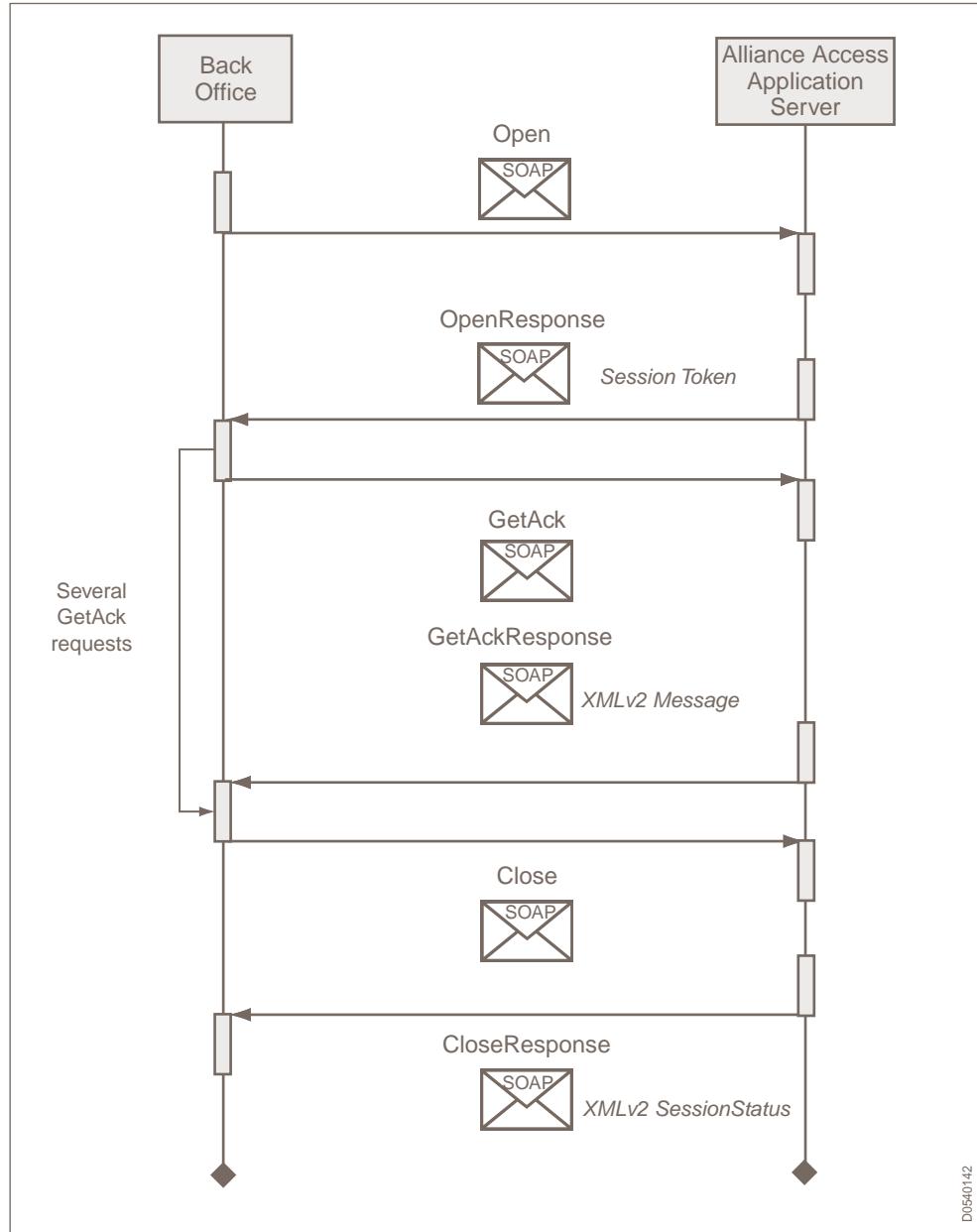
The description of the message flow assumes that:

- A To or To&From message partner that uses the SOAP connection method.
- For mixed FileAct mode:**

The data directory that corresponds to the **Output Attachment Path** in the message partner profile has been defined and with correct access permissions. The back-office application searches this directory for files that it receives from SWIFTNet.

- An Exit point is defined for the message partner, to hold the messages that are awaiting delivery to the back-office application.

SOAP - reception from SWIFTNet



The back-office application can send **GetAck** request to Alliance Access if the SOAP message partner that is defined in Application Interface allows it. It can send several **GetAck** requests during one session.

Note

If the message partner is defined as **To&From message partner**, then messages are exchanged using the **Put** and **GetAck** messages while the session is open.

Reception of a file from SWIFTNet

Alliance Access receives a file from SWIFTNet and sends it to a back-office application, as follows:

1. The back-office application starts a session by sending an **Open** request.

Alliance Access confirms the session is open by sending an **OpenResponse**. This response contains the session token that identifies the session, and which must be used in each message that is exchanged as part of the session.

2. The back-office application sends a **GetAck** request, to retrieve any messages that are waiting to be delivered to the back-office application.

The **GetAck** request has a timeout specified in it.

3. On reception of the **GetAck** message, Alliance Access performs the following actions:

a. Validates the session token in the **GetAck** message, to ensure that it matches the token returned in the **OpenResponse**.

b. If the SOAP message partner that is associated with the session is configured for local authentication, then Alliance Access checks the local authentication of the message.

For more information, see "Local Authentication of SOAP Messages" on page 591.

c. Checks that the sequence number of the received message is within the window size is defined for the session.

For more information about how the sliding window works in the SOAP host adapter, see "Window Size" on page 584.

d. If the **GetAck** request specifies an Ack client reference, then Alliance Access marks the associated message as acknowledged.

e. Fetches the next MT or XML-based message that is waiting for delivery in the exit point.

For FileAct, Alliance Access prepares the SOAP message to transfer the file:

FileAct mode	Action taken by Alliance Access
Full	Adds the payload file as a SOAP attachment to the XML message. The body of the XML message is not required.
Mixed	Stores the payload file in the data directory that corresponds to the Output Attachment Path in the SOAP message partner profile. Places the name of the payload file in the body of the XMLv2 message.

4. If the processing of the **GetAck** message is successful, then Alliance Access replies to the back-office application with a **GetAckResponse**. If not, a SOAP fault message is sent to the back-office application.

For more information about SOAP faults, see "SOAP Fault - soapenv:Fault" on page 596.

The session remains open, and Alliance Access processes subsequent **GetAck** messages based on the window size.

5. The back-office application ends an interactive SOAP message exchange session with Alliance Access by sending a **Close** message that specifies the session token of the

session to be closed. Alliance Access sends a **CloseResponse** message to confirm that the session is closed.

Payload filenames

The file name can contain the characters, A-Za-z0-9 ._. Alliance Access replaces any other character with an underscore _.

Depending on the value of the **Extension** field in the message partner profile, an optional file name extension is added to the file name.

A.1.6.4 Prepare to Use FileAct over SOAP

Purpose

Use the instructions in this section to prepare Alliance Access to communicate with a back-office application using SOAP.

Prepare to use FileAct over SOAP

On Alliance Access, do the following:

1. Determine which FileAct mode to use:

- full

Next, go to Step 4 on page 584.

- mixed

Next, go to Step 2 on page 583.

2. Create the directories that Alliance Access will use to exchange files with each back-office application.

Ensure that the directories have correct permissions:

- **Emission from Back Office**

It must be possible to open the **Input Attachment Path**.

- **Reception at the Back Office**

It must be possible to write to the **Output Attachment Path**.

3. Configure a message partner profile for each back-office application that will use SOAP to communicate with Alliance Access.

Note that:

- **Emission from Back Office**

From **Message Partners**: the directory is specified in **Input Attachment Path**

- **Reception at the Back Office**

To **Message Partners**: the directory is specified in **Output Attachment Path** field.

The message partner profile will provide the SOAP transmission parameter for file transfers between the back-office application and the correspondent.

4. For **From Message Partners**, determine whether to use First In First Out (**FIFO**) order. The order in which messages are processed affects how Alliance Access will process the messages from the back-office application.
For more information about FIFO affects the use of the sliding window in the SOAP host adapter, see "Window Size" on page 584.
5. Verify the settings of the following system management parameters suit the requirements of the back-office application:
 - **File Digest Algorithm**
6. Ensure that payload files do not exceed 250 MB.

A.1.6.5 Recovery of a SOAP Session

Introduction

This section describes how Alliance Access recovers sessions with the SOAP host adapter.

Session Rebuild

In the case of an Alliance Access restart, Alliance Access resumes the traffic as if nothing happened. Alliance Access rebuilds the SOAP session and resets it in the state that it was before the Alliance Access restart. The emission and reception window is rebuilt in such a state that:

- the messages being sent or received are in the window
- the messages waiting acknowledgement are identified

The SOAP host adapter sends an error to the back-office application when:

- a message sent by the back-office application is not within the window
- the messages that the back-office application is acknowledging are not present in the window

Messages re-sent with Possible Duplicate Emission

When, at session closure, messages sent by Alliance Access to the back-office application have not been acknowledged yet, the session is aborted, and these messages have their Network Status set to "Network Aborted". The messages are requeued in the exit point. If the back-office application requests these messages again, then they are re-sent with a possible duplicate emission indication when the session is re-opened.

A.1.6.6 Window Size

A.1.6.6.1 Sliding Window

Description of a sliding window

The SOAP Host Adapter implements a sliding window mechanism.

A sliding window defines the boundary and size of a range of actions within which there are actions waiting to be completed. For example, if the window size is 2 means that there are exactly two actions pending completion

A window of w elements means that Alliance Access can process w actions simultaneously, and that Alliance Access starts a new action only when it has processed all the w actions successfully

A direct consequence of this mechanism is that while the range is bound, the number of concurrent actions can be as small regardless of the actual window size. For example, the number of concurrent actions can be one action even if the window size is 5.

First-in-first-out (FIFO) order

The actions to be processed have a precise sequence number.

When the actions are run in first-in-first-out (FIFO) order, then the sliding window behaves as a counting window. Therefore, there is just a count of the actions pending completion, without any boundary.

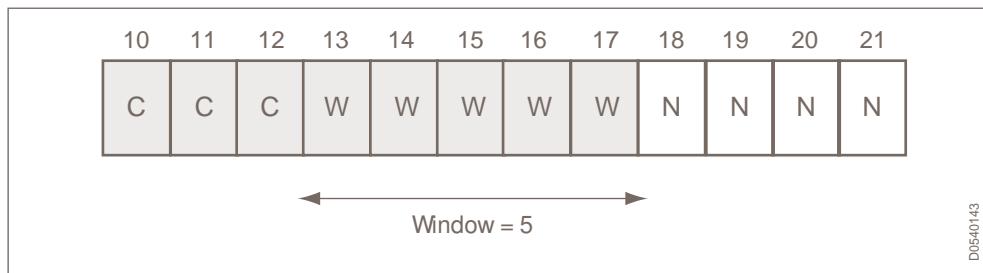
However, if actions are not processed in FIFO order, then the window enforces a boundary to the range of the actions that are pending completion.

Example

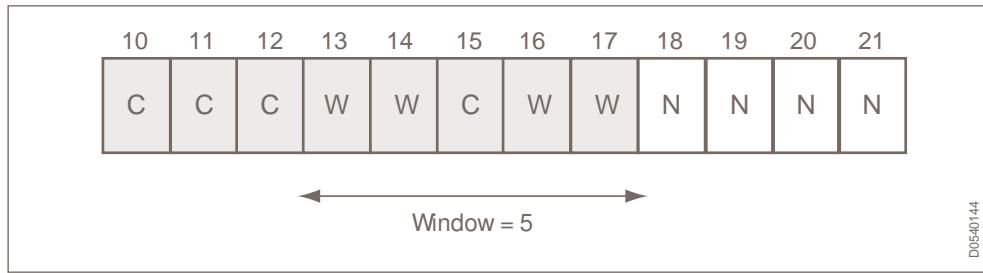
In the diagrams in this example, the following conventions are used:

- "C" means "Completed",
- "W" means "Waiting for completion"
- "N" means "Not started"
- Actions are numbered from 1 to n

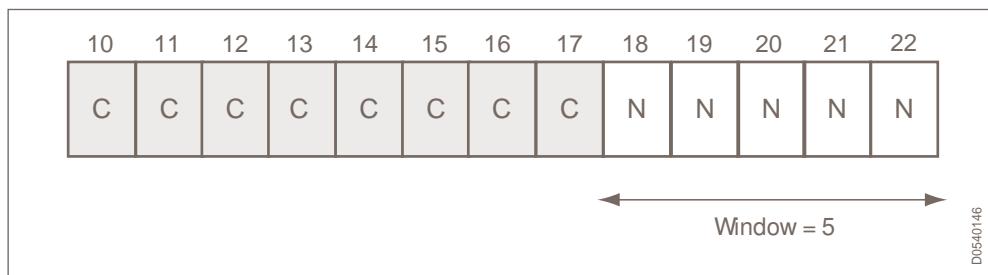
For example, the size of the window is 5:



Action 15 is completed. The window does not slide to the right because the window size of 5 specifies that all 5 actions must be completed before another action starts:



However, when action 13 is completed, the entire window slides five positions to the right, starting at 18 and ranging to 22:



A.1.6.6.2 Window in the Flow from Back-Office Applications

Flow from back office

The implementation of the sliding window in the SOAP host adapter enables acknowledgement messages to be resent if a previously sent acknowledgement is not received, or if a back-office application resends a message.

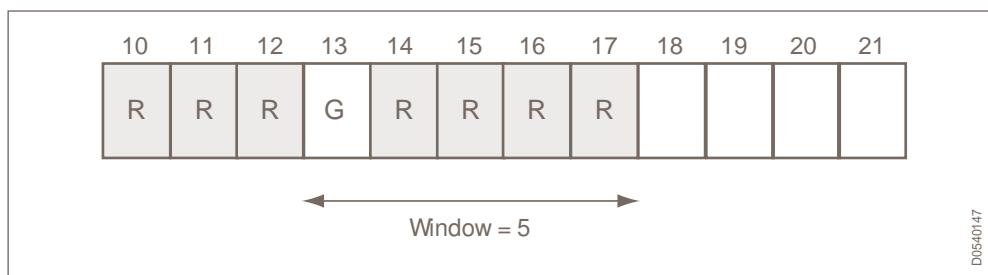
If FIFO is used, then Alliance Access waits until all the previous messages are received before it stores the messages.

Example

In the diagrams in this example, the following conventions are used:

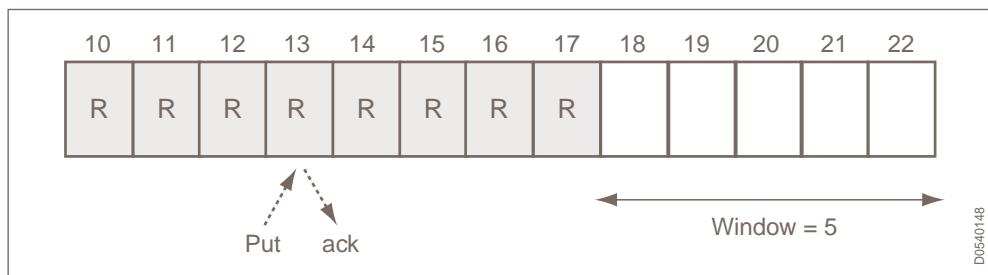
- R means a "Received message"
- "C" means "Completed",
- "G" means a "Gap"
- Actions are numbered from 1 to n

For example, a back-office application sends messages to Alliance Access and the SOAP Host Adapter uses a window size of 5:



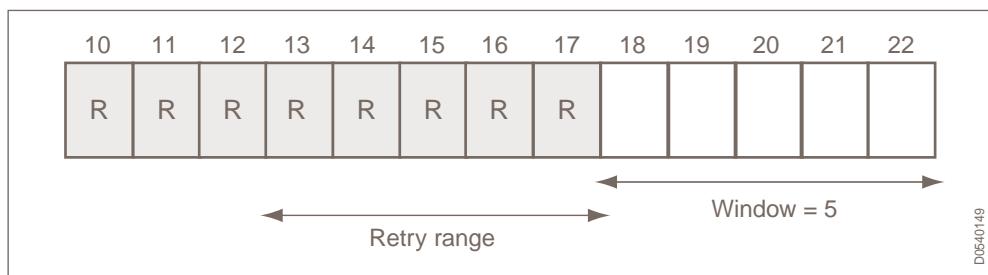
The SOAP host adapter receives messages 14 through 17 successfully, but message 13 has not been received. Therefore, the window does not move to the right. At some point, the back-

office application sends message 13 and the SOAP host adapter sends the appropriate acknowledgement:



At that moment, the back-office application is still waiting for the acknowledgement of the message 13. In the worst scenario, if the acknowledgement can be lost, then the back-office application receives an error which prompts it to re-sends message 13. However, the SOAP adapter has received and processed message 13, and the window has moved to the right. Therefore, the SOAP host adapter window expects new messages between 18 and 22, but it must be ready to accept attempts to resend message 13 through 17.

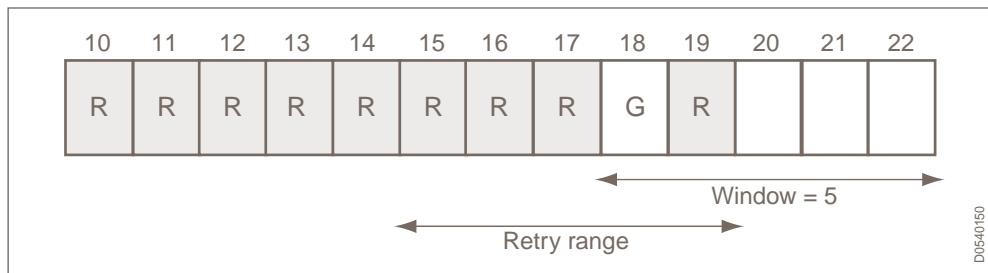
A retry range must be defined:



Note The retry range and the window usually overlaps.

If the back-office application finally manages to send message 13 and receive an acknowledgement successfully for it, then the back-office application starts sending messages 18 through 22.

The SOAP host adapter may receive message 19 before message 18, as shown in the following diagram:



The retry range on the SOAP host adapter moves two positions to the right. Since the message 19 got received, you can assume that the back-office application received acknowledgement for messages 14 and before (otherwise, the back-office application would have sent a message outside of its own window of 5). In reality, the back-office application received all the acknowledgement of messages up to 17, but the SOAP host adapter has no way of knowing this until it receives message 22.

Rules for retry range and window size

The following rules can be defined:

- The retry range spans from the last-received message to W-1 positions on the left:
Retry range = [Last_R-W+1; Last_R]
- The window spans from the first missing message to W-1 positions on the right:
Window = [First_G ; First_G+W-1]
- The full acceptable range for message reception on the SOAP host adapter is the overlap of these two ranges:
Acceptable range = [Last_R-W+1; First_G+W-1]

where First_G is either the first gap or, if no gap exists, the next message to be received.

The maximum size of the range is twice the window size. The minimal size of the range is the window size.

A.1.6.6.3 Window in the Flow towards Back-Office Applications

Flow towards back-office

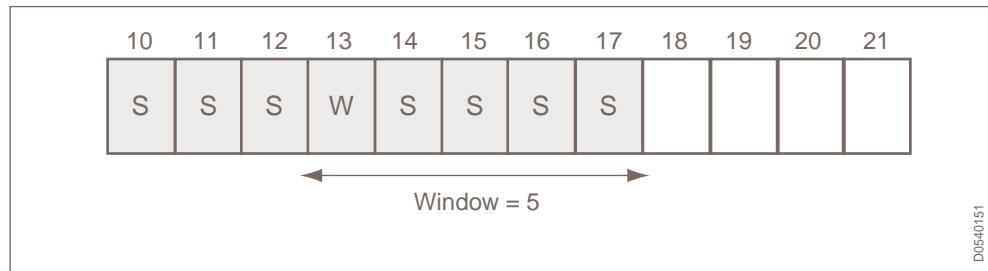
A similar sliding window mechanism is put in place for the flow of messages from the SOAP host adapter to the back-office applications. In this flow, the SOAP host adapter sends messages to the back-office application as replies to the **GetAck** request sent by the back-office application.

Example

In the diagrams in this example, the following conventions are used:

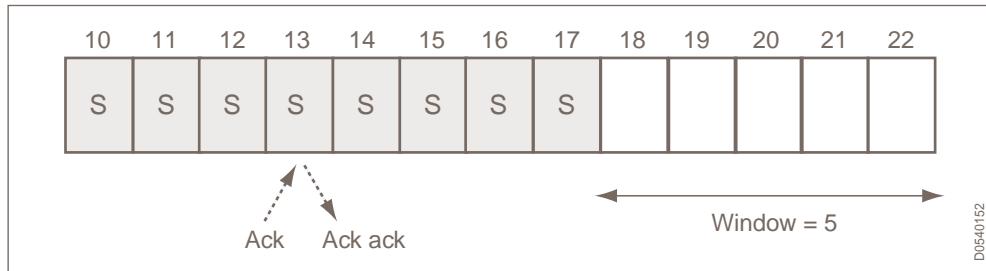
- R means a "Received message"
- S means "Sent message"
- W means a "Waiting acknowledgement"
- Actions are numbered from 1 to n

For example, a SOAP host adapter sends messages to the back-office application the SOAP Host Adapter uses a window size of 5:



On reception of message 13, the back-office application sends an ACK message to acknowledge the reception of message 13. The SOAP host adapter replies to the back-office

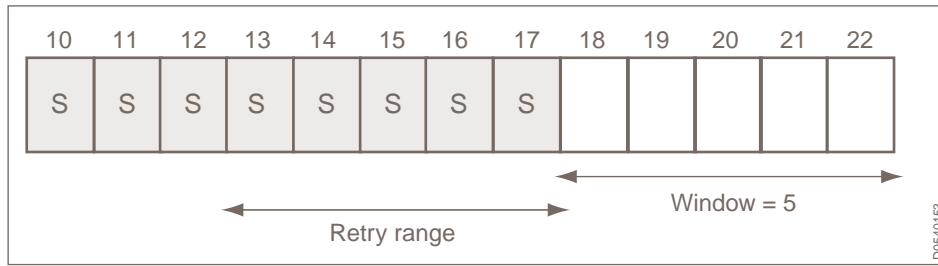
application with another ACK message to inform the back-office application that message 13 has been processed successfully:



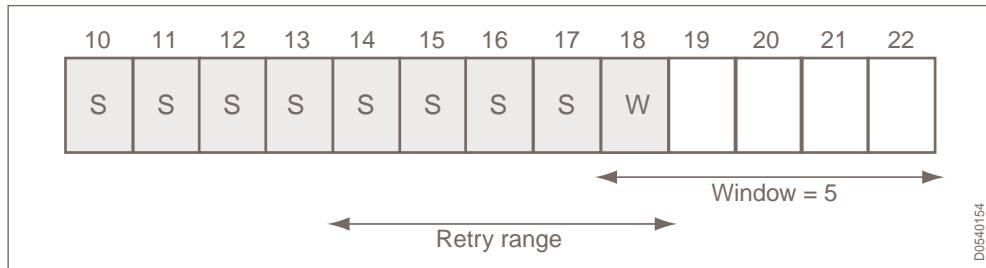
If this ACK message is lost between the SOAP host adapter and the back-office application, then the back-office application sends a new **GetAck** request to retrieve message 13. The SOAP host adapter must accept this retry request even though its window is now 18 to 22. A retry range is defined.

At that point, the window of the back-office application ranges from 13 to 17, whereas the window of the SOAP host adapter ranges from 18 to 22.

As a consequence, there must be a retry range between message 13 and 17 because it is possible that all messages between 13 and 17 have failed for a similar reason:



However, as soon as the SOAP host adapter receives a new **GetAck** request for message retrieval, it means that the back-office application received all required information. Therefore, retries of message 13 are not expected any more, but retries of message 18 are now possible:



Rules for retry range and window size

The following rules can be defined:

- The retry range spans from the last received message (acknowledged or not) to W-1 positions on the left:

$$\text{Retry range} = [\text{Last_R}-\text{W}+1; \text{Last_R}]$$
- The window spans from the first non-acknowledged message to W-1 positions on the right:

$$\text{Window} = [\text{First_W}; \text{First_W}+\text{W}-1]$$
- The full acceptable range for message retrieval on the SOAP host adapter is the overlap of these two ranges:

Acceptable range = [Last_R-W+1; First_W+W-1]

where First_W is the first message waiting for acknowledgement or, if none, the next unretrieved message.

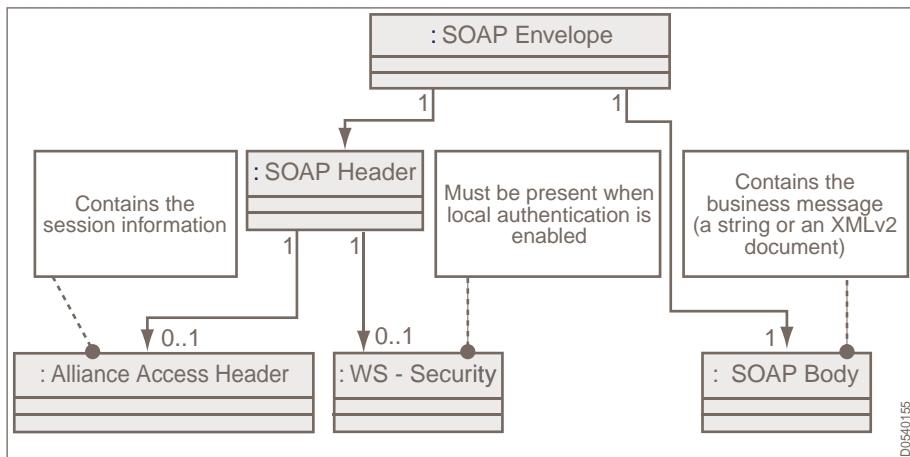
The maximum size of the range is twice the window size. The minimal size of the range is the window size.

Note When the sequence number reaches its maximum value (999999), it restarts at 1. This can lead to scenarios where the window and retry ranges have start values numerically higher than the end values.

A.1.6.7 SOAP Message

Structure of a SOAP message

A SOAP message that is exchanged between the back-office applications and Alliance Access the Alliance Access SOAP host adapter has a common structure, which is presented in the following figure:



The different elements of such a SOAP message are:

- SOAP Header (optional):
 - Alliance Access Header (soapha:SAAHeader)
 - Web Service Security Header (wsse:security)
- SOAP Body (mandatory)

All the SOAP messages generated by invoking the operations exposed by the SOAP host adapter web service of Alliance Access comply with this structure.

SOAP Header

The following headers are optional parts of a SOAP message:

Header type	Description	More information
Alliance Access Header (soapha:SAAHeader)	contains information specific to the session opened between the back-office application and the Alliance Access SOAP host adapter.	"SAA Header Block - soapha:SAAHeader" on page 593

Header type	Description	More information
Web Service Security Header (wsse:security)	provides local authentication at the level of the SOAP messages between the back-office application and the Alliance Access SOAP host adapter.	"Local Authentication of SOAP Messages" on page 591 "Local Authentication - wsse:Security" on page 594

Soap Body

The mandatory SOAP body: this is the business message itself (MT or XML-based message).

The mandatory SOAP body contains the business message itself: a string or an XMLv2 document. Examples of the SOAP body are provided in "SAA Header Block - soaph:SAAHeader" on page 593, and in the [Knowledge Base Tip 2236509](#).

A.1.6.8 Local Authentication of SOAP Messages

Overview

The local authentication between a back-office application and Alliance Access SOAP adapter is supported using the WS-Security standard (for more information, see [OASIS: SOAP Message Security 1.0](#)).

The Web Service Security Header is a standard block that facilitates the encryption and authentication of SOAP messages between two applications at the message level, rather than at transport level.

The Web Service Security Header block contains the local authentication message code (LMAC) calculated by the application sending the SOAP message. The calculation uses the HMAC SHA-256 algorithm on a canonicalised version of the SOAP message (the SOAP body and the SAAHeader block if present) using the Local Authentication key defined within the message partner in Alliance Access.

For more information about the Web Service Security Header, see "Local Authentication - wsse:Security" on page 594.

Compliance requirements

To remain compliant with the WS-Security standards, Application developers must take the following points into consideration:

- For SOAP, the HMAC algorithm must be performed without truncation. Therefore, the signature has a size of 256 bits and not 128 bits.

For more information, see [WS I: Basic Security Profile 1.0](#).

- The signature is calculated on the digests of the canonical form of the SOAP body and header blocks, as described in [OASIS: SOAP Message Security 1.0](#).

A.1.6.9 XML Structures

Overview

This section defines the XML structures used in the context of the Alliance Access SOAP host adapter.

A.1.6.9.1 Namespaces and Algorithms

A.1.6.9.1.1 Namespace of the SOAP Host Adapter

Description

The URN of the SOAP host adapter namespace.

urn:swift:saa:xsd:soapha

A.1.6.9.1.2 Namespace Prefixes

Namespace

Namespace URIs represent some application-dependent or context-dependent URI. The choice of any namespace prefix is not semantically significant. The prefixes used in this document are selected to refer to the standard schemas.

The following table shows the namespaces and prefixes that are used in this document:

Prefix	Namespace	Comment
soapha	urn:swift:saa:xsd:soapha	Elements of the SOAP host adapter
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	Web services Security (for more information, see <i>OASIS: SOAP Message Security 1.0</i>)
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	Web services Utility (for more information, see <i>OASIS: SOAP Message Security 1.0</i> and "The Attribute ID" on page 594)
c14n	http://www.w3.org/2001/10/xml-exc-c14n#	Exclusive XML canonicalisation
ds	http://www.w3.org/2000/09/xmldsig#	XML signature Syntax and Processing
soapenv	http://schemas.xmlsoap.org/soap/envelope	Elements of the SOAP envelope
xs	http://www.w3.org/2001/XMLSchema	XML schema

A.1.6.9.1.3 Algorithms

Algorithms

These type definitions provide names that represent the algorithm URIs which are used in this document:

Type	Definition	Comment
uri-hmac-sha256	string = "http://www.w3.org/2001/04/xmldsig-more#hmac-sha256"	Algorithm: HMAC with SHA-256 (see <i>HMAC: Keyed-Hashing for Message Authentication</i>)
uri-sha256	string = "http://www.w3.org/2001/04/xmlenc#sha256"	Hashing algorithm SHA-256 (see <i>Federal Information Processing Standards Publications Secure Hash Algorithm</i>)
uri-xml-exc-c14n	string = "http://www.w3.org/2001/10/xml-exc-c14n#"	XML exclusive canonicalisation C14N (see <i>W3C Recommendation - Exclusive XML-Canonicalisation version 1.0</i>)

A.1.6.9.2 SOAP Message - soapenv:Envelope

Tags

Tag	Definition	Description
soapenv:Envelope	soapenv:Header soapenv:Body	Standard structure of a SOAP message. The encoding must be UTF-8. Although only the tags and the attributes of SOAP host adapter are documented here, the message can comprise any other tags and attributes that comply with SOAP.
soapenv:Header	SAAHeader wsse:Security [0..1]	The SAA header (for more information, see "SOAP Message" on page 590) is the header block required by the SOAP host adapter. It is interpreted or produced by the SOAP host adapter. One optional security header block is present for local authentication signature (for more information, see "Local Authentication of SOAP Messages" on page 591). It is interpreted or produced by the SOAP host adapter (the Alliance Access actor).
soapenv:Body	attribute { wsu:Id : string [0..1] } { ANY soap:Fault }	The message body that is required by the SOAP host adapter. The attribute Id must be present when the local authentication is enabled (for more information, see "Namespace of the SOAP Host Adapter" on page 592). A SOAP fault is never present in a client request. A SOAP fault is never signed (no security header).

A.1.6.9.3 SAA Header Block - soapha:SAAHeader

SAA Header block

The optional SAA Header block contains information specific to the session opened between the back-office application and the Alliance Access SOAP host adapter.

Tag	Definition	Description
SAAHeader	SessionToken SequenceNumber [0..1] ClientRef [0..1] AckClientRef [0..1]	
SessionToken	String	The session token identifying the session
SequenceNumber	Integer	The first sequence number that is used by the SOAP host adapter when sending messages to the back-office application. The values are in [1, 999999].
ClientRef	String	The reference the back office uses to identify the message it will receive from the SOAP adapter following a GetAck request
AckClientRef	String	The back-office reference of the previous received message that it has acknowledged

Example

```

<SAAHeader xmlns="http://swift.com/saa/soapha" Id="SAAHeader">
  <SessionToken>404d4051-3bba-4661-afda-6471cf2b942a</SessionToken>
  <SequenceNumber>388</SequenceNumber>
  <ClientRef>B0Reference020</ClientRef>
  <AckClientRef>AckB0Reference011</AckClientRef>
</SAAHeader>

```

A.1.6.9.4 Local Authentication - wsse:Security

A.1.6.9.4.1 The Attribute ID

Attribute

If the local authentication is enabled for the message partner indicated in SAAHeader, then the attribute ID must be present in the body and in each header block comprising the SAAHeader. The attribute ID can have any value as long as it provides a unique reference in the scope of the SOAP message.

This attribute belongs to the namespace `wsu` but is also accepted in the local namespace (without prefix).

Usage of Attribute ID

To ensure integrity of parts of the message, the URI attribute in `ds:Reference` must point to the attribute ID of the part to be authenticated:

Usage of the attribute ID

To ensure integrity of	ds:Reference points to Attribute ID of
payload of the message	<code>soapenv:Body</code>
session token	<code>SAAHeader</code>
message partner name ⁽¹⁾	<code>keyInfo</code>

(1) The Message partner name in `ds:KeyName` determines which LAU key is used to compute the signature

A.1.6.9.4.2 The Security Header Block of SOAP Host Adapter

Security

The following description is a simplified excerpt from [OASIS: SOAP Message Security 1.0](#) document presenting the settings that are specific to the SOAP host adapter. The security header block must be built as described in the [OASIS: SOAP Message Security 1.0](#) document.

Tag	Definition	Description
<code>wsse:Security</code>	<code>attribute {</code> <code> soapenv:actor:urn:swift:saa</code> <code>}</code> <code>ds:Signature</code>	The security header block contains the XML signature corresponding to the local authentication presented in "Local Authentication - wsse:Security" on page 594.
<code>ds:Signature</code>	<code>ds:SignedInfo</code> <code>ds:SignatureValue</code> <code>ds:KeyInfo</code>	
<code>ds:SignedInfo</code>	<code>ds:CanonicalizationMethod</code> <code>ds:SignatureMethod</code>	There must be references for all the header blocks and the body.

Tag	Definition	Description
	ds:Reference [2..n]	
ds:CanonicalizationMethod	<pre>attribute { Algorithm : uri-xml-exc-c14n } c14n:InclusiveNamespaces</pre>	<p>The SOAP host adapter requires and supports only the C14N exclusive canonicalisation method.</p> <p>For more information, see W3C Recommendation - Exclusive XML-Canonicalisation version 1.0.</p>
ds:SignatureMethod	<pre>attribute { Algorithm : uri-hmac-sha256 }</pre>	<p>The SOAP host adapter requires and supports only the HMAC / SHA 256 signature method.</p> <p>For more information, see HMAC: Keyed-Hashing for Message Authentication.</p>
ds:SignatureValue	PCDATA Base64 string	The signature is inserted here encoded in Base64.
ds:KeyInfo	ds:KeyName	
ds:KeyName	String	The SOAP host adapter requires information to identify the key used for the local authentication. The id of the message partner defined in Alliance Access is provided here.
ds:Reference	<pre>attribute { URI : string } ds:Transforms ds:Digestmethod ds:DigestValue</pre>	<p>The attribute URI refers any part of a SOAP message that must be checked by local authentication.</p> <p>These can include:</p> <ul style="list-style-type: none"> • soapenv:Body • SAAHeader • dsKeyInfo <p>It uses the name provided by the attribute Id of this header block.</p> <p>For more information, see "The Attribute ID" on page 594 and ds:SignedInfo.</p>
ds:Transforms	ds:Transform [1..n]	
ds:Transform	<pre>attribute { Algorithm : uri-xml-exc-c14n } c14n:InclusiveNamespaces [0..1]</pre>	<p>The SOAP host adapter requires and supports only the C14N exclusive canonicalisation method.</p> <p>For more information, see W3C Recommendation - Exclusive XML-Canonicalisation version 1.0.</p>
ds:DigestMethod	<pre>attribute { Algorithm : uri-sha256 } EMPTY</pre>	<p>The SOAP host adapter requires and supports only the digest method SHA 256.</p> <p>For more information, see Federal Information Processing</p>

Tag	Definition	Description
		Standards Publications Secure Hash Standard .
ds:DigestValue	PCDATA Base64 string	The digest is inserted here encoded in Base64.
c14n:InclusiveNamespaces	attribute { c14n:PrefixList : string }	For more information, see W3C Recommendation - Exclusive XML-Canonicalisation version 1.0 .

A.1.6.9.5 SOAP Fault - soapenv:Fault

Fault mechanism

The standard SOAP Fault mechanism is used to report error and/or status information to the calling application.

As per W3C recommendation, the SOAP Fault element appears once as a body entry of the SOAP response.

The detail tag of the SOAP fault either contains a SAAFault element or a SessionFault element. These elements have the following structure:

Tag	Definition	Description
reason	string	Short text that describes the reason for the error
context	string	Provides details about the action being performed before the error occurred
severity	string	Provides the severity of the error: severe or transient
details	string	Provides more information on the error and on the possible resolution actions

A.1.6.10 SOAP Host Adapter Web Service

Overview

The SOAP Host Adapter Web service gathers the operations that can be invoked to exchange SOAP messages containing MT, XML-based, or FileAct messages between back-office applications and Alliance Access.

Operations

The SOAP Host Adapter Web service exposes the following operations:

- **Open:** open a session
- **Close:** close a session
- **Put:** send a message to Alliance Access
- **GetAck:** request Alliance Access to send a message waiting delivery to the back-office application and optionally acknowledge a message received from Alliance Access
- **Ack:** acknowledge a message received from Alliance Access

WSDL and Schema Information

WSDL and schema file location on Windows: %ALLIANCE%\MXS\xsd

WSDL and schema file location on UNIX or Linux: \$ALLIANCE/MXS/xsd

WSDL file: soapha.wsdl

Schema file: embedded in the soapha WSDL, SAA_XML_v2_0_2.xsd

WSDL get operation: <https://hostname:port/soapha/?WSDL>

Namespace:

- WSDL namespace: urn:swift:saa:wsdl
- SOAP host adapter schema namespace: urn:swift:saa:xsd:soapha

A.1.6.10.1 Open

Description

This operation requests the opening of a session for the exchange of MT, XML-based, or FileAct messages using the SOAP host adapter between Alliance Access and back-office applications.

Input

Open - This element contains the Open element.

Open

Name	Type	Description	Allowed values
MessagePartnerName	MessagePartnerName	The identity of the message partner defined in Alliance Access for which a session will be opened	
SequenceNumberToSAA	SequenceNumber	The first sequence number that is used by the back-office application when sending messages to the SOAP host adapter	[1,999999]
WindowSize	WindowSize	The requested number of messages which can remain unacknowledged within an emission or reception window	[1,10]
FlowDirection	Direction	The direction of the flow for which a session will be opened	To_MessagePartner From_MessagePartner To_And_From_MessagePartner

Name	Type	Description	Allowed values
RoutingMode	RoutingMode	<p>This parameter is used to enable a deferred commit or rollback between Alliance Access and Alliance Converter. It is optional, and if not present, the default value is <code>Immediate</code>.</p> <p>When set to <code>Immediate</code>, each message received from the back office (or read in an exit point to the back office) is immediately sent/routed (or sent to the back office) by Alliance Access.</p> <p>When set to <code>Deferred</code>, messages from the back office (or to the back office) are kept in the <code>_AI_from_APPLI</code> queue (or in the exit points) until the session is closed. When the session is closed, all of the message are sent/routed together.</p>	Immediate Deferred

Output

OpenResponse - This element returns the `OpenResponse` element which contains the `OpenResponseDetails`.

OpenResponse

Name	Type	Description	Allowed values
OpenResponseDetails	OpenResponseDetails		

OpenResponseDetails

Name	Type	Description	Allowed values
SequenceNumberFromSAA	SequenceNumber	The first sequence number that will be used by the SOAP host adapter when sending messages to the back-office application	[1,999999]
WindowSize	WindowSize	The negotiated number of messages which can remain unacknowledged within an emission or reception window	[1,10]

SAAHeader

The SAAHeader returns the session token allocated by Alliance Access. This session token must be repeated in any subsequent message request being part of this session.

Example

Open request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:swift:saa:xsd:soapha">
  <soapenv:Header />
  - <soapenv:Body>
  - <urn:Open>
    <urn:messagePartnerName>SoapHA</urn:messagePartnerName>
    <urn:sequenceNumberToSAA>1</urn:sequenceNumberToSAA>
    <urn>windowSize>5</urn>windowSize>
    <urn:flowDirection>To_And_From_MessagePartner</urn:flowDirection>
  </urn:Open>
  </soapenv:Body>
</soapenv:Envelope>
```

Open response

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Header>
    <SAAHeader xmlns="urn:swift:saa:xsd:soapha">
      <SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</SessionToken>
    </SAAHeader>
  </S:Header>
  <S:Body>
    <OpenResponse xmlns="urn:swift:saa:xsd:soapha">
      <openResponseDetails>
        <sequenceNumberFromSAA>1</sequenceNumberFromSAA>
        <windowSize>5</windowSize>
      </openResponseDetails>
    </OpenResponse>
  </S:Body>
</S:Envelope>
```

A.1.6.10.2 Close

Description

This operation requests the closing of a session for the exchange of MT, XML-based, or FileAct messages using the SOAP host adapter between Alliance Access and back-office applications.

Input

Close - This element contains the empty element Close.

SAAHeader - The SAAHeader contains the session token of the session to be closed by the Alliance Access SOAP host adapter upon request from the back office.

RoutingAction - This parameter can be set to either Commit or Rollback. It is mandatory if the RoutingMode parameter was present and set to Deferred in the corresponding Open session call. Note that the failure to provide the RoutingAction in this case causes a protocol error, and the entire session is aborted. It is ignored if the RoutingMode parameter was not present or was set to Immediate in the corresponding Open session.

Output

CloseResponse - This element returns the XMLv2 SessionStatus element as described in "SessionStatus" on page 717.

Example

Close request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:swift:saa:xsd:soapha">
  <soapenv:Header>
    <urn:SAAHeader Id="SAAHeader">
      <urn:SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</urn:SessionToken>
    </urn:SAAHeader>
  </soapenv:Header>
  <soapenv:Body>
    <urn:Close />
  </soapenv:Body>
</soapenv:Envelope>
```

Close response

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <CloseResponse xmlns="urn:swift:saa:xsd:soapha">
      <Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
        xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
        xmlns:SwInt="urn:swift:snl:ns.SwInt" xmlns:SwSec="urn:swift:snl:ns.SwSec">
        <Saa:Header>
          <Saa:SessionStatus>
            <Saa:MessagePartner>SoapHA</Saa:MessagePartner>
            <Saa:CreationTime>20081203132739</Saa:CreationTime>
            <Saa:SessionNr>0001</Saa:SessionNr>
            <Saa:InputFile />
            <Saa:.IsSuccess>true</Saa:.IsSuccess>
            <Saa:Accepted>1</Saa:Accepted>
            <Saa:Rejected>0</Saa:Rejected>
          </Saa:SessionStatus>
        </Saa:Header>
      </Saa:DataPDU>
    </CloseResponse>
  </S:Body>
</S:Envelope>
```

A.1.6.10.3 Put

Description

This operation allows a back-office application to send SOAP messages containing MT, XML-based, or FileAct messages to the Alliance Access SOAP host adapter.

Input

Put - This element contains the XMLv2 Message element as described in "Message" on page 695.

SAAHeader - The SAAHeader contains the session token of the session being used and the sequence number associated to the message sent.

Output

PutResponse - This element contains the XMLv2 MessageStatus element as described in "MessageStatus" on page 716.

SAAHeader - The SAAHeader contains the session token of the session being used and the sequence number associated to the message sent.

Example

Put request

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:swift:saa:xsd:soapha">
<soapenv:Header>
<urn:SAAHeader Id="SAAHeader">
  <urn:SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</urn:SessionToken>
  <urn:SequenceNumber>1</urn:SequenceNumber>
</urn:SAAHeader>
</soapenv:Header>
<soapenv:Body>
<urn:Put>
  <DataPDU xmlns="urn:swift:saa:xsd:saa.2.0">
    <Revision>2.0.2</Revision>
    <Header>
      <Message>
        <SenderReference>REF10812031316</SenderReference>
        <MessageIdentifier>fin.999</MessageIdentifier>
        <Format>MT</Format>
        <Sender>
          <BIC12>SAASBEBBAXXX</BIC12>
          <FullName>
            <X1>SAASBEBBAXXX</X1>
          </FullName>
        </Sender>
        <Receiver>
          <BIC12>SAATBEBBXXXX</BIC12>
          <FullName>
            <X1>SAATBEBBXXXX</X1>
          </FullName>
        </Receiver>
        <InterfaceInfo>
          <UserReference>REF10812031316</UserReference>
        </InterfaceInfo>
        <NetworkInfo>
          <FINNetworkInfo />
        </NetworkInfo>
        <SecurityInfo>
          <FINSecurityInfo />
        </SecurityInfo>
      </Message>
    </Header>
  <Body>DQo6MjA6VFJOIEZUSTAwMA0KOjc50lpaWlpaWlpaWlpaWlpaWlpa</Body>
</DataPDU>
</urn:Put>
</soapenv:Body>
</soapenv:Envelope>

```

Put response

```

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Header>
  <SAAHeader Id="SAAHeader" xmlns="urn:swift:saa:xsd:soapha">
    <SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</SessionToken>
    <SequenceNumber>1</SequenceNumber>
  </SAAHeader>
</S:Header>
<S:Body>
  <PutResponse xmlns="urn:swift:saa:xsd:soapha">
    <Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
      xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
      xmlns:SwInt="urn:swift:snl:ns.SwInt" xmlns:SwSec="urn:swift:snl:ns.SwSec">
      <Saa:Revision>2.0.2</Saa:Revision>
    <Saa:Header>
      <Saa:MessageStatus>
        <Saa:SenderReference>REF10812031316</Saa:SenderReference>
    
```

```

<Saa:SeqNr>000001</Saa:SeqNr>
<Saa:.IsSuccess>true</Saa:.IsSuccess>
</Saa:MessageStatus>
</Saa:Header>
</Saa:DataPDU>
</PutResponse>
</S:Body>
</S:Envelope>

```

A.1.6.10.4 GetAck

Description

This operation allows a back-office application to request, from the Alliance Access SOAP host adapter, MT, XML-based, or FileAct messages that are waiting for delivery in the exit point associated to the Alliance Access message partner. It also acknowledges the reception of the messages sent by Alliance Access.

Input

GetAck - This element contains a time-out after which Alliance Access replies that no messages are to be returned to the application.

GetAck

Name	Type	Description	Allowed values
Timeout	Timeout		Between 1 and 100 seconds inclusive

SAAHeader - The SAAHeader contains the session token of the session being used, the reference the back-office associates to the message it receives, the reference of the message for which it acknowledges reception (for more information, see "SOAP Message - soapenv:Envelope" on page 593).

Output

GetAckResponse - This element contains an XMLv2 element whose type depends on the message retrieved from the exit point:

GetAckResponse

XMLv2 Element	Type of retrieved message	Document Reference
TransmissionReport	Transmission notification	"TransmissionReport" on page 711
DeliveryReport	Delivery notification reconciled with the original message	"DeliveryReport" on page 715
HistoryReport	History or information notification	"HistoryReport" on page 709
DeliveryNotification	Delivery notification	"DeliveryNotification" on page 713
Message	Message sent from Alliance Access to the back-office application	"Message" on page 695

If there is no message to be retrieved, then the SAAHeader does not include any sequence number.

SAAHeader - The SAAHeader contains the session token of the session being used and the sequence number used by Alliance Access to identify the message.

Example

GetAck request

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:swift:saa:xsd:soapha">
<soapenv:Header>
<urn:SAAHeader Id="SAAHeader">
  <urn:SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</urn:SessionToken>
  <urn:ClientRef>REF1</urn:ClientRef>
</urn:SAAHeader>
</soapenv:Header>
<soapenv:Body>
  <urn:GetAck />
</soapenv:Body>
</soapenv:Envelope>

```

GetAck response with a Message as XMLv2 element.

```

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Header>
<SAAHeader Id="SAAHeader" xmlns="urn:swift:saa:xsd:soapha">
  <SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</SessionToken>
  <SequenceNumber>1</SequenceNumber>
  <ClientRef>REF1</ClientRef>
</SAAHeader>
</S:Header>
<S:Body>
  <GetAckResponse xmlns="urn:swift:saa:xsd:soapha">
    <Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
      xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
      xmlns:SwInt="urn:swift:snl:ns.SwInt" xmlns:SwSec="urn:swift:snl:ns.SwSec">
      <Saa:Revision>2.0.2</Saa:Revision>
      <Saa:Header>
        <Saa:Message>
          <Saa:SenderReference>REF10812031316</Saa:SenderReference>
          <Saa:MessageIdentifier>fin.999</Saa:MessageIdentifier>
          <Saa:Format>MT</Saa:Format>
          <Saa:SubFormat>Input</Saa:SubFormat>
        <Saa:Sender>
          <Saa:BIC12>SAASBEBBAXXX</Saa:BIC12>
        <Saa:FullName>
          <Saa:X1>SAASBEBBAXXX</Saa:X1>
        </Saa:FullName>
      <Saa:Sender>
        <Saa:Receiver>
          <Saa:BIC12>SAATBEBBXXXX</Saa:BIC12>
        <Saa:FullName>
          <Saa:X1>SAATBEBBXXXX</Saa:X1>
        </Saa:FullName>
      <Saa:Receiver>
        <Saa:InterfaceInfo>
          <Saa:UserReference>REF10812031316</Saa:UserReference>
          <Saa:MessageCreator>ApplicationInterface</Saa:MessageCreator>
          <Saa:MessageContext>Original</Saa:MessageContext>
          <Saa:MessageNature>Text</Saa:MessageNature>
        <Saa:InterfaceInfo>
          <Saa:NetworkInfo>
            <Saa:Priority>Normal</Saa:Priority>
            <Saa:IsPossibleDuplicate>false</Saa:IsPossibleDuplicate>
            <Saa:IsNotificationRequested>false</Saa:IsNotificationRequested>
            <Saa:Service>swift.fin</Saa:Service>
            <Saa:Network>Application</Saa:Network>
            <Saa:SessionNr>0001</Saa:SessionNr>
          <Saa:SeqNr>000001</Saa:SeqNr>
          <Saa:FINNetworkInfo>
            <Saa:MessageSyntaxVersion>0805</Saa:MessageSyntaxVersion>
            <Saa:CorrespondentInputTime>20081203122109</Saa:CorrespondentInputTime>

```

```
</Saa:FINNetworkInfo>
</Saa:NetworkInfo>
</Saa:Message>
</Saa:Header>
<Saa:Body>DQo6MjA6VFJOIEZUSTAwMA0KOjc5OlpaWlpaWlpaWlpaWlpa</
Saa:Body>
</Saa:DataPDU>
</GetAckResponse>
</S:Body>
</S:Envelope>
```

A.1.6.10.5 Ack

Description

This operation allows a back-office application to acknowledge the last message it received from the Alliance Access SOAP host adapter.

Input

Ack - Empty

SAAHeader - The SAAHeader contains the session token of the session being used, the reference of the message for which it acknowledges reception. For more information, see "SAA Header Block - soapha:SAAHeader" on page 593.

Output

AckResponse - Empty

SAAHeader - The SAAHeader contains the session token of the session being used.

Example

Ack request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:swift:saa:xsd:soapha">
<soapenv:Header>
<urn:SAAHeader Id="SAAHeader">
<urn:SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</urn:SessionToken>
<urn:AckClientRef>REF1</urn:AckClientRef>
</urn:SAAHeader>
</soapenv:Header>
<soapenv:Body>
<urn:Ack />
</soapenv:Body>
</soapenv:Envelope>
```

Ack response

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Header>
<SAAHeader Id="SAAHeader" xmlns="urn:swift:saa:xsd:soapha">
<SessionToken>1be691d7-97d5-4a49-8b70-88a63013d447</SessionToken>
<AckClientRef>REF1</AckClientRef>
</SAAHeader>
</S:Header>
<S:Body>
<AckResponse xmlns="urn:swift:saa:xsd:soapha" />
</S:Body>
</S:Envelope>
```

A.1.7 WebSphere MQ

Overview

The WebSphere MQ method enables files and SWIFT messages to be exchanged between Alliance Access and back-office applications through IBM WebSphere MQ. The WebSphere MQ connection method requires the licence package **13:MQ HOST ADAPTER**.

The WebSphere MQ connection method supports the following data formats:

- MQ-MT
- XML version 2

Alias queues, remote queues, and clustered queues are supported.

A.1.7.1 Configuration of WebSphere MQ

Overview

Before you use the WebSphere MQ Host Adapter in Alliance Access, you may have to define the environment variables as described in this section. This will depend on how you have configured your IBM WebSphere MQ software, and where it is installed.

If none of these environment variables are set, then default locations are searched.

A.1.7.1.1 Installation Directory for WebSphere MQ

WebSphere MQ on UNIX or Linux platforms

On UNIX or Linux, the following table provides the default directory where IBM WebSphere MQ is installed on the Alliance Access machine:

Platform	Default location
AIX	/usr/mqm/lib
Oracle Solaris	/opt/mqm/lib
Linux	/opt/mqm/lib

If the WebSphere MQ software is not installed in the default directory, then you must add the following line to the Alliance Access instance file, **.swa.\$ALLIANCE_INSTANCE.rc**:

Platform	Line to add to the instance file
AIX	export LIBPATH=\$LIBPATH:/fileys1/mqm/lib
Linux	
Oracle Solaris	LD_LIBRARY_PATH=\$LD_LIBRARY_PATH:/fileys1/mqm/lib

The following conditions apply for the UNIX platform:

- /fileys1/mqm/lib is a directory containing the WebSphere MQ library
- The Alliance Access instance file is located in the home directory of the Alliance Access Administrator (\$ALLIANCE_INSTANCE is the environment variable describing the name of the Alliance Access instance). This file is a hidden file.

WebSphere MQ on Windows platform

On Windows, ensure that the IBM WebSphere MQ environment variables are defined in the System Properties (Advanced tab) in the Control Panel.

A.1.7.1.2 Connection to WebSphere MQ Client

Purpose

There are two ways to implement the WebSphere MQ Host Adapter as a WebSphere MQ client:

- define the location of the WebSphere MQ Queue Manager using an environment variable, **MQSERVER**
- install a WebSphere MQ channel table, using two environment variables, **MQCHLTAB** and **MQCHLLIB**

Location of the WebSphere MQ Queue Manager

The easiest way to implement a WebSphere client is to define the environment variable, **MQSERVER**.

The value of **MQSERVER** contains the TCP/IP and WebSphere MQ parameters that are required for the connection to the WebSphere MQ Queue Manager:

Platform	Action to take
UNIX or Linux	Add the following line to the Alliance Access instance file .swa.\$ALLIANCE_INSTANCE.rc : <code>export MQSERVER=CHANCLI/TCP/'111.222.333.444(1414)'</code>
Windows	Define an environment variable in the System Properties (Advanced tab) in the Control Panel: <ul style="list-style-type: none"> • Variable name: MQSERVER • Variable value: CHANCLI/TCP/111.222.333.444(1414)

Using this environment variable limits access to a single WebSphere MQ Queue Manager. For more information about the **MQSERVER** variable, see the information about using IBM WebSphere MQ environment variables in the WebSphere MQ documentation about clients.

WebSphere MQ Channel Table

The second way to implement a WebSphere client is to install a WebSphere MQ channel table on the Alliance Access machine. The channel table describes all the WebSphere MQ channels that can be used to reach different WebSphere MQ Queue Managers.

In this case, the following two environment variables must be defined:

- **MQCHLTAB** defines the file name where channels are described. The default file name is **AMQCLCHL.TAB**.
- **MQCHLLIB** defines the directory where the channel file is located.

For example:

Platform	Action to take
UNIX or Linux	Add the following lines to the Alliance Access instance file .swa.\$ALLIANCE_INSTANCE.rc : <code>export MQCHLTAB=<filename></code>

Platform	Action to take
	<code>export MQCHLLIB=<pathname></code>
Windows	<p>Define the environment variables in the System Properties (Advanced tab) in the Control Panel:</p> <ul style="list-style-type: none"> • Variable name: MQCHLTAB Variable value: <filename> • Variable name: MQCHLLIB Variable value: <pathname>

A.1.7.2 WebSphere MQ Concepts

Introduction

WebSphere MQ is a communications system that provides asynchronous delivery of data across a broad range of hardware and software platforms.

This section provides a brief overview of the four fundamental concepts in WebSphere MQ:

- messages
- queues
- queue managers
- channels

For more information about WebSphere MQ, see the WebSphere MQ documentation.

A.1.7.2.1 WebSphere MQ Messages

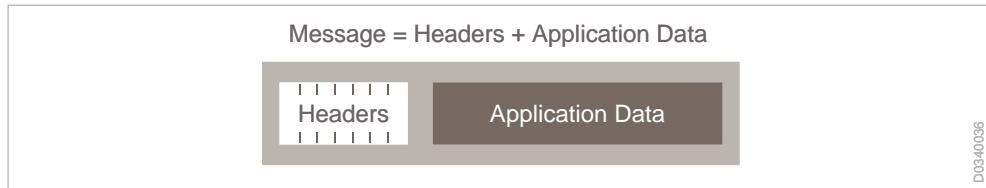
Definition

Applications use messages to exchange data. A WebSphere MQ *message* is a string of bytes that has a meaning for the applications that use it. The applications can be running on the same platform, or on different platforms.

A physical MQ message is the smallest unit of information that can be placed on or removed from a queue. A WebSphere MQ message has two parts:

- header (also called message descriptor)
- application data (the payload)

The message descriptor identifies the message and contains control information. The Alliance Access defines the structure of the application data.

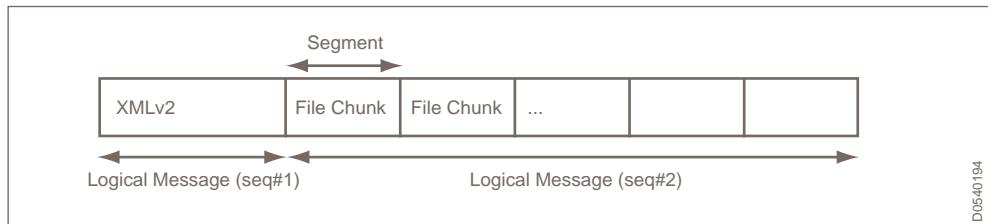


Logical MQ messages

If the payload of the message is extremely large, then it can be split across several messages. WebSphere MQ can group several physical messages together into a group of logical messages or it can segment the physical message into several file chunks and group them into one logical message. The distribution depends on the functionality support by the applications.

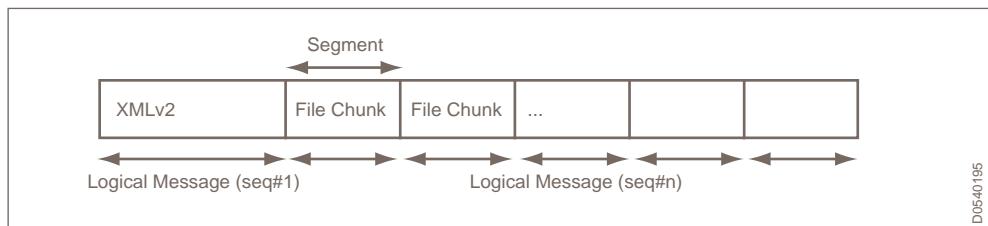
With a large message is segmented, each physical message in the group has the same Group Identifier and Message Sequence Number (GroupID and MsgSeqNumber) in their Message Descriptor parts. However, the Message identifier and Offset values (MsgId, and Offset) in their Message Descriptor parts differ.

The following diagram shows a file that is segmented and grouped into two logical messages:



With a large message is not segmented and is only grouped, then each physical message in the group has the same Group Identifier (GroupID) in their Message Descriptor parts.

The following diagram shows a file that is not segmented but is grouped into several logical messages:

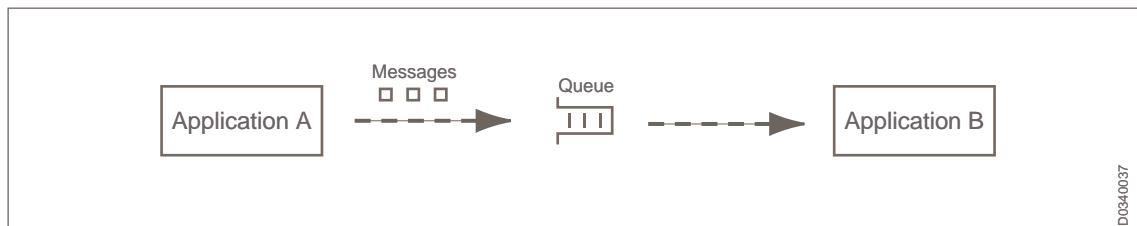


For more information about the components of an MQ message, see the WebSphere MQ documentation.

A.1.7.2.2 WebSphere MQ Queues

Definition

A WebSphere MQ *queue* is a data structure in which messages are stored. The messages may be put on or retrieved from the queue by applications. Queues exist independently of the applications that use them.



A.1.7.2.3 Queue Managers and MQI Channels

Queue manager

A WebSphere MQ *queue manager* is an entity that provides queue-based services to applications, and manages the queues that belong to it. Such queues are referred to as *local queues* for that queue manager. The queue manager ensures that messages are put on the correct queue, as requested by the application. Every queue belongs to a single queue manager. The same queue name can exist in different queue managers.

Applications put messages on and get messages from queues. For that purpose, applications must connect to a queue manager that is said to be a *local queue manager* for that application.

In a simple configuration, a single queue manager is created and local queues are defined on this queue manager. Applications can then connect to this queue manager and can use its queues to exchange messages.

MQI channel

An application connects to a queue manager through an MQI channel. An MQI channel is bi-directional, it must be created as a **Server-connection Channel** on the queue manager (see the WebSphere MQ clients documentation).

A.1.7.2.4 Remote Queue Managers and Message Channels

About remote queue managers

An application can get messages only from the local queues of a local queue manager. However, an application can put a message in a queue managed by a queue manager to which it is not directly connected. Such a queue manager is a *remote queue manager* for that application and the queues are said to be *remote queues*. An application addresses a queue by specifying its queue name and the name of the queue manager that manages that queue.

About message channels

A *message channel* (not to be confused with an MQI channel) provides a communication path between two queue managers. The message channel is used to transmit messages from one queue manager to another, and shields the application programs from the complexities of the underlying networking protocols. A message channel can transmit messages in one direction only. Two message channels are required if you required bi-directional communication between two queue managers. The configuration of message channels is out of the scope of this document. For more information, see the WebSphere MQ documentation.

Note	Do not confuse the concept of local and remote queue managers with that of a local or remote physical location. For example, you can have a local queue manager that connects to an application by an MQI channel while the application and the queue managers reside on different systems.
-------------	---

A.1.7.2.5 Application Connectivity

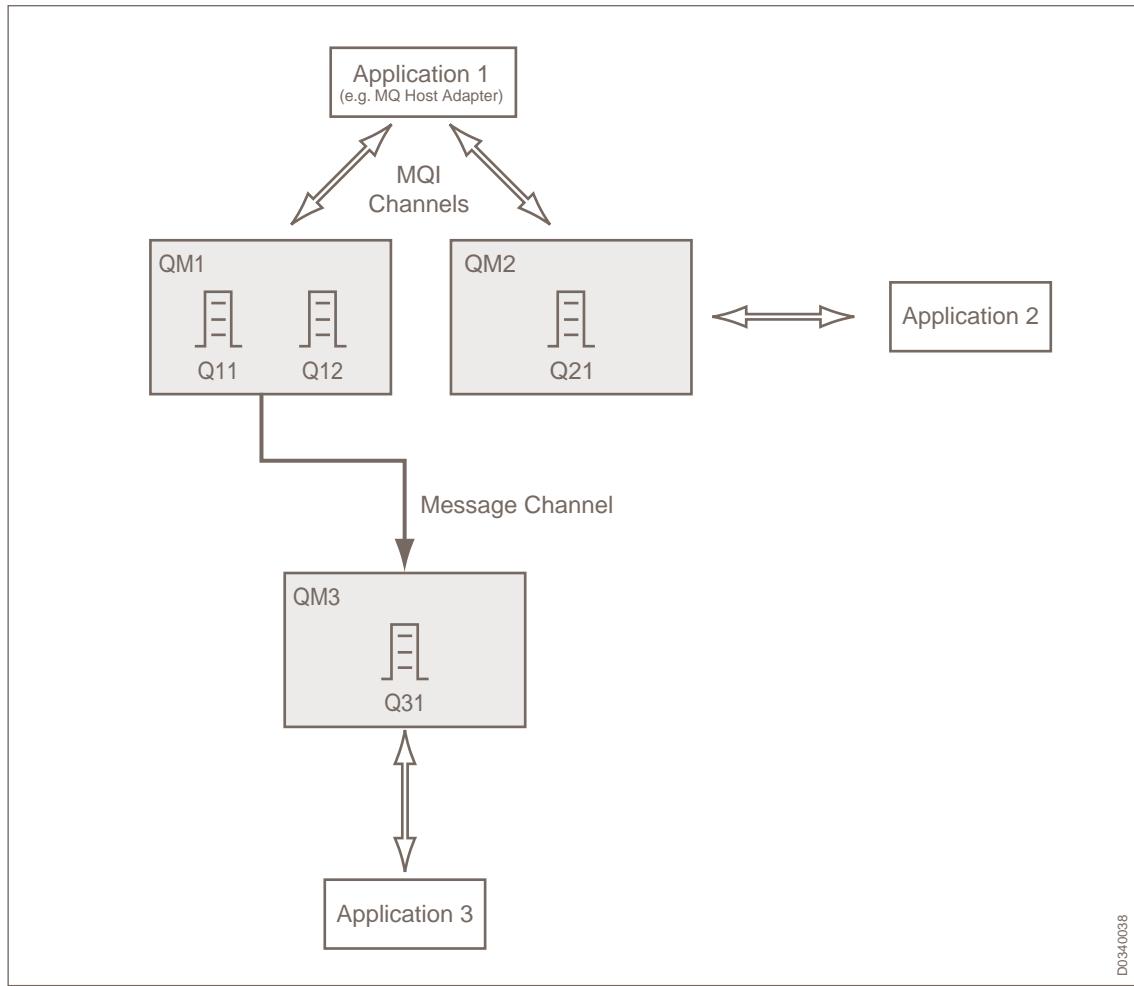
Specification requirements

Applications may connect directly to several local queue managers, by establishing several MQI channels. When an application tries to establish a connection to a queue, it must specify the queue address and the MQI channel to a local queue manager through which the queue is reached. The queue address consists of the queue name and queue manager name.

A.1.7.2.6 WebSphere MQ Concept Summary

Illustration of concepts

The following diagram provides an overview of the fundamental WebSphere MQ concepts:



D0340038

Note The concept queue managers shown in the graphic are abbreviated for simplicity, for example, QM1, QM2, and QM3.

Local and remote queue managers

QM1 is a *local queue manager* for **Application 1**.

QM2 is a *local queue manager* for **Application 1** and **Application 2**.

QM3 is a *local queue manager* for **Application 3** and a *remote queue manager* for **Application 1**.

Local and remote queues

Q11 and **Q12** are *local queues* of **QM1**.

Q21 is a *local queue* of **QM2**.

Q31 is a *local queue* of **QM3**, but also a *remote queue* for **QM1**.

Client channels and message channels

Application 1 is connected directly to **QM1** and **QM2** by two *MQI channels*.

Application 2 is connected directly to **QM2** with one *MQI channel*.

Application 3 is connected directly to **QM3** with one *MQI channel*.

QM1 can transmit messages to **QM3** using the *message channel*.

Application 1 can put messages on **Q31** of **QM3** using its *MQI channel* to **QM1**.

A.1.7.3 Structure of a WebSphere MQ Message

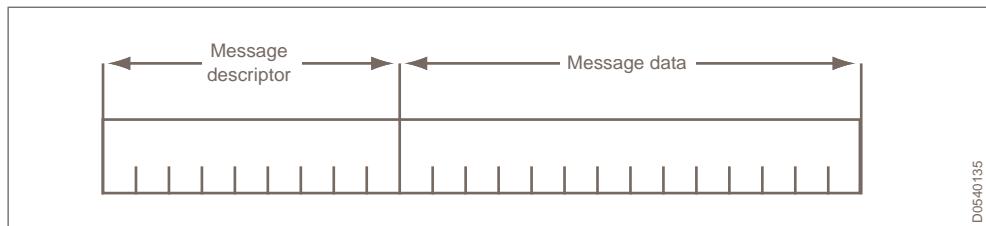
Description

Alliance Access supports the following types of WebSphere MQ messages:

- Datagram (`MQMT_DATAGRAM`)
- Request (`MQMT_REQUEST`)
- Report (`MQMT_REPORT`), a response message for an `MQMT_DATAGRAM`
- Reply (`MQMT_REPLY`), a response message for an `MQMT_REQUEST`

WebSphere MQ message

The following diagram shows the structure of a WebSphere MQ message:



Elements in an MQ Message

The following table describes the parts in an MQ message that Alliance Access interprets to process the message successfully. The elements that Alliance Access requires are marked as Mandatory (M). If an element is marked optional (O), and has a non-null value, then Alliance Access processes it appropriately:

Description of the elements

Part	Description	From ⁽¹⁾	To ⁽²⁾	To (Resp) ⁽³⁾
MQMessageDescriptor or	Contains the WebSphere MQ-defined fields. The following sections outline the fields that Alliance Access can modify in the MQ Descriptor. See "MQ Message Descriptor" on page 612.	M	M	M

Part	Description	From ⁽¹⁾	To ⁽²⁾	To (Resp) ⁽³⁾
MQMessageData	<p>Contains the message that is being exchanged between applications.</p> <p>The message data part is sent in one of the following transport formats:</p> <ul style="list-style-type: none"> MQ-MT (MQ-MT message) See "MQ-MT Format" on page 635. XML version 2 (DataPDU) See "XML Version 2 (XMLv2)" on page 685. 	M	M	O

(1) Represents a message request that Alliance Access receives from a message partner.

(2) Represents a notification, a system message, or a message request that Alliance Access sends to a message partner.

(3) Represents a response message request that Alliance Access sends to a message partner.

A.1.7.4 MQ Message Descriptor

Introduction

This section describes the elements that are included in the MQ Message Descriptor when it is included in the following messages:

- Message Request, that Alliance Access receives from a message partner through WebSphere MQ
- Message Response, that Alliance Access sends to WebSphere MQ, if it is requested
- Message Request, that Alliance Access sends to a message partner through WebSphere MQ
- Notification message or a System message, that Alliance Access sends to a message partner through WebSphere MQ, if it is requested.

Note This section describes the elements in the MQ Descriptor that Alliance Access interprets when it processes an MQ message. It does not describe all the elements of the MQ Descriptor. The elements that Alliance Access requires are marked as Mandatory (M). If an element is marked Optional (O) and has a non-null value, then Alliance Access processes it.

For more information about the elements in the MQ Descriptor, see the [IBM WebSphere MQ Application Programming Reference](#).

A.1.7.4.1 Message Request from WebSphere MQ to Alliance Access

Message Request

In this section, a message request is an MT or MX message that a back-office application sends to Alliance Access through WebSphere MQ.

Description of elements

The elements in the MQ Message Descriptor have the following values when they are included in a message request from a back-office application:

Elements in MQMessageDescriptor

Element	Description	Mandatory?
MsgType	<p>The type of message, which is one of the following:</p> <ul style="list-style-type: none"> Request (<code>MQMT_REQUEST</code>), which requires a response from Alliance Access Datagram (<code>MQMT_DATAGRAM</code>), which does not require a response from Alliance Access 	M
Report	<p>This element is present if an application requires a report message, regarding one of the following:</p> <ul style="list-style-type: none"> a report about the success of actions that relate to the original message the action to take when processing the MsgID or CorrelID in the message <p>Alliance Access can interpret the following values⁽¹⁾ in the <code>Report</code> element:</p> <p><code>MQRO_PAN</code> <code>MQRO_NAN</code> <code>MQRO_NEW_MSG_ID</code> <code>MQRO_PASS_MSG_ID</code> <code>MQRO_COPY_MSG_ID_TO_CORREL_ID</code> <code>MQRO_PASS_CORREL_ID</code></p>	O
CodedCharSetID	<p>The Coded Character Set ID (CCSID) which is the character set identifier of data in the message.</p> <p>Alliance Access converts the message request to <code>UTF8</code> character sets before reading it from a queue.</p>	M
Format	<p>A code that an application uses to indicate the nature of the data in the message.</p> <p>Alliance Access can interpret the following values⁽²⁾ in the <code>Format</code> element:</p> <p><code>MQFMT_STRING</code> <code>MQFMT_NONE</code> <code>MQFMT_MD_EXTENSION</code> <code>MQFMT_REF_MSG_HEADER</code> <code>MQFMT_DEAD_LETTER_HEADER</code> <code>MQFMT_IMS</code> <code>MQFMT_IMS_VAR_STRING</code></p>	M
MsgId	<p>A message identifier which an application uses to distinguish one message from another.</p> <p>Present if the application requires a response for the message.</p>	O
ReplyToQ	<p>The name of the queue to which Alliance Access sends the requested report.</p> <p>Present if the <code>MsgType</code> is "<code>MQMT_REQUEST</code>".</p>	O
ReplyToQMgr	<p>The Queue Manager, which is the owner of the <code>ReplyToQ</code> queue.</p> <p>Present if the <code>MsgType</code> is "<code>MQMT_REQUEST</code>".</p>	O

Element	Description	Mandatory?
Priority	The priority that WebSphere MQ assigns to the message	M
CorrelID	The correlation identifier	O
BackoutCount	A count that WebSphere MQ uses to detect errors that arise from processing. The queue manager fills this field automatically. If this field is not "0", then Alliance Access sets the Possible Duplicate Emission flag of the message to "true".	M

- (1) For information about how Alliance Access uses these values, see "Message Response to WebSphere MQ" on page 614. You can find a detailed description of these values in the [IBM WebSphere MQ Application Programming Reference](#).
- (2) You can find a detailed description of these values in the [IBM WebSphere MQ Application Programming Reference](#).

A.1.7.4.2 Message Response to WebSphere MQ

Overview

You can reconcile WebSphere MQ messages using the report message feature of WebSphere MQ. The report message (either a Report or a Reply) provides information about the initial processing that Alliance Access has performed on the message. The report message provides the Alliance Access instance that processed the message, the UUMID, and error validation information.

An application can request a report for a message optionally, by including a `Report` element in the MQ Message Descriptor part of the message. The `Report` element can also specify how to set the message and correlation identifiers in the report message.

If an application requests a report message and if one of the following conditions are met, then Alliance Access creates a Message Response for the message:

- The `MsgType` of the original message is "*Datagram*" and MQ requested either a PAN or a NAN report for the message.
- The `MsgType` of the original message is "*Request*".

If Alliance Access creates a Message Response, then it sends it to the Queue and Queue Manager that are specified in the original Message Request.

Description of elements

The elements in the MQ Message Descriptor have the following values when they are included in a message response, which Alliance Access sends to WebSphere MQ:

Elements in MQMessageDescriptor

Element	Description	Availability
<code>MsgType</code>	The type of message response, which is one of the following: <ul style="list-style-type: none"> • Report (<code>MQMT_REPORT</code>), if the original message was a Datagram • Reply <code>MQMT_REPLY</code>, if the original message was a Request. 	M
<code>Feedback</code>	This field indicates whether an error was reported during the processing of the MQ Message Data.	M

Element	Description	Availability
	If no error is reported, then a PAN message is sent with value <code>MQFB_PAN</code> . If an error is reported, then a NAN message is sent with one of values outlined in the section, see "Feedback options for NAN" on page 616.	
CodedCharSetID	The Coded Character Set ID (CCSID) which is the character set identifier of data in the message. Alliance Access sends a message in one of these character sets before writing to a queue: <ul style="list-style-type: none">• ASCII, for MQ-MT format⁽¹⁾• UTF8, for XML version 2	M
Format	A code that an application uses to indicate the nature of the data in the message. Alliance Access uses the format, <code>MQFMT_STRING</code> for a response message.	M
MsgId	If the Report field of the original message contained <code>"MQRO_NEW_MSG_ID"</code> , then the MsgID of the message response is the SUMID + the Instance Number of the original message. If the Report field of the original message contained <code>"MQRO_PASS_MSG_ID"</code> , then the MsgID of the message response is the same as the MsgId of the original message.	M
Priority	The priority of the Message response is the same as the priority of the original message.	M
CorrelID	If the Report field of the original message contained <code>"MQRO_COPY_MSG_ID_TO_CORREL_ID"</code> , then the CorrelID of the message response is the same as the MsgID of this response message. If the Report field of the original message contained <code>"MQRO_PASS_CORREL_ID"</code> , then the CorrelID of the message response is the same as the MsgID of the original message.	M
AccountingToken	The value of the Unit element of the original message. This allows an application to track the cost associated with processing the message. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O
ApplIdentityData	Information about the originator of the message. <code><SAA instance name> / (<Queue name> Completed)</code> where <code><Queue name></code> is the queue in which the message is stored in Alliance Access. Present if Transfer SAA Info and Use MQ Descriptor are both selected in the message partner profile.	O
PutApplName	The name of the process Alliance Access process for the MQ Interface ("MXS_ha") The Queue manager fills this field automatically.	M

Element	Description	Availability
UserIdentifier	The name of the operating system user that owns the Alliance Access instance. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O

(1) For MQHA, the CCSID used is 437. For MQSA, the CCSID is the one configured as the default at the queue manager level.

Feedback options for NAN

The Feedback field in the MQ Message Descriptor indicates whether an error was reported during the processing of the MQ Message Data.

The value of the Feedback field depends on the message validation level that was requested in the message. If no validation was configured, then the feedback is always positive.

Feedback value	MQ code for Feedback	Description
FB_MSG_NOTVALIDATED	MQFB_APPL_FIRST + 1	The message failed validation
FB_MSG_NOTROUTED	MQFB_APPL_FIRST + 2	The routing of the message failed.

A.1.7.4.3 Request from Alliance Access to WebSphere MQ

Message request

In this section, a message request is an MT or an MX message that Alliance Access sends to a back-office application.

Description of elements

The elements in the MQ Message Descriptor have the following values when they are included in a request, which Alliance Access sends to WebSphere MQ:

Elements in MQMessageDescriptor

Element	Value	Availability
MsgType	The type of message, which is a MQMT_DATAGRAM	M
CodedCharSetID	The Coded Character Set ID (CCSID) which is the character set identifier of data in the message. Alliance Access sends a message in one of these character sets before writing to a queue: <ul style="list-style-type: none"> • ASCII, for MQ-MT format⁽¹⁾ • UTF8, for XML version 2 	M
Format	A code that an application uses to indicate the nature of the data in the message. Alliance Access uses the format, MQFMT_STRING.	M
MsgId	SUMID (16 bytes)	M
Priority	The Alliance Access priority of the message instance, mapped to the WebSphere scale of priorities.	M

Element	Value	Availability
AccountingToken	The value of the Unit element of the original message. This allows an application to track the cost associated with processing the message. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O
ApplIdentityData	Information about the originator of the message. <SAA instance name>/(<Queue name> Completed]) where <Queue name> is the queue in which the message is stored in Alliance Access. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O
PutApplName	The name of the process Alliance Access process for the MQ Interface ("MXS_ha") The Queue manager fills this field automatically.	M
UserIdentifier	The name of the operating system user that owns the Alliance Access instance. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O

- (1) For MQHA, the CCSID used is 437. For MQSA, the CCSID is the one configured as the default at the queue manager level.

A.1.7.4.4 Notification or System Message to WebSphere MQ

Overview

This section describes the elements that Alliance Access interprets in the MQ descriptor of notification messages and system messages.

Notification messages include Transmission, Delivery, Information, and History messages that Alliance Access creates from additional instances of a message, based on the results of message reconciliation.

A System message is a Delivery Notification that Alliance Access receives from the SWIFT network to provide status about the delivery of a message.

Transmission notification

A Transmission notification is a message representing the result of the transmission to the SWIFT network. SWIFT performs full syntax and semantic checks before it returns an acknowledgement (ACK). Other checks, such as validity of the sender and the receiver, are also performed. The checks can cause a message to be rejected and a negative acknowledgement (NAK) is returned in response.

Delivery Notification

A Delivery Notification is a message that provides status about the progress of message processing. Alliance Access receives delivery notification messages, which can be reconciled with the original message through a reference in the CorrelId field. You can also append the text of the original message to the Delivery Notification message.

Information notification

An information notification (also called an intervention) is a message that the Routing application in Alliance Access creates to show details about the result of routing or processing.

History notification

A history notification is a list of information notification that the Routing application in Alliance Access creates to provide an overview of the processing that Alliance Access performed on a message.

System message

To provide information about the delivery of a message, Alliance Access receives a Delivery Notification from SWIFTNet, which is of the following:

- MT messages: an MT 010, MT 011, MT 012, MT 015, or MT 019.
- MX or FpML messages: a response, that is, not a message.

When Alliance Access receives a Delivery Notification from SWIFTNet, it creates an original message instance for the Delivery Notification. If an application has requested a Delivery Notification for a message request, then Alliance Access sends the message instance for this Delivery Notification message to the application as a System Delivery Notification message.

Note As a result of reconciling the Delivery Notification from SWIFTNet, Alliance Access can create an additional message instance (of type Delivery Notification) for the message request instance. In this case, a Delivery Notification and System Delivery Notification message can exist for one message request. Since the priority of a System Message is higher than a notification message, Alliance Access may send a System Delivery Notification message to an application before it transmits a Transmission notification.

Description of elements

The elements in the MQ Message Descriptor have the following values when they are included in a notification or a system message, which Alliance Access sends to WebSphere MQ:

Elements in MQMessageDescriptor

Element	Description	Availability
MsgType	The type of message, which is a <code>MQMT_DATAGRAM</code>	M
CodedCharSetID	<p>The Coded Character Set ID (CCSID) which is the character set identifier of data in the message.</p> <p>Alliance Access sends a message in one of these character sets before writing to a queue:</p> <ul style="list-style-type: none"> • <code>ASCII</code>, for MQ-MT format⁽¹⁾ • <code>UTF8</code>, for XML version 2 	M
Format	<p>A code that an application uses to indicate the nature of the data in the message.</p> <p>Alliance Access uses the format, <code>MQFMT_STRING</code> .</p>	M
MsgId	SUMID (16 bytes)	M
Priority	The value "10" less the priority in the original message.	M

Element	Description	Availability
CorrelID	For a Transmission or and a Delivery notification message, the CorrelID is the same as the MsgId of the original message request. For an Information notification, a History notification, or a system message, the CorrelID is the SUMID.	M
AccountingToken	The value of the Unit element of the original message. This allows an application to track the cost associated with processing the message. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O
ApplIdentityData	Information about the originator of the message. <SAA instance name> / (<Queue name> where <Queue name> is the name of the exit point from where the message was processed by a message partner. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O
PutApplName	The name of the process Alliance Access process for the MQ Interface ("MXS_ha") The Queue manager fills this field automatically.	M
UserIdentifier	The name of the operating system user that owns the Alliance Access instance. Present if Transfer SAA Information and Use MQ Descriptor are both selected in the message partner profile.	O

(1) For MQHA, the CCSID used is 437. For MQSA, the CCSID is the one configured as the default at the queue manager level.

A.1.7.5 FileAct over WebSphere MQ

Purpose

The WebSphere Host Adapter allows the FileAct messages to use the same queues as the other message flows. This makes Alliance Access easier to integrate with back-office applications, and allows several instances of Alliance Access to read from the same MQ queue. To achieve this, you must select Full FileAct mode in the Message Partner profile.

The WebSphere Host Adapter supports the exchange of FileAct messages over WebSphere MQ in two modes:

- Full FileAct mode - where both the XML version-2 message and the FileAct payload are transferred between the back-office application and Alliance Access over WebSphere MQ.
- Mixed FileAct mode - where the XMLv2 message is transferred between the back-office application and Alliance Access over WebSphere MQ, and the FileAct payload is transferred over the local file system. This is similar to the File Transfer connection method.

Full FileAct mode

When the WebSphere Host Adapter is operating in Full FileAct Mode, it transfer messages or files over FileAct using two MQ messages:

- MQ message containing the FileAct settings in the XML version 2 format

This MQ message is associated with the MQ message that carries the payload.

- MQ message containing the file payload

If the payload is greater than the configured maximum size of a message at the queue manager or channel (**Chunk Size**) then the payload can be grouped or segmented into several MQ messages. For more information about calculating the **Chunk Size**, see "Calculation of Chunk Size" on page 620.

The MQ Host Adapter does not enforce the usage of message segmentation. The MQ Host Adapter supports the case where the FileAct payload is split into multiple logical messages that are part of the same group. In this case, the first logical message must be the XMLv2 message, and the other logical messages are the different chunks of the FileAct payload. For more information, see "WebSphere MQ Messages" on page 607.

The following outlines the segmentation and grouping that the WebSphere Host Adapter supports:

Direction	MQ Host Adapter supports	Limitation
Input from back-office application	any combination of both grouping and segmentation	The first logical message must not be segmented and must be the XMLv2 message.
Output to the back-office application	either segmentation or message grouping	This depends on the value of Don't use Segmentation and Chunk Size parameters in the message partner profile.

Calculation of Chunk Size

Ensure that both Alliance Access and the back-office application can handle the chunk sizes effectively.

For example, you can use the following formula to determine an effective value for **Chunk Size**:

`MAX_FileAct_Size / Chunk Size > MAX_Uncommitted message - 1`

where:

- `MAX_FileAct_Size` is the maximum FileAct payload size being exchanged.
The default is 250 Mb.
- `Chunk size` is the size of each chunk (default at SAA side is 32 Kb).
- `MAX_Uncommitted message` is the number of messages that a transaction can hold. You can configure this at the Queue manager side, and the default is 10,000.

1 is deducted because the XMLv2 message is always included before the chunks.

A.1.7.6 Management of a WebSphere MQ Session

Introduction

This section describes how Alliance Access recovers sessions with the MQ Host Adapter.

A.1.7.6.1 Recovery of a WebSphere MQ Connection

Overview

If the **Keep Session Open** option is selected in the message partner profile and a session connection is lost, then the session status changes to "Interrupted" and Alliance Access attempts to re-establish the connection to WebSphere MQ.

If the **Keep Session Open** option is not selected and a session connection is lost, then the session status changes to "Closed".

Recovery attempts

System parameters specify the frequency of the recovery attempts, as follows:

1. After the number of seconds that are specified in **Recovery Time - Initial** have elapsed, then Alliance Access attempts to re-open the session for the first time.
2. If the reconnection is unsuccessful, then Alliance Access increases the time between the reconnection attempts by the value specified in **Recovery Time - Increment**, and attempts to re-establish the connection.
3. The time interval between attempts is increased after every attempt until it reaches the value specified in **Recovery Time - Max**, after which Alliance Access attempts the reconnection at these intervals.

Recovery of a Full FileAct session

Alliance Access uses the WebSphere options, MQ MQGMO_ALL_MSGS_AVAILABLE and MQGMO_ALL_SEGMENTS_AVAILABLE. This ensures that Alliance Access processes a message only after all the segments and messages of the logical message are in the queue. If a segment is missing, then the Alliance Access does not process the logical message.

If Alliance Access exits unexpectedly while processing a message or segment, then the action can be recovered and all the messages that Alliance Access processed are rolled back and placed in the MQ queue again. The "Backout count" of these rolled-back messages are incremented and Alliance Access treats them as a Possible Duplicate the next time that it processes them.

When sending a FileAct message over WebSphere MQ, Alliance Access only routes the FileAct instance when the complete message has been sent to the back-office application.

After the message is sent, Alliance Access cannot know whether a segment is lost during its transfer. It is the responsibility of the WebSphere MQ infrastructure to ensure that no messages are lost. The application reading the FileAct messages can use the same set of options as Alliance Access to process messages only after all segments are present in the queue.

A.1.7.6.2 Closure of an MQ Session

Automatic sessions

If you close an automatic session for an incoming message partner (that is, with **From Message Partner** as the **Allowed direction**) or for an outgoing message partner (that is, with **To Message Partner** as the **Allowed direction**), then Alliance Access re-opens the session automatically. To avoid this session reopening, you must first disable the message partner and afterwards close the session.

Manual sessions

You can stop a manual session of either an incoming or outgoing message partner.

A.2 Message Formats

A.2.1 Common Application Server (CAS) Format

Overview

This section shows examples of messages accepted by Application Interface when processed using the Common Application Server (CAS) protocol. Alliance Access supports CAS protocol standards 1 and 2.

Note The CAS1 data format does not allow transmission of any authentication results. PKI signatures are not transmitted.

In the Application Interface, two connection methods currently support Common Application Server (CAS):

- **File Transfer (CAS).** File Transfer using the CAS message format permits you to send and receive batch message files in either Network Dependent Format (NDF) or the Network Independent Format (NIF).
- **Interactive.** Interactive permits you to send and receive individual messages either Network Dependent Format (NDF) or the Network Independent Format (NIF).

A.2.1.1 The Common Application Server (CAS) Protocol

Overview

As part of the Application Interface, Alliance Access supports CAS protocol standards 1 and 2. The Interactive and the File Transfer connection methods are used to transfer messages of a specified format between Alliance Access and a message partner. This transfer is carried out according to Common Application Server (CAS) standards.

Both CAS protocols provide a common form of access between SWIFT terminal products (CBTs) and back-office mainframe applications. In addition to this, using the CAS protocol permits Alliance Access to store messages received from networks other than SWIFT.

Messages received using the CAS protocol, may be formatted according to either the Network Dependent Format (NDF) or the Network Independent Format (NIF).

Network Dependent Format (NDF)

This format matches the SWIFT network. Using the NDF format, financial institutions currently communicating with ST400 systems can re-use much of their CAS application software when switching to Alliance Access.

Network Independent Format (NIF)

With this format, the body of the message is limited to the financial data, that is, block 4 of the SWIFT message format. The network-related information is in a network independent format.

Using the NIF syntax enables financial institutions to use Alliance Access to exchange and process messages which are coming from SWIFT or non-SWIFT networks, for example, CHIPS, CHAPS, Fedwire, SIC, and so on.

Network Format

Network	NDF	NIF
SWIFT	Application Service Profile	Application Service Profile
UNIX or Linux only: Sic	-	User Format Services (UFS)
UNIX or Linux only: Other networks	-	User Format Services (UFS)

CAS Message Encoding/Decoding

The NDF and NIF formats are defined using the ISO standard Abstract Syntax Notation 1 (ASN.1). Its companion, the Basic Encoding Rules (BER) Standard defines how data described using ASN.1 can be exchanged using a common transfer syntax.

The messages exchanged between Alliance Access and message partners are encoded to the common transfer syntax for transmission, and from the common transfer syntax on reception.

In addition to the ASN.1 notation used by both CAS 1 and CAS 2 standards, the CAS 2 standard also supports the notation, *Text Encoding*. This notation has been developed to simplify the implementation of the CAS protocol. The structure and parameters of the CAS protocol remain unchanged, but the text encoding method uses special text characters to delimit the start and end of each structure block and field within the message.

A.2.1.2 CAS Format

Example

The following is an example of a SWIFT input message in CAS format, with the Processing Data Units (PDUs) non-encoded

Note The example shows only the more commonly used fields. It does not contain all possible PDU fields available to the protocol.

```

MXADataPDU ::=

{
    version = 2
    senderReference = >NDF.SN2-RSVA<
    mxADataPDU = 1 (choice rank)
    message ::=

    {
        messageFormat = swiftNDF (0x1f)
        messageLPI ::=
        {
            dispositionState = ready (0x9)
            networkAttribute ::=
            {
                networkApplicationName = swiftInterface (0x1)
            } -- networkAttribute --
            targetApplication ::=
            {
                targetApplicationRule = cBTApplicationRule (0x2)
            } -- targetApplication --
        } -- messageLPI --
        messageText ::=
        {
    }
}

```

```

msgText =
  (00000000) 7B 31 3A 46 30 31 41 45 4E 54 42 45 44 41 41 58 >(1:F01AENTBEDAAX<
  (00000010) 58 58 2E 53 53 2E 2E 53 45 51 2E 2E 7D 7B 32 3A >XX.SS..SEQ..){2:<
  (00000020) 49 31 30 30 41 45 4E 54 42 45 44 41 58 58 58 58 >I100AENTBEDAXXX<
  (00000030) 55 7D 7B 33 3A 7B 31 30 38 3A 41 43 4B 20 20 20 >U){3:{108:ACK <
  (00000040) 4D 54 31 30 30 20 30 30 31 7D 7D 7B 34 3A 0D >MT100 0001}}{4:<
  (00000050) 0A 3A 32 30 3A 41 43 4B 20 20 20 4D 54 31 30 30 >.:20:ACK MT100<
  (00000060) 20 30 30 30 31 0D 0A 3A 33 32 41 3A 38 38 30 38 > 0001..:32A:8808<
  (00000070) 30 38 55 53 44 31 2C 0D 0A 3A 35 30 3A 58 0D 0A >08USD1,..:50:X.<
  (00000080) 3A 35 32 41 3A 41 45 4E 54 42 45 44 41 0D 0A 3A >:52A:AENTBEDA..:<
  (00000090) 35 33 41 3A 41 45 4E 54 42 45 44 41 0D 0A 3A 35 >53A:AENTBEDA..:5<
  (000000A0) 34 41 3A 41 45 4E 54 42 45 44 41 0D 0A 3A 35 36 >4A:AENTBEDA..:56<
  (000000B0) 41 3A 41 45 4E 54 42 45 44 41 0D 0A 3A 35 37 41 >A:AENTBEDA..:57A<
  (000000C0) 3A 41 45 4E 54 42 45 44 41 0D 0A 3A 35 39 3A 58 >:AENTBEDA..:59:XX<
  (000000D0) 58 0D 0A 3A 37 30 3A 58 0D 0A 3A 37 31 41 3A 4F >X..:70:X..:71:0<
  (000000E0) 55 52 0D 0A 3A 37 32 3A 2F 41 2F 31 32 33 34 35 >UR..:72:/A/12345<
  (000000F0) 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 >6789012345678901<
  (00000100) 32 33 34 35 36 37 38 39 30 0D 0A 2F 41 2F 34 35 >234567890..//A/45<
  (00000110) 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 >6789012345678901<
  (00000120) 32 33 34 35 36 37 38 39 30 0D 0A 2F 41 2F 34 35 >234567890..//A/45<
  (00000130) 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 >6789012345678901<
  (00000140) 32 33 34 35 36 37 38 39 30 0D 0A 2F 41 2F 34 0D >234567890..//A/4.<
  (00000150) 0A 2D 7D >.-}<
  } -- messageText --
} -- message --
} -- MXADataPDU --

```

A.2.1.3 CAS Message with ASN.1 Encoding

Example

The following example is a CAS message in network-dependent format (NDF), with ASN.1 encoding.

```

00000000 02 30 30 32 35 38 30 81 FF 80 01 02 81 17 4F 53 .002580.....09
00000010 57 41 4C 42 45 42 30 58 58 58 31 30 30 41 42 43 WALEBB0XXX100ABC
00000020 44 45 46 47 48 AA 81 E0 80 01 1F A4 15 80 01 01 DEFCH.....D
00000030 A8 03 80 01 01 8B 01 00 AD 03 80 01 01 8E 03 44 .....(1:F01SW
00000040 4F 43 A7 81 C3 84 81 C0 7B 31 3A 46 30 31 53 57 0C.....(1:F01SW
00000050 41 4C 55 53 33 30 41 58 58 58 30 30 35 38 30 30 ALUS30AXXXX005800
00000060 31 38 39 39 7D 7B 32 3A 4F 31 30 30 31 32 32 38 1899)(2:01001228
00000070 39 39 30 31 31 35 53 57 41 4C 42 45 42 30 41 58 990115SWALEBB0AX
00000080 58 58 30 34 32 31 30 30 36 33 32 36 39 39 30 31 XX04210063269901
00000090 31 35 30 36 32 39 4E 7D 7B 34 3A 0D 0A 3A 32 30 150629N)(4:...:20
000000A0 3A 41 42 43 44 45 46 47 48 0D 0A 3A 33 32 41 3A :ABCDEFGH..:32A:
000000B0 39 39 30 31 31 33 42 45 46 31 30 30 30 2C 0D 0A 990113BEF1000,..:
000000C0 3A 35 30 3A 41 42 43 44 45 46 47 48 0D 0A 3A 35 :50:ABCDEFGH..:5
000000D0 39 3A 41 42 43 44 45 46 47 48 0D 0A 2D 7D 7B 35 9:ABCDEFGH..-}{5
000000E0 3A 7B 4D 41 43 3A 30 44 38 33 42 33 36 30 7D 7B :(MAC:0D83B360){5
000000F0 43 48 4B 3A 39 41 31 30 42 41 43 35 42 42 31 30 CHK:9A10BAC5EB10
00000100 7D 7B 54 4E 47 3A 7D 7D 02 30 30 33 39 33 30 82 ){TNG:}).003930.
00000110 01 75 80 01 02 81 17 49 53 57 41 4C 55 53 33 30 .....ISWALUS30
00000120 58 58 58 31 30 30 41 42 43 44 45 46 47 48 AB 82 XX0100ABCDEFCH..
00000130 01 65 A0 0D 80 0B 53 57 41 4C 55 53 33 30 58 58 .....,SWALUS30XX
00000140 58 81 01 03 A2 81 B2 80 01 1F A4 05 A8 03 80 01 X.....(1:F01SWA
00000150 01 A7 81 A5 84 81 A2 7B 31 3A 46 30 31 53 57 41 .....(1:F01SWA
00000160 4C 42 45 42 30 41 58 58 58 30 34 32 31 30 30 36 LEBB0AXXXX0421006
00000170 33 32 36 7D 7B 32 3A 49 31 30 30 53 57 41 4C 55 326)(2:II00SWALU
00000180 53 33 30 58 58 58 58 4E 7D 7B 34 3A 0D 0A 3A 32 S30XXXXN)(4:...:2
00000190 30 3A 41 42 43 44 45 46 47 48 0D 0A 3A 33 32 41 0:ABCDEFGH..:32A
000001A0 3A 39 39 30 3 131 33 42 45 46 31 30 30 30 2C 0D :990113BEF1000,..:
000001B0 0A 3A 35 30 3A 41 42 43 44 45 46 47 48 0D 0A 3A ..:50:ABCDEFGH..:
000001C0 35 39 3A 41 42 43 44 45 46 47 48 0D 0A 2D 7D 7B 59:ABCDEFGH..-}{5
000001D0 35 3A 7B 4D 41 43 3A 30 44 38 33 42 33 36 30 7D 5:(MAC:0D83B360)
000001E0 7B 43 48 4B 3A 39 41 31 30 42 41 43 35 42 42 31 (CHK:9A10BAC5EB1
000001F0 30 7D 7B 54 4E 47 3A 7D 7D A3 1F A1 03 80 01 14 0)(TNG:)).....
00000200 82 01 00 83 01 01 86 0F 53 57 49 46 54 20 49 6E .....SWIFT In
00000210 74 65 72 66 61 63 65 87 01 01 AB 7B 80 01 01 A1 terface....{.....
00000220 03 80 01 01 82 02 01 A5 83 02 18 B6 85 01 02 A6 .....
00000230 66 30 64 80 01 00 81 0C 39 39 30 31 31 35 31 31 fod....99011511
00000240 33 31 31 36 82 0F 53 57 49 46 54 20 49 6E 74 65 3116..SWIFT Inte
00000250 72 66 61 63 65 83 06 53 59 53 54 45 4D 84 38 7E rface..SYSTEM.8(
00000260 31 3A 46 32 31 53 57 41 4C 42 45 42 30 41 58 58 1:F21SWALEBB0AXX
00000270 58 30 34 32 31 30 30 36 33 32 36 7D 7B 34 3A 7B X0421006326)(4:(
00000280 31 37 37 3A 39 39 30 31 31 35 31 32 32 38 7D 7B 177:9901151228)(4:(
00000290 34 35 31 3A 30 7D 7D 451:0})
```

A.2.1.4 CAS2 Message with ASN.1 Encoding

PKI signatures

If the **Transfer PKI Signatures** option is selected in the message partner profile, then the PKI signature is transferred in a new field `sigValue`. It contains the complete `Signature` element (as provided by SWIFTNet Link) that is relevant to the message. The `sigValue` field has a maximum size of 5000 bytes. Tag ID 21 is created in `MXAMessage.messageLPI` for this purpose.

If both a MAC-equivalent signature and a PAC2-equivalent signature are present, then the PAC2-equivalent is appended to the MAC-equivalent signature in the `sigValue` field.

Note Back-office applications must be ready to receive and store PKI signatures.

MAC/PAC values

If the **Always Transfer MAC/PAC** option has been selected for the message partner profile, and the message contains no MAC/PAC values, then dummy MAC/PAC trailers are added to

the MT message and sent to the back-office application. The value of these dummy MAC and PAC trailers is 00000000.

Signature result

The MAC-equivalent signature verification result is passed by means of the field `authResult`.

The PAC-equivalent signature verification result is passed by means of the field `pacResult`.

For dual-signed messages of type MT 096, the signature verification result of the PKI signatures will be passed in the existing `pacResult` tag.

The verification result has one of the following values:

- `successCurrent`
- `bypassed`
- `failed`

A.2.1.5 CAS Message with Text Encoding

Example

The following example is a CAS message in network-dependent format (NDF), with text encoding.

```

00000000 02 30 30 24 22 31 3A 41 56 45 52 3A 30 30 20 20 .00421:AMER:0000
00000010 31 3A 32 3A 53 52 45 46 3A 30 30 20 32 32 3A 4F 1:2:3REF:00023:0
00000020 53 57 41 4C 42 45 42 30 58 58 58 31 30 30 41 42 #NAME#0000000000000000
00000030 42 44 45 46 47 48 23 4D 4D 52 47 3A 4D 46 4F 52 #DE#0000000000000000
00000040 3A 30 30 30 30 38 3A 73 77 69 66 74 4E 44 46 23 :00008:swift#MFI#
00000050 4D 4C 50 49 3A 4F 4D 53 47 3A 30 30 30 30 34 3A #NAME#00004:00004:
00000060 54 72 75 65 23 4E 45 54 41 3A 4E 57 41 4E 3A 30 True#NETA:NAME:0
00000070 30 30 31 34 3A 73 77 69 66 74 49 6E 74 65 72 66 0014:swiftInterface
00000080 61 62 65 2A 4E 45 54 41 3A 41 55 54 52 3A 30 30 ac#NETA:AUTH:0000
00000090 30 31 34 3A 73 75 63 65 73 73 42 75 72 72 65 014:success#Curre
000000A0 6E 74 23 4D 4F 52 47 3A 42 42 54 41 3A 30 30 30 nt#MORG:NETA:000
000000B0 31 34 3A 72 77 69 66 74 49 6E 74 65 72 66 61 62 14:swiftInterface
000000C0 65 2A 4D 4F 52 47 3A 52 4F 55 54 2A 30 30 30 30 e#MORG:ROUT:0000
000000D0 32 3A 44 4F 42 3A 4D 4C 50 49 23 4D 54 58 54 3A 3:DOC#MLPI#TEXT:
000000E0 54 45 58 54 2A 30 30 21 39 22 3A 7B 31 3A 46 30 TEXT:00132:(1..F0
000000F0 31 52 57 41 4C 55 52 23 30 41 58 58 58 30 30 25 #NAME#0000000000000000
00000100 28 30 30 31 28 29 39 7D 7E 32 3A 4F 31 30 30 31 8001899)(2:0L001
00000110 32 32 38 29 29 30 31 21 35 53 57 41 42 45 42 228930115#NAME#
00000120 30 41 58 58 30 34 22 31 20 30 36 23 32 36 39 0ANXXX04210062269
00000130 39 30 31 31 25 30 36 22 39 4E 7D 7B 34 3A 0D 0A 9011506293N)(4:..
00000140 3A 32 30 3A 41 42 43 44 45 46 47 48 0D 0A 3A 33 :20:ABCDEFH..:2
00000150 32 41 3A 39 39 30 31 21 32 42 45 46 31 30 30 28:9901112#REF!1000
00000160 2C 02 0A 3A 35 30 3A 41 42 43 44 45 46 47 48 0D ..:50:ABCDEFH.
00000170 0A 3A 35 39 3A 41 42 43 44 45 46 47 48 0D 0A 2D ..:59:ABCDEFH..-
00000180 7D 7B 35 3A 7B 4D 41 42 3A 30 44 38 33 42 32 36 )(5:(#NAME#0D82B36
00000190 30 71 7B 42 44 4B 3A 29 41 31 30 42 41 43 35 42 0)(#NAME#9A10#REF!C5B
000001A0 42 31 30 7D 7B 54 4E 47 3A 7D 7B 3A 4D 54 58 54 810)(TNG:):#TEXT
000001B0 2A 4D 4D 52 47 02 30 30 37 39 37 3A 41 56 45 52 #NAME#00797:AMER
000001C0 3A 30 30 30 31 3A 22 3A 53 52 45 46 3A 30 30 :00001:2:3REF:0
000001D0 30 32 33 3A 49 53 57 41 4C 55 53 32 30 58 58 58 023:ISNAME#00000000
000001E0 31 30 30 41 41 42 44 45 46 47 48 23 4D 52 45 50 100#ABCDEFH#REF#
000001F0 22 41 44 44 52 3A 41 44 58 31 3A 30 20 30 31 31 #ADDR:ADCL:00011
00000200 3A 52 57 41 4C 55 52 23 30 58 58 58 2A 41 44 44 :#NAME#000000000000
00000210 52 2A 4F 4D 46 44 3A 20 30 30 24 3A 66 75 6C R:#REF!00004:ful
00000220 6C 23 4F 4D 52 47 3A 4D 4F 4F 52 3A 30 30 30 20 30 1#NAME#MFI#REF!0000
00000230 38 3A 72 77 69 66 74 4E 44 46 23 4D 52 45 50 45 23 8:swift#MFI#MLPI#
00000240 4E 45 54 41 3A 4E 57 41 4E 3A 30 30 30 31 34 3A #NAME#NAME:00014:
00000250 73 77 69 66 74 49 6E 74 65 72 66 61 63 65 3A 4E swiftInterface#N
00000260 45 54 41 3A 4D 4C 50 49 23 4D 54 58 54 3A 54 45 #NAME#MLPI#TEXT:TE
00000270 58 54 3A 30 30 31 36 32 3A 7B 31 3A 46 30 31 53 XT:00162:(1..F0L3
00000280 57 41 4C 42 45 42 30 41 58 58 58 30 34 32 31 30 #NAME#000000000000
00000290 30 36 33 32 3A 7D 7B 32 3A 49 31 30 30 53 57 41 06326)(2:IL0030A
000002A0 4C 55 53 33 30 58 58 58 4E 7D 7B 34 3A 0D 0A 1#NAME#000000000000
000002B0 3A 32 30 3A 41 42 43 44 45 46 47 48 0D 0A 3A 33 :20:ABCDEFH..:2
000002C0 32 41 3A 39 39 30 31 31 33 42 45 46 31 30 30 2A:9901112#REF!1000
.....
```

```
.....000002D0 2C 0D 0A 3A 35 30 3A 41 42 43 44 45 46 47 48 0D ..:50:ABCDEFCH. ....
000002E0 0A 2A 25 39 3A 41 42 43 44 45 46 47 48 0D 0A 2D ..:59:ABCDEFCH. -.
000002F0 7D 7B 35 3A 7B 4D 41 42 3A 30 44 38 33 42 33 36 )<5:(MAC:0D8EB36
00000300 30 7D 7B 42 48 4B 3A 39 41 21 30 42 41 42 35 42 0 )<(CHK:9A10EAC5B
00000310 42 31 20 7D 7B 54 4E 47 3A 7D 7D 2A 4D 54 58 54 E10 )<(TNG:)>*MTXT
00000320 2A 4F 4D 52 47 23 52 4C 50 49 23 4B 4F 52 49 3A *MSGHELPINMORI:
00000330 42 42 54 41 3A 30 30 31 32 3A 6D 65 73 72 61 CDTA:00012:mess
00000340 67 65 45 6E 74 72 73 2A 4D 4F 52 49 3A 4D 4F 44 geEntry*MOREI:MOD
00000350 49 3A 30 30 30 35 3A 46 61 6C 73 65 3A 4F 4D 1:00005:False:0M
00000360 52 47 3A 30 30 30 34 3A 54 72 75 65 3A 52 45 3C:00004:True:RE
00000370 50 41 3A 30 30 30 31 35 3A 53 57 49 46 54 21 49 PA:00015:SWIFT I
00000380 6E 74 65 72 66 61 63 65 3A 42 54 4E 4F 3A 30 30 nterface:BTNO:00
00000390 30 30 34 3A 54 72 75 65 2A 52 4C 50 49 23 54 52 004:True*MLPI#TR
000003A0 52 4D 3A 4E 45 54 57 3A 30 30 30 31 32 3A 73 77 SH:BTNO:00012:sw
000003B0 69 66 74 4E 65 74 77 6F 72 6B 23 4E 41 54 54 3A iftNetwork#NATT:
000003C0 4E 57 41 4E 3A 30 30 31 34 3A 72 77 69 66 74 NNAME:00014:swit
000003D0 49 6E 74 65 72 66 61 63 65 2A 4E 41 54 54 3A 4E Interface#NATT:N
000003E0 52 45 53 3A 30 30 30 32 3A 24 32 21 3A 4E 52 3E3:00003:421:MS
000003F0 45 51 3A 20 30 30 34 3A 31 32 32 36 3A 4F 44 EG:00004:62826:MD
00000400 4C 56 3A 30 30 31 32 3A 6E 65 74 77 6F 72 6B LU:00012:network
00000410 41 63 6E 65 64 22 49 4E 54 56 3A 49 42 41 54 3A Acked#INTV:ICAT:
00000420 30 20 20 32 36 3A 74 72 61 6E 73 6D 69 72 69 00026:transmissi
00000430 6F 6E 52 65 70 6F 72 74 42 61 74 65 67 6F 72 79 onReportCategory
00000440 3A 42 52 54 4D 3A 30 30 30 31 32 3A 29 39 30 31 :CTRM:00012:3901
00000450 31 35 31 31 33 31 31 36 3A 4L 50 50 4C 3A 30 30 15111116:APPL:00
00000460 30 31 25 3A 52 57 49 46 54 20 49 6E 74 65 72 66 015:SWIFT Interf
00000470 61 63 65 3A 4F 50 48 52 3A 30 30 20 20 36 32 52 arc:OPER:00006:3
00000480 59 52 54 45 4D 3A 54 45 50 54 3A 30 20 30 35 36 YSTEM:TEXT:00056
00000490 3A 7B 31 3A 46 32 31 53 57 41 4C 42 45 42 30 41 :(1:F2130A8E0B0A
000004A0 58 58 58 30 24 32 21 30 30 23 32 36 7D 73 34 XXX0421006326)(4
000004B0 3A 7B 31 37 37 3A 39 39 30 31 31 35 21 32 32 38 :(177:9901151228
000004C0 7D 7B 34 35 31 3A 30 3D 7D 2A 49 4E 54 56 2A 54 )<451:0>*INTV#T
000004D0 52 53 4D 2A 4D 52 45 50
RSM#MREP
```

A.2.1.6 CAS2 Message with Text Encoding

PKI signature

If the **Transfer PKI Signatures** option is selected in the message partner profile, then the PKI signature is transferred in a new field **SIGV**. This field contains the complete Signature element (as provided by SWIFTNet Link) that is relevant to the message. The **SIGV** field is created in **MXAMessage.MLPI** and has a maximum of 5000 bytes.

If both a MAC-equivalent signature and a PAC2-equivalent signature are present, then the PAC2-equivalent signature is appended to the MAC-equivalent signature in the **SIGV** field.

Note Back-office applications must be ready to receive and store PKI signatures.

MAC/PAC trailers

If the **Always Transfer MAC/PAC** option is not selected in the message partner profile, then MAC/PAC trailers are not added to the MT message and are not sent to the back-office application.

If the **Always Transfer MAC/PAC** option has been selected for the message partner profile, then dummy MAC/PAC trailers are added to the MT message and sent to the back-office application. The value of these dummy MAC and PAC trailers is 00000000.

Signature result

The MAC-equivalent signature verification result is passed in the existing field **AUTR**.

The PAC-equivalent signature verification result is passed in the existing field **PACR**.

For dual-signed messages of type MT 096, the signature verification result of the PKI signatures will be passed in the existing **PACR** tag.

The verification result has one of the following values:

- `successCurrent`
- `bypassed`
- `failed`

A.2.2 MERVA/2 Format

MAC/PAC values

If a message to be transferred to the back-office application contains a MAC and/or PAC, then the MAC/PAC values are transferred in the MAC/PAC trailers in block 5.

If there are no MAC/PAC values, and if the option **Always Transfer MAC/PAC** has been set for the message partner, then a dummy value ("00000000") is transferred in the MAC/PAC trailers in block 5.

PKI signatures

If the **Transfer PKI Signatures** option is set for the message partner, then the PKI signature is transferred in a new trailer in block S, identified by the `SIG:` identifier. It contains the complete `Signature` element (as provided by SWIFTNet Link) that is relevant to the message, as follows:

```
{S:{SIG:<SwSec:Signature>... </SwSec:Signature >} }
```

The `SIG:` trailer is the last trailer in the block S.

If both the PKI signature that is replacing the MAC, and PAC1 if present, (MAC-equivalent signature) and the PKI signature that is replacing the PAC2 (PAC2-equivalent signature) are present, then the PAC2-equivalent is appended to the MAC-equivalent signature in one SIG trailer.

Note Back-office applications must be ready to receive and store PKI signatures.

Signature result

The verification result is not passed with the message in the block S.

Example

Each message in a file starts with a 4-byte count of the message length in hexadecimal. Here is an example of part of a SWIFT input message file:

MERVA/2 Format

Line Number	Messages in Hexadecimal	Messages in ASCII
OD83:0100	70 00 00 00 7B 31 3A 46-30 31 53 41 45 53 56 41(1:F01SAESVA
OD83:0110	56 41 41 58 58 58 31 32-33 34 31 32 33 34 35 36	VAAAXXX1234123456
OD83:0120	7D 7B 32 3A 49 33 39 38-53 54 45 50 42 45 42 42){2:I398STEPPEBB
OD83:0130	58 58 58 55 33 7D 7B-33 3A 7B 31 30 38 3A 74	XXXXU3}{3:(108:t
OD83:0140	65 73 74 30 30 31 7D 7D-7B 34 3A 0D 0A 3A 32 30	est001)){4:..:20
OD83:0150	3A 6D 76 32 73 65 74 31-30 30 31 0D 0A 3A 31 32	:mv2set1001..:12
OD83:0160	3A 39 39 39 0D 0A 3A 37-37 45 3A 58 0D 0A 2D 7D	:999..:77E:X..-}
OD83:0170	7C 00 00 00 7B 31 3A 46-30 31 53 41 45 53 56 41(1:F01SAESVA
OD83:0180	56 41 41 58 58 58 31 32-33 34 31 32 33 34 35 36	VAAAXXX1234123456
OD83:0190	7D 7B 32 3A 49 37 30 31-53 54 45 50 42 45 42 42){2:I701STEPBEEB
OD83:01A0	58 58 58 55 33 7D 7B-33 3A 7B 31 30 38 3A 74	XXXXU3}{3:(108:t
OD83:01B0	65 73 74 30 30 32 7D 7D-7B 34 3A 0D 0A 3A 32 37	est002)){4:..:27
OD83:01C0	3A 31 2F 31 0D 0A 3A 32-30 3A 6D 76 32 73 65 74	:1/1..:20:mv2set

Note For notification instances, no Unique File Transfer Reference is included.

Examples of Message Formats

You can find examples of the MERVA/2 message format in files with the **.mv2** extension in the following directory:

- Windows: %alliance%\SWIFT\SERVER\MXS\batch_examples
- UNIX or Linux: \$ALLIANCE/MXS/batch_examples

A.2.3 PC Connect (DOS-PCC)

A.2.3.1 Description of PC Connect (DOS-PCC) Format

Overview

Batch message files processed follow a standard format for both input, and output. The DOS message file is in ST200 PC Connect format.

MAC/PAC values

If a message to be transferred to the back-office application contains a MAC and/or PAC, then the MAC/PAC values are transferred in the MAC/PAC trailers in block 5.

If there are no MAC/PAC values and if the option **Always Transfer MAC/PAC** has been set for the message partner, then a dummy value ("00000000") is transferred in the MAC/PAC trailers in block 5.

PKI signatures

If the **Transfer PKI Signatures** flag is set for the message partner, then the PKI signature is transferred in a new trailer in block S, identified by the **SIG:** identifier. It contains the complete Signature element (as provided by SWIFTNet Link) that is relevant to the message, as follows:

```
{S:{SIG:<SwSec:Signature>... </SwSec:Signature >}}
```

The **SIG** trailer is the last trailer in the block S.

If both the PKI signature replacing the MAC, and PAC1 if present, (MAC-equivalent signature) and the PKI signature replacing the PAC2 (PAC2-equivalent signature) are present, then the PAC2-equivalent is appended to the MAC-equivalent signature in one SIG trailer.

Note Back-office applications must be ready to receive and store PKI signatures.

Signature result

If the message to be transferred to the back-office application is MAC-equivalent PKI-signed, then the verification result is passed with the message in block S.

A.2.3.2 Batch Input and Output in DOS-PCC Format

Constraints

The format for input and output files is identical.

The following constraints apply:

- Output messages are preceded by the user ACK (F21).
- The disk that stores the message files must be formatted and write enabled (in the case of Batch Output).
- Each message within a file starts with "01" hex and ends with "03" hex. Space between the end of the message and the end of a sector (512 bytes), are filled with the hex character "20" or null "00".
- Each message starts on a sector boundary and may take up more than one sector.
- All messages must be in 8-bit ASCII.

Examples of Message Formats

You can find examples of the DOS-PCC message format in files with the **.dos** extension in the following directory:

- Windows: %alliance%\SWIFT\SERVER\MXS\batch_examples
- UNIX or Linux: \$ALLIANCE/MXS/batch_examples

Example

The following example is provided in both hexadecimal and ASCII so that the details are clear.

DOS-PCC Input Message Format

```

0001-0016      01 7B 31 3A 46 30 31 42 42 4E 4B 42 45 42 42 41 .(1:F01BBNKBEBA
0017-0032      58 58 58 31 32 33 34 31 32 33 34 35 36 7D 7B 32 XXX1234123456}{2
0033-0048      3A 49 31 30 30 41 4E 59 42 42 45 42 42 58 58 58 :I1000ANYBEBBXX
0049-0064      58 55 33 30 30 33 7D 7B 33 3A 7B 31 30 38 3A 53 XU3003}{3:(108:S
0065-0096      3A 0D 0A 3A 32 30 3A 52 45 46 46 49 4C 2D 30 30 :.:20:REFFIL-00
0097-0112      31 2D 4C 30 31 30 30 0D 0A 3A 33 32 41 3A 39 31 1-L0100.:32A:91
0113-0128      30 37 30 31 55 53 44 31 30 2C 30 30 0D 0A 3A 35 0701USD10,00.:5
0129-0144      30 3A 4F 52 44 45 52 49 4E 47 20 43 55 53 54 4F 0:0RDERING CUSTO
etc. until
..... .....
0417-0432      57 20 54 48 45 20 47 4F 4F 44 53 0D 0A 3A 37 31 W THE GOODS..:71
0433-0448      41 3A 42 45 4E 0D 0A 3A 37 32 3A 2F 52 43 42 2F A:BEN..:72:/RCB/
0449-0464      0D 0A 2F 42 45 4E 4F 4E 4C 59 2F 0D 0A 2D 7D 03 ..:/BENONLY/...}.
0481-0496      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0497-0512      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

```

DOS-PCC Output Message Format

```

00000000      01 7B 31 3A 46 32 31 53 57 41 4C 55 53 33 30 41 .(1:F21SWALUS30A
00000010      58 58 58 30 30 35 38 30 30 31 38 39 39 7D 7B 34 XXX0058001899}{4
00000020      3A 7B 31 37 37 3A 39 39 30 31 31 35 31 31 33 31 :(177:9901151131
00000030      7D 7B 34 35 31 3A 30 7D 7D 7B 31 3A 46 30 31 53 }{451:0}}(1:F01S
00000040      57 41 4C 55 53 33 30 41 58 58 58 30 30 35 38 30 WALUS30AXXX00580
00000050      30 31 38 39 39 7D 7B 32 3A 4F 31 30 30 31 32 32 01899){2:0100122
00000060      38 39 39 30 31 31 35 53 57 41 4C 42 45 42 30 41 8990115SWALEB0A
00000070      58 58 58 30 34 32 31 30 30 36 33 32 36 39 39 30 XXX0421006326990
00000080      31 31 35 30 36 32 39 4E 7D 7B 34 3A 0D 0A 3A 32 1150629N}{4:..:2
00000090      30 3A 41 42 43 44 45 46 47 48 0D 0A 3A 33 32 41 0:ABCDEFGH..:32A
000000A0      3A 39 39 30 31 31 33 42 45 46 31 30 30 30 2C 0D :990113BEF1000,.
000000B0      0A 3A 35 30 3A 41 42 43 44 45 46 47 48 0D 0A 3A .:50:ABCDEFGH..:
000000C0      35 39 3A 41 42 43 44 45 46 47 48 0D 0A 2D 7D 7B 59:ABCDEFGH..-}{5
000000D0      35 3A 7B 4D 41 43 3A 30 44 38 33 42 33 36 30 7D 5:(MAC:0D83B360)
000000E0      7B 43 48 4B 3A 39 41 31 30 42 41 43 35 42 42 31 {CHK:9A10BAC5BB1
000000F0      30 7D 7B 54 4E 47 3A 7D 7D 7B 53 3A 7B 53 50 44 0}{TNG:}}{S:(SPD
00000100      3A 7D 7B 53 41 43 3A 7D 7B 43 4F 50 3A 50 7D 7D :}{SAC:}{COP:P}}
00000110      03 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
00000120      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000130      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000140      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000150      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000160      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000170      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000180      20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

```

A.2.4 RJE

A.2.4.1 Description of RJE Format

Overview

Message files processed through the RJE connection method follow a standard format for both input, and output. The RJE message file is in ST200 RJE format.

Output messages are preceded by the user ACK (F21).

Alliance Access accepts "real" ST200 RJE format messages without any modification required to the existing format. Alliance Access handles the following:

- Stripping ST200 non-essential header and trailer information
 - Ignoring empty messages (messages beginning and ending with \$\$)
 - Synonym notations for CRLF (such as EM ITB, EM ETB, \n, nl, Cr, Lf)

- Stripping or translating non-'x' character sets

If after stripping or translating the character, the message is still valid, the message will not be moved to _MP_mod_text. Validation of the message is performed after the action.

MAC/PAC values

If a message to be transferred to the back-office application contains a MAC and/or PAC, then the MAC/PAC values are transferred in the MAC/PAC trailers in block 5.

If there are no MAC/PAC values, and if the field **Always Transfer MAC/PAC** has been set for the message partner, then a dummy value ("00000000") is transferred in the MAC/PAC trailers in block 5.

PKI signatures

If the **Transfer PKI Signatures** flag is set for the message partner, then the PKI signature is transferred in a new trailer in block S, identified by the **SIG:** identifier. It contains the complete Signature element (as provided by SWIFTNet Link) that is relevant to the message, as follows:

```
{S:{SIG:<SwSec:Signature>... </SwSec:Signature >}}
```

The **SIG:** trailer is the last trailer in block S.

If both the PKI signature replacing the MAC [+PAC1 if present] (MAC-equivalent signature) and the PKI signature replacing the PAC2 (PAC2-equivalent signature) are present, then the PAC2-equivalent is appended to the MAC-equivalent signature in one **SIG** trailer.

Note Back-office applications must be ready to receive and store PKI signatures.

Signature result

If the message to be transferred to the back-office application is MAC-equivalent PKI-signed, then the verification result is passed with the message in block S.

A.2.4.2 Batch Input and Output

Examples of Message Formats

You can find examples of the RJE message format in files with the **.rje** extension in the following directory:

- Windows: %alliance%\SWIFT\SERVER\MXS\batch_examples
- UNIX or Linux: \$ALLIANCE/MXS/batch_examples

Overview

Each message within an RJE message file is delimited using the "\$" character.

The format for input and output files is identical, although input messages do not generally contain the MAC trailer. The following example shows a batch output file containing two messages.

Output messages are preceded by the user ACK (F21).

All messages must be in 8-bit ASCII. The following example is printed in both hexadecimal and ASCII so that the details are clear.

RJE Message Format: Input Format

```
00000000h: 7B 31 3A 46 30 31 53 4D 4C 54 42 45 42 42 41 58 ; {1:F01SMLTBEBBAX
00000010h: 58 58 31 32 33 34 31 32 33 34 35 36 7D 7B 32 3A ; XX1234123456}{2:
00000020h: 49 39 39 39 43 48 41 53 55 53 33 33 58 58 58 58 ; I999CHASUS33XXXX
00000030h: 4E 32 7D 7B 33 3A 7B 31 30 38 3A 53 54 53 2F 54 ; N2}{3:{108:STS/T
00000040h: 20 39 35 30 38 32 31 31 32 33 32 7D 7D 7B 34 3A ; 9508211232}}{4:
00000050h: 0D 0A 3A 32 30 3A 4E 4F 54 31 2E 30 30 31 2E 30 ; ..:20:NOT1.001.0
00000060h: 30 31 0D 0A 3A 37 39 3A 54 45 58 54 31 0D 0A 4C ; 01..:79:TEXT1..L
00000070h: 49 4E 45 32 0D 0A 4C 49 4E 45 33 0D 0A 2D 7D 24 ; INE2..LINE3..-}$
00000080h: 7B 31 3A 46 30 31 53 4D 4C 54 42 45 42 42 41 58 ; {1:F01SMLTBEBBAX
00000090h: 58 58 31 32 33 34 31 32 33 34 35 36 7D 7B 32 3A ; XX1234123456}{2:
000000a0h: 49 39 39 39 43 48 41 53 55 53 33 33 58 58 58 58 ; I999CHASUS33XXXX
000000b0h: 4E 32 7D 7B 33 3A 7B 31 30 38 3A 53 54 53 2F 54 ; N2}{3:{108:STS/T
000000c0h: 20 39 35 30 38 32 31 31 32 33 32 7D 7D 7B 34 3A ; 9508211232}}{4:
000000d0h: 0D 0A 3A 32 30 3A 4E 4F 54 32 2E 30 30 31 2E 30 ; ..:20:NOT2.001.0
000000e0h: 30 32 0D 0A 3A 37 39 3A 54 45 58 54 32 0D 0A 4C ; 02..:79:TEXT2..L
000000f0h: 49 4E 45 32 0D 0A 4C 49 4E 45 33 0D 0A 2D 7D ; INE2..LINE3..-}
```

Note The input sequence number of the RJE message in block 1 is overwritten by Alliance when the message is passed on to the SWIFT network.

RJE Message Format: Output Format

```
00000000h: 7B 31 3A 46 32 31 53 41 41 46 42 45 42 42 41 58 ; {1:F21SAAFBEBBAX
00000010h: 58 58 30 30 30 31 30 30 30 30 32 7D 7B 34 3A ; XX0001000002}{4:
00000020h: 7B 31 37 37 3A 31 34 30 35 32 38 31 33 35 32 7D ; {177:1405281352}
00000030h: 7B 34 35 31 3A 30 7D 7D 7B 31 3A 46 30 31 53 41 ; {451:0}}{1:F01SA
00000040h: 41 46 42 45 42 42 41 58 58 58 30 30 30 31 30 30 ; AFBEBBAXX000100
00000050h: 30 30 30 32 7D 7B 32 3A 4F 31 30 31 31 33 35 32 ; 0002}{2:01011352
00000060h: 31 34 30 35 32 38 53 41 41 46 42 45 42 42 41 58 ; 140528SAAFBEBBAX
00000070h: 58 58 30 30 30 31 30 30 30 30 30 35 31 34 30 35 ; XX00010000051405
00000080h: 32 38 31 33 35 32 4E 7D 7B 34 3A 0D 0A 3A 32 30 ; 281352N}{4...:20
00000090h: 3A 41 42 43 44 45 46 47 48 0D 0A 3A 32 38 44 3A ; :ABCDEFGH..:28D:
000000a0h: 30 30 30 30 31 2F 30 30 30 30 31 0D 0A 3A 33 30 ; 00001/00001..:30
000000b0h: 3A 31 34 30 35 32 38 0D 0A 3A 32 31 3A 41 42 43 ; :140528..:21:ABC
000000c0h: 44 45 46 47 48 0D 0A 3A 33 32 42 3A 45 55 52 31 ; DEFGH..:32B:EUR1
000000d0h: 30 30 30 2C 0D 0A 3A 35 39 3A 41 42 43 44 45 46 ; 000...:59:ABCDEF
000000e0h: 47 48 0D 0A 3A 37 31 41 3A 53 48 41 0D 0A 2D 7D ; GH..:71A:SHA..-}
000000f0h: 7B 35 3A 7B 43 48 4B 3A 43 41 32 37 34 30 39 46 ; {5:{CHK:CA27409F
00000100h: 38 33 38 42 7D 7D 7B 53 3A 7B 53 41 43 3A 7D 7B ; 838B}}{S:{SAC:}{COP:P}}
```

A.2.5 MQ-MT Format

Introduction

The following sections describe the structure of message in MQ-MT format.

A.2.5.1 Structure of a Message in MQ-MT Format

Description of elements

In the following table, the columns **From**, **To**, and **To (Resp)** indicate whether Alliance Access requires an element to process a message successfully.

The columns represent the following:

- **From** - a message request that Alliance Access receives from a message partner
- **To** - a notification, a system message, or a message request that Alliance Access sends to a message partner.
- **To (Resp)** - a response message that Alliance Access sends to a message partner.

When an WebSphere MQ message is sent in MQ-MT format, it has the following elements in the Message Data part. The elements that Alliance Access requires are marked as Mandatory

(M). If an element is marked Optional (O) and has a non-null value, then Alliance Access processes it:

Elements in MQ-MT message

Element	Description	Type	From	To	To (Resp)
UUMID	The UUMID of the message. Present if the option Transfer UUMID is selected in the message partner profile.	String (45 bytes) padded with spaces	O	O	O
Message	The business data that is being exchanged between applications. This can contain the one of the types of information, as outlined in "MQMTMessage" on page 637.	MQMTMessage	M	M	O
OriginalMessage	A FIN message, with an optional block 4. ⁽¹⁾ Block 4 is included if Send original message has one of the following values in the message partner profile: <ul style="list-style-type: none">• When created by another Message Partner• When message modified• Always	FIN message	--	O	--
ValidationErrorCode	The error code that applies if the requested level of message validation has failed. Present if: <ul style="list-style-type: none">• an error is reported during message processing (Feedback element in the MQ Message Descriptor does not contain <code>MQFB_PAN</code>), and• Transfer Validation Code is selected in the message partner profile.	The field contains the offset in block 4 that caused the error, as follows: <code>{REP:{ERR:(<error_information>)} }</code> <code><error information></code> is a string, such that: <code><error_code> - <error explanation> at offset <offset></code>	--	--	O

Element	Description	Type	From	To	To (Resp)
S-Block	<p>Present if:</p> <ul style="list-style-type: none"> • Transfer SAA Information is selected and Use MQ Descriptor is not selected • Add Routing Code is selected. 	<p>S-Block</p> <p>See "Codes in the Trailer (Block S)" on page 750 and "Routing Code Trailer" on page 756.</p>	O	O	--

(1) The blocks 1, 2, 3, and 5 are always present.

A.2.5.2 MQMTMessage

Overview

The MQMTMessage part of the Message Data in a WebSphere MQ message carries the business data that is being exchanged between Alliance Access and an application. The MQMTMessage part can carry the information of the following type:

- SWIFT Output Message
- Transmission Notification
- Delivery Notification
- Information Notification
- History Notification
- System Delivery Notification

Message Request

A message request is carried in the FIN Output message.

Transmission Notification

Alliance Access uses the Message Data part of WebSphere MQ to store information related to the transmission notification and optionally, on the original message. (an option in the message partner profile).

The Feedback element only has meaning for a report message (MQ Report/Reply). To check the status of a message, you must check the content of the ACK.

Delivery Notification

When you create a message, you can request that the progress of your message is monitored. This results in Alliance Access receiving a message about the message delivery, which can be reconciled with the original message. In such cases, creates a Delivery Notification.

The Delivery Notification contains a reference to the original message through the CorrelId field of WebSphere MQ Descriptor. The text of the original message can be appended to the Delivery Notification.

Information Notification

Alliance Access uses the Message Data part of WebSphere MQ to store data that is related to the Information notification and optionally on the original message.

The Information notification has a structure which resembles a SWIFT ACK message, and it can contain a block S.

Block 1 contains `INF` instead of the `F21` to indicate this is an Information Notification, the sender logical terminal code, followed by `"0000"` for the SWIFT session number, and `"000000"` for the SWIFT sequence number.

There is no block 2.

Block 4 does not contain a `Crlf` at the beginning. The following tags have been defined inside block 4:

TAG	Description	
DAT	The date and time of the information notification in the format <code>YYYYMMDDHHMMSS</code> . The date is the Co-ordinated Universal Time (UTC), which is the time standard the operating system uses.	
CAT	The information notification category. The following are defined:	
	00–None	illegal value of the intervention
	01–Routing	generated by the creation or routing of a message
	02–Security	security related. For example, bypass of authentication
	03–NetworkReport	generated when transmitting to a network
	04–DeliveryReport	generated by traffic reconciliation
	05–NetworkFormattedTransmitted	a network-formatted transmitted intervention
	06–NetworkFormattedReceived	a network-formatted received intervention
	07–MessageModified	intervention contains safe store of a message text which has been modified
	08–MessageScissored	scissors and broadcast related
	09–Other	all other types of intervention
	n–Unknown	(n > 9) unknown intervention category
NAM	The information notification name. Alliance Access does not offer a fixed list of these. However, some examples are <code>"Instance routed"</code> , <code>"Message Processed"</code> , <code>"Report text"</code> , and <code>"User delivery report"</code> .	
TXT	The information notification text.	
OPR	The name of the operator.	

History Notification

Alliance Access uses the Message Data part of WebSphere MQ to store data that is related to the History notification and optionally on the original message.

The History notification contains the last 10 interventions of a message.

The History notification has a structure which resembles a SWIFT ACK message, and it can contain a block S.

Block 1 contains `HIS` instead of the `F21` to indicate this is a History Notification, the sender logical terminal code, followed by "0000" for the SWIFT session number, and "000000" for the SWIFT sequence number.

There is no block 2.

Block 4 does not contain a `Crlf` at the beginning. The tags have been defined inside block 4 for a History notification as for an Information Notification.

System Message

A Delivery Notification System Message is of the following messages MT 010, MT 011, MT 012, MT 015, or MT 019. Alliance Access sends it to an application in a FIN Output message.

A system message contains a SWIFT block 1, 2, and 5.

The block S of the system message offers the same trailers as a SWIFT output message. The block S can include a `SYS` tag. The `CON` and `TRN` tags are optional in a System Message.

System messages have a WebSphere MQ priority 7.

Important If System Messages are sent to WebSphere MQ, then it is possible that the System Messages are delivered before the Transmission Notification for the corresponding message. This happens when the system messages have a higher priority within Alliance Access than the transmission notifications. SWIFT recommends that applications which use the Traffic Reconciliation within Alliance Access ensure that Delivery Notifications are delivered before the Transmission Notifications.

A.2.6 XML Format 1

Introduction

The following sections describe the format of the Protocol Data Units (PDUs) exchanged between Alliance Access and the application.

Examples of Message Formats

You can find examples of the XML version 1 message format in files on Windows **Samples_v1.zip**, on UNIX or Linux **Samples_v1.tar.Z** in the following directory:

- Windows: `%alliance%\SWIFT\SERVER\MXS\batch_examples`
- UNIX or Linux: `$ALLIANCE/MXS/batch_examples`

A.2.6.1 XML Data Format Description

A.2.6.1.1 Protocol Data Units

Description

The application and Alliance Access exchange PDUs that are sequences of bytes with the following structure:

Prefix	Length	Signature	DataPDU
--------	--------	-----------	---------

- **Prefix** (1 byte): the character `0x1e`

- **Length** (6 bytes): length (in bytes) of the Signature and DataPDU fields. This length is base-10 encoded as six ASCII characters, and is left-padded with zeros, if needed.
- **Signature** (24 bytes) : signature computed on the DataPDU using the HMAC-SHA256 algorithm: the first 128 bits are base64-encoded.

This signature authenticates the originator of the DataPDU (the application or Alliance Access) and guarantees the integrity of the DataPDU. This action is referred to as local authentication (LAU). If Alliance Access is configured to not require LAU, then the field must contain NULL characters.

- **DataPDU**: XML structure containing the information relevant to be processed (message or report) encoded in UTF-8. The first byte of this field must be the character < -(0x3C). A byte-order marker is not supported.

The structure of the DataPDU is described in the rest of this section.

Each document has a structure defined as:

```
<?xml version="1.0" encoding="utf-8"?><Saa:DataPDU
xmlns:Saa="urn:swift:xsd:saa.mxs.01">
...
</Saa:DataPDU>
```

A DataPDU field that Alliance Access sends to the application may contain structured data that is received from SWIFTNet. Therefore, the field may contain the following additional namespace declarations:

```
xmlns:Sw="urn:swift:snl:ns.Sw"
xmlns:SwInt="urn:swift:snl:ns.SwInt".
xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
xmlns:SwSec="urn:swift:snl:ns.SwSec"
<?xml version="1.0" encoding="utf-8"?>
```

The signature is computed on the complete DataPDU field, that includes the string <?xml version="1.0" encoding="utf-8"?>. The XML representation must not be altered between the signature computation and the verification.

A batch file that is exchanged using File Transfer can contain one or more consecutive PDUs.

A.2.6.1.2 Alliance Access WebSphere MQ Interface

XML format supported

The Alliance Access WebSphere MQ Interface (MQSA) also supports the XML format. However, it only uses the DataPDU structure. The Prefix, Length, and Signature are not supported by MQSA 7.0.

When instructed by the application that sends the message, MQSA has to send back a reply to that application, indicating whether the message was accepted or rejected by Alliance Access. MQSA uses the LogicalReply element for this.

A.2.6.1.3 Structure of the DataPDU

Conventions used

This section describes the various XML elements that can be present in the DataPDU field. The description uses a table format, and the elements are ordered top-down.

The corresponding schema is located in the following directory in the Alliance Access release tree:

On Windows: **MXS\xsd\SAA_XML_v1_0.xsd**

On UNIX or Linux: **/MXS/xsd/SAA_XML_v1_0.xsd**

In the following tables, the columns **From** and **To** indicate whether the element is mandatory (M), optional (O) or not applicable (--) for the corresponding direction of a message or report exchange. The directions are defined as follows:

- **From:** from the application to Alliance Access
- **To:** from Alliance Access to the application

DataPDU

Element	Description	Type	From	To
SenderReference	Contains the UUMID of the message. Not present if LogicalReply is present.	String(1..50)	--	O
(Message 	The Message.	Message	M	M
Report 	The Report.	Report	--	M
LogicalReply)	LogicalReply sent to MQSA.	LogicalReply	--	M

Message

Element	Description	Type	From	To
MessageFormat	The message format. Possible values are: <ul style="list-style-type: none"> • MX 	String	M	M
MessageSubFormat	The message sub-format. Possible values are: <ul style="list-style-type: none"> • Input • Output From: only Input is allowed.	String	M	M
Sender	The address of the message sender message sender (see "AddressFullName"). The first 8 characters of the X1 member must match the institution of the RequestorDN (case insensitive, see "SWIFTNetRequestAttribute").	AddressFullName	M	M
Receiver	The address of the message receiver (see Address).	Address	M	M
LiveMessage	Is it a live message or is it a test message?: <ul style="list-style-type: none"> • true: message is Live • false: test message (pilot) 	Boolean	--	M

Element	Description	Type	From	To
MessageNature	<p>The message nature.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • FinancialNature • TextNature • NetworkNature • SecurityNature • ServiceNature <p>For MX messages, the value FinancialNature must be used.</p>	String	M	M
MessageLPI	The Local Processing information.	MessageLPI	M	M
MessageTPI	The Transmission information.	MessageTPI	M	M
MessageSRI	The Sender-to-Receiver information.	MessageSRI	M	M
MessageText	Contains the message text, that is, the Application Header ⁽¹⁾ (if required) and the Business Document. Both are described in the documentation of the Solutions.	Any	M	M

(1) If an Application Header is required, then the schema of the Application Header for each message that is part of a Solution is listed in the Implementor section of the Standards Handbook for that specific Solution.

MessageLPI

Element	Description	Type	From	To
OriginalMessage	<p>The Alliance Access instance type:</p> <ul style="list-style-type: none"> • true: Original instance • false: Copy instance 	Boolean	--	O
ModifyAllowed	<p>If set to true, then the message can be modified using Message Management (available on Alliance Web Platform).</p> <p>If set to false, then the message cannot be changed.</p> <p>Default value:</p> <ul style="list-style-type: none"> • as defined in the Message Partner configuration • true for MQSA 	Boolean	O	--
DeleteInhibited	<p>If set to true, then only its creator can delete the message, if it is still in the creation queue.</p> <p>Default value: false</p>	Boolean	O	--
MinValidation	<p>Requested message validation level.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • None 	String	O	--

Element	Description	Type	From	To
	<ul style="list-style-type: none"> • Minimum Extract routing keywords from message text • Intermediate (same as minimum) • Maximum (same as minimum) <p>If specified, has precedence over the Alliance Access configuration.</p>			
CBTPriority	The Alliance Access message priority. If not present, then it is determined by the field NetworkPriority (see "MessageTPI").	Integer(0..9)	O	--
DispositionState	<p>The requested message disposition state. The corresponding routing point name is listed between parentheses.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Verify (_MP_verification) • (_Authorise_MP_authorisation) • Modify (_MP_mod_text) • Ready based on the preferred network settings of the Receiver in the Alliance Access Correspondent Information File <p>Taken into account if TargetApplicationRule (see "TargetApplication") is "CBTApplication".</p> <p>Not applicable to MQSA.</p>	String	O	--
NetworkAttribute	Set of network-related attributes.	NetworkAttribute	M	M
SecurityAttribute	Set of security-related attributes.	SecurityAttribute	O	O
FormatAttribute	Set of format-related attributes. Not currently used.	FormatAttribute	O	O
TargetApplication	<p>Specifies where the message has to be created in Alliance Access.</p> <p>If specified, has precedence over the Alliance Access Message Partner configuration.</p> <p>Not applicable to MQSA.</p>	TargetApplication	O	--
MessageOrigin	The Alliance Access component that created the message. See "MessageOrigin".	MessageOrigin	--	O

Element	Description	Type	From	To
CBTRoutingInfo	The routing point the message instance was located on before emission to the application.	String(1..20)	--	O
MANRoutingCode	Information to influence the routing in Alliance Access. The code entered here is visible through the routing keyword "Routing_code".	String(1..6)	O	O
DuplEmission	Indicates whether Alliance Access already attempted to send this message instance to the application.	Boolean	--	O

NetworkAttribute

Element	Description	Type	From	To
SWIFTNetRequestAttribute	SWIFTNet request attributes.	SWIFTNetRequest Attribute	M	M
SWIFTNetResponseAttribute	SWIFTNet response network attributes.	SWIFTNetResponse Attribute	--	O

SWIFTNetRequestAttribute

For Standards MX messages, the PKI signature, if present, is transferred using the SWIFTNetRequestAttribute:AuthValue elements. The PKI signature verification result is passed in the SWIFTNetRequestAttribute:AuthResult elements.

Element	Description	Type	From	To
RequestorDN	The requestor DN.	String(1..100)	M	M
ResponderDN	The responder DN.	String(1..100)	M	M
Service	The SWIFTNet service name.	String(1..30)	M	M
RequestType	<p>The identification of the message (that is, the Message Identifier)</p> <p>For an MX message, the format is:</p> <pre><bus. area>.<msg type>.<variant>.<version></pre> <p>For example, ifds.001.001.01</p> <p>It corresponds to the namespace of the URI of the XML Document in the MessageText which has following structure:</p> <pre>urn-prefix: [[service name]\$]Message Identifier</pre>	String(1..30)	M	O
NRIndicator	<p>Indicates whether non-repudiation requested.</p> <p>Default value: as defined in the Alliance Access emission profile configuration</p>	Boolean	O	--
NonRepType	Non-repudiation processing information (Type).	String	--	O

Element	Description	Type	From	To
	<p>Possible Values are:</p> <ul style="list-style-type: none"> • SvcOpt • SvcMand 			
NonRepWarning	Non-repudiation processing information (Warning)	String	--	O
SwiftRef	<p>The reference generated by the central SWIFT infrastructure.</p> <p>Always present for output messages, Transmission Reports with NetworkDeliveryStatus NetworkAcked and Delivery Reports.</p> <p>Format:</p> <p>SWITCHid-YYYY-MM- DDTHH:MM:SS.procId.digitsZ</p> <p>Where:</p> <ul style="list-style-type: none"> • SWITCHid is the ID of the switch that generated the reference • procid is the process ID of the process that created the reference • digits makes the reference unique within a given second. <p>The timestamp is the time of generation of the reference in UTC.</p>	String	--	O
SwiftRequestRef	<p>The reference generated by the emitting SWIFTNet Link.</p> <p>Always present for output messages, Transmission Reports with NetworkDeliveryStatus NetworkAcked and Delivery Reports.</p> <p>SNLid-YYYY-MM- DDTHH:MM:SS.procId.digitsZ</p> <p>Where SNLid is the ID of the SWIFTNet Link that generated the reference.</p> <p>The other parts are identical to the format of SwiftRef.</p>	String	--	O
CBTReference	The reference generated by the Alliance Access (for messages sent) or by the correspondent application (for messages received).	String	--	O
SNLEndPoint	The SWIFTNet Link endpoint. Real-time messages only.	String	--	O
SnFQueueName	The store-and-forward queue name.	String	--	O
SnFIInputTime	SWIFTNet storage location and time of a store-and-forward request (UTC).	String	--	O
	<p>Format:</p> <p>nnnn : YYYY-MM-DDTHH:MM:SS</p>			

Element	Description	Type	From	To
	Where nnnn is the SWIFT internal storage identifier.			
SnFPDMHistory	Duplication history details. Output messages only.	Any ⁽¹⁾	--	O
ValidationDescriptor	MVal processing result.	Any ⁽²⁾	--	O
AuthResult	The authentication result. Possible values are: <ul style="list-style-type: none">• Success• Bypassed• Failed	String	--	O
AuthValue	The authentication value.	Any ⁽²⁾	--	O

(1) For previous delivery attempts, this SWIFTNet specific data element provides the delivery attempt history. See "Additional Information" for a description of this structure.

(2) These fields contain SWIFTNet data elements that are provided for purposes of completeness. Further processing of these elements is not required.

SWIFTNetResponseAttribute

Element	Description	Type	From	To
ResponderDN	The responder DN.	String	--	O
NonRepType	Non-repudiation processing information (Type). Possible Values are: <ul style="list-style-type: none">• SvcOpt• SvcMand Real-time messages only.	String	--	O
NonRepWarning	Non-repudiation processing information (Warning) Real-time messages only.	String	--	O
ResponseRef	The reference generated by the central SWIFT infrastructure. For format information, see <code>SwiftRef</code> in "SWIFTNetRequestAttribute". Real-time messages only.	String	--	O
SwiftResponseRef	The reference generated by the emitting SWIFTNet Link. For format information, see <code>SwiftRequestRef</code> in "SWIFTNetRequestAttribute".	String	--	O
CBTReference	The reference generated by the responding application. Real-time messages only.	String	--	O

Element	Description	Type	From	To
DuplCreation	<p>Indicates whether the response is a possible duplicate.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • None • PDE <p>Real-time messages only.</p>	String	--	O
ValidationDescriptor	<p>MVal processing result of the response.</p> <p>Real-time messages only.</p>	Any ⁽¹⁾	--	O
AuthResult	<p>The authentication result of the response.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Success • Bypassed • Failed <p>Real-time messages only.</p>	String	--	O
AuthValue	<p>The response authentication value.</p> <p>Real-time messages only.</p>	Any ⁽¹⁾	--	O

(1) These fields contain SWIFTNet data elements that are provided for purposes of completeness. Further processing of these elements is not required.

SecurityAttribute

Element	Description	Type	From	To
SWIFTNetSecurityAttribute	SWIFTNet security attributes.	SWIFTNetSecurity Attribute	M	M

SWIFTNetSecurityAttribute

Element	Description	Type	From	To
SigningRequired	<p>Indicates whether signing of the message is required upon emission.</p> <p>If specified, it overrides the Alliance Access emission profile configuration.</p>	Boolean	O	--
SignerDN	The Signer DN	String	--	O

MessageTPI

Element	Description	Type	From	To
NetworkDelivNotify	<p>Indicates whether a positive delivery notification is requested.</p> <p>Default value: false</p>	Boolean	O	--
Network	The network over which the message was transmitted.	String	--	M

Element	Description	Type	From	To
	<p>Possible values are:</p> <ul style="list-style-type: none"> • ApplicationNetwork • SwiftNetNetwork • OtherNetwork 			
NetworkPriority	<p>The Network priority.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Normal • Urgent <p>If the field CBTPriority is not present (see "MessageLPI"), then its value is derived as follows:</p> <ul style="list-style-type: none"> • Normal maps to 7 • Urgent maps to 5 <p>Default value: Normal</p>	String	O	O
NetworkSessionNr	The Network Session number.	Integer	--	M
NetworkSeqNr	The Network Sequence number.	Integer	--	M
DuplCreation	<p>Indicates whether the message was marked as duplicate by the sender (PDE), or if the store-and-forward central system attempted to deliver the message multiple times (PDM).</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • None • PDM • PDE • PDE_PDM 	String	--	O

MessageSRI

Element	Description	Type	From	To
UserReference	The Message User Reference. This corresponds to the SWIFTNet RequestRef (part of the InterAct RequestHeader)	String(1..30)	O	O
UserPDE	The application indicates whether the message is a possible duplicate.	Boolean	O	--

Report

Element	Description	Type	From	To
Addressee	The address of the receiver of the original instance (see "AddressFullName").	AddressFullName	--	M

Element	Description	Type	From	To
OrigMessageFields	<p>The level of detail that Alliance Access provides about the original message, as defined in the Alliance Access configuration.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • NoOriginal <p>The next element ("OrigMessage") is not present. Used when the Message Partner is configured to never send the original messages for notifications.</p> <p>When the message partner is configured to include the original message in the report, the following values define the elements of the original message that are present in "OrigMessage":</p> <ul style="list-style-type: none"> • Minimum • Condensed • Full • Expanded <p>In this release, there is no distinction between the last 4 possibilities. OrigMessage always contains the full message details, including the MessageText.</p>	String	--	M
OrigMessage	<p>The original message.</p> <p>Not present if OrigMessageFields contains NoOriginal.</p>	Message	--	O
ReportLPI	The report Local Processing Information.	ReportLPI	--	M
(TransmissionReport 	Transmission report.	TransmissionReport	--	M
DeliveryReport)	<p>Delivery report.</p> <p>Indicates whether the message has been received by the correspondent or not.</p>	DeliveryReport	--	M

ReportLPI

Element	Description	Type	From	To
OrigSenderReference	The Original Sender reference.	String(1..40)	--	O
MessageOrigin	The Alliance Access component that created the message. See "MessageOrigin"	MessageOrigin	--	M
Modified	Indicates whether the message has been modified within Alliance Access.	Boolean	--	O
OriginalRelatedMessage	Indicates whether this report is about an Original (true) or a Copy instance (false) of the message.	Boolean	--	O

Element	Description	Type	From	To
	Not applicable to MQSA.			
ReportingApplication	The Alliance Access application that generated the report.	String	--	M
BackToNonOriginator	Indicates whether the report is sent back to the entity that created the message in Alliance Access. Not applicable to MQSA.	Boolean	--	O
DuplEmission	Indicates whether Alliance Access already attempted to send this message instance to the application.	Boolean	--	O

TransmissionReport

Element	Description	Type	From	To
Network	The network over which the message was transmitted. Possible values are: <ul style="list-style-type: none">ApplicationNetworkSwiftNetNetworkOtherNetwork	String	--	M
NetworkAttribute	The network attributes.	NetworkAttribute	--	M
NetworkSessionNr	The Network Session number.	Integer	--	M
NetworkSeqNr	The Network Sequence number.	Integer	--	M
NetworkDeliveryStatus	The network delivery status. Possible values are: <ul style="list-style-type: none">NetworkAckedNetworkNackedNetwork_N_A No network transmission status is available, that is, Alliance Access did not yet attempt to send the message. <ul style="list-style-type: none">NetworkRejectedLocally The message was rejected by Alliance Access before emission. <ul style="list-style-type: none">NetworkAborted The message emission was aborted due to a communication error before the acknowledgement was received. <ul style="list-style-type: none">NetworkTimedOut	String	--	M

Element	Description	Type	From	To
	<p>The acknowledgement for the message was not received within the allowed time.</p> <ul style="list-style-type: none"> • NetworkWaitingAck <p>Transient state.</p> <p>Unless the Alliance Access routing is configured to do so, the last 3 values are not reported to the application.</p>			
Interventions	The list of interventions.	Intervention [1..N]	--	M

DeliveryReport

Element	Description	Type	From	To
Network	<p>The network over which the message was transmitted.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • ApplicationNetwork • SwiftNetNetwork 	String	--	M
NetworkAttribute	The network attributes.	NetworkAttribute	--	M
NetworkSessionNr	The Network Session number.	Integer	--	M
NetworkSeqNr	The Network Sequence number.	Integer	--	M
ReceiverDeliveryStatus	<p>The delivery notification status.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • RcvUnknown • RcvOverdue • RcvDelivered • RcvAborted • RcvDelayedNak • RcvAcked • RcvNacked • RcvTruncated 	String	--	M
Interventions	The list of interventions	Intervention [1..N]	--	M

Intervention

Element	Description	Type	From	To
IntvCategory	Intervention category.	String	--	M

Element	Description	Type	From	To
	<p>Possible values are:</p> <ul style="list-style-type: none"> • TransmissionReport • DeliveryReport • TransmissionResponse: can be present in TransmissionReport 			
CreationTime	<p>The intervention creation time.</p> <p>Format:</p> <p>YYMMDDHHMMSS</p>	String	--	M
ApplicationOrigin	The application that created the intervention.	String	--	M
OperatorOrigin	The name of operator that triggered the intervention creation.	String	--	M
Text	The intervention text.	Any ⁽¹⁾	--	M

(1) This field contains SWIFTNet data elements for Alliance intervention categories DeliveryReport and TransmissionResponse. For more information, see "Additional Information", "Creation of an Emission Appendix", "User Delivery Notifications from SWIFTNet Store-and-forward", and "Business Response for SWIFTNet Real-Time".

LogicalReply

This element is used exclusively by MQSA.

Element	Description	Type	From	To
SenderReference	Contains the UUMID of the message if it has been added to the Alliance Access database. Not present if the message has not been added.	String(1..50)	--	O
SuccessIndication	<p>Indicates the result of the processing of the original message by MQSA:</p> <ul style="list-style-type: none"> • true: if the message was added successfully by MQSA • false: if an error occurred during the processing of the message by MQSA 	Boolean	--	M
ErrorText	<p>Text associated with the error.</p> <p>Only present if SuccessIndication is false.</p>	String	--	O

Address

Element	Description	Type	From	To
(Nickname 	<p>The correspondent nickname.</p> <p>Currently not applicable to MQSA.</p>	String(1..32)	M	--
Fullname)	The correspondent full name.	AddressFullName	M	M

AddressFullName

Element	Description	Type	From	To
X1	The correspondent X1 part. The institution BIC11.	String(11..11)	M	M
X2	The correspondent X2 part. Present if correspondent type is: <ul style="list-style-type: none">• Department• Application• Individual	String(1..20)	O	O
X3	The correspondent X3 part. Present if correspondent type is: <ul style="list-style-type: none">• Application<ul style="list-style-type: none">contains routing information• Individual<ul style="list-style-type: none">contains the last name	String(1..20)	O	O
X4	The correspondent X4 part. Present if correspondent type is Individual	String(1..20)	O	O
FinancialInstitution	Name of the institution.	String(1..105)	O	O
BranchInformation	Branch information.	String(1..70)	O	O
CityName	City name.	String(1..35)	O	O
Location	Location.	String(1..105)	O	O
CountryCode	Country code.	String(2..2)	O	O

TargetApplication

This element is not used by MQSA.

Element	Description	Type	From	To
TargetApplicationRule	The routing function to be performed on the message by Alliance Access. Possible values are: <ul style="list-style-type: none">• InternalRouting<ul style="list-style-type: none">The target routing point is determined by the Alliance Access routing rules.• CBTApplication<ul style="list-style-type: none">The target routing point is determined by the value of DispositionState (see "MessageLPI").• RoutingPoint	String	M	--

Element	Description	Type	From	To
	The target routing point is specified in TargetRoutingPoint.			
TargetRoutingPoint	The target routing point. Mandatory if TargetRoutingRule is "RoutingPoint".	String(1..20)	O	--

MessageOrigin

Element	Description	Type	From	To
CBTApplication	The Alliance Access application that created the message. Possible values are: <ul style="list-style-type: none">• ApplicationInterface• SwiftnetInterface• MessageEntry• Messenger• Other	String	--	M
MessagePartner	The Message Partner that created the message. Present if CBTApplication is ApplicationInterface. Not applicable to MQSA.	String	--	O
SessionNr	The session number. Present if CBTApplication is ApplicationInterface. Not applicable to MQSA.	Integer	--	O
SeqNr	The sequence number. Mandatory when MessagePartner is present. Not applicable to MQSA.	Integer	--	O

FormatAttribute

Element	Description	Type	From	To
FormatAttributeMX	MX format attributes	FormatAttributeMX	M	M

FormatAttributeMX

Element	Description	Type	From	To
None	Reserved for future use.			

A.2.6.1.4 Additional Information

Introduction

The elements described in this section are not included in the DataPDU schema described in "Structure of the DataPDU".

- AckNack
- SwGbl:Status
- Sw:SnFPDMHistory
- Sw:NotifSnFRequestHandle
- SwInt:ValidationDescriptor

These are Alliance Access or SWIFTNet specific data elements that Alliance Access provides to the application for completeness. Further processing of these elements is not required, but their structure is listed below. Note that the structure of these elements can evolve with future releases of SWIFTNet.

AckNack

Element	Description	Type	From	To
PseudoAckNack	Alliance Access-generated Pseudo SWIFT Acknowledgement (for more information see "Creation of an Emission Appendix").	String	--	M
SwGbl:Status	Optional SWIFTNet report status.	SwGbl:Status	--	O

SwGbl:Status

Element	Description	Type	From	To
SwGbl:StatusAttributes	Report status of top-level processing of called function. Can occur multiple times when the function does iterative processing (for example, a message validation function may return all syntax errors).	SwGbl:StatusAttributes [1..N]	--	M

SwGbl:StatusAttributes

Element	Description	Type	From	To
SwGbl:Severity	Possible values are: <ul style="list-style-type: none"> • Fatal • Transient • Logic • Success • Warning 	String	--	M
SwGbl:Code	Status code. The list of error codes is available in SWIFTNet Link Error Codes (part of the SWIFTNet Link documentation set).	String	--	M

Element	Description	Type	From	To
SwGbl:Parameter	Content depends on the error.	Any [0..N]	--	O
SwGbl:Text	Textual description. No processing, except display/print for information, must be performed on this element.	String	--	O
SwGbl:Action	Proposed corrective action.	String	--	O
SwGbl:Details	Lower level detailed report.	SwGbl:Details [0..N]	--	O

SwGbl:Details

Element	Description	Type	From	To
SwGbl:Code	Status code.	String	--	M
SwGbl:Text	Textual description.	String	--	O
SwGbl:Action	Proposed corrective action.	String	--	O

An example of the SwGbl:Status can be found in the Transmission Report samples listed in "File Transfer Examples".

Sw:SnFPDMHistory

Element	Description	Type	From	To
Sw:SnFPDMHistory	In case of previous delivery attempts, gives the delivery attempt history.	Sw:SnFDeliveryHistory	--	M

Sw:SnFDeliveryHistory

Element	Description	Type	From	To
Sw:SnFDeliveryInfo	Message delivery information. In case of disaster take-over (SWIFT side), all messages present in the queue at the moment of the disaster are flagged for possible duplicate delivery, but without delivery information.	Sw:SnFDeliveryInfo [0..N]	--	O

Sw:SnFDeliveryInfo

Element	Description	Type	From	To
Sw:SwiftTime	SWIFT time of the delivery attempt (UTC). Format: YYYY-MM-DDTHH:MM:SSZ	String	--	O
SwSec:UserDN	Authoriser DN of the session owner.	String	--	O
Sw:SnFSessionId	Store-and-forward session identifier when the message was delivered. Format: <queue>:(d p):<6 digit session number>	String	--	O
SwInt:SNLId	SNL ID of the physical SWIFTNet Link where message was delivered.	String	--	O

Element	Description	Type	From	To
Sw:RetryReason	Reason why the message failed delivery.	SwGbl>Status [0..1]	--	O

Sample SnFPDMHistory structure as described in the previous tables:

```

<Sw:SnFPDMHistory>
  <Sw:SnFDeliveryInfo>
    <Sw:SwiftTime>2003-07-19T08:58:37Z</Sw:SwiftTime>
    <SwSec:UserDN>ou=zurich,o=bankwxyz,o=swift</SwSec:UserDN>
    <Sw:SnFSessionId>bankwxyz_applicq1:p:000458</Sw:SnFSessionId>
    <SwInt:SNLId>SNL00835D1</SwInt:SNLId>
    <Sw:RetryReason>
      <SwGbl>Status>
        <SwGbl>StatusAttributes>
          <SwGbl:Severity>Transient</SwGbl:Severity>
          <SwGbl:Code>See Error Guide</SwGbl:Code>
          <SwGbl:Text>One liner error description</SwGbl:Text>
          <SwGbl:Action>Retry Message</SwGbl:Action>
        </SwGbl>StatusAttributes>
      </SwGbl>Status>
    </Sw:RetryReason>
  </Sw:SnFDeliveryInfo>
</Sw:SnFPDMHistory>

```

Sw:NotifySnFRequestHandle

Element	Description	Type	From	To
Sw:SnFRef	Store-and-forward message reference of the notification. Contains the SwiftRef of the original message (see "SWIFTNetRequestAttribute").	String	--	M
Sw:SnFRefType	Type of message for which this notification is provided. Possible values: <ul style="list-style-type: none">• InterAct	String	--	M
Sw:AcceptStatus	Type of store-and-forward notification Possible values: <ul style="list-style-type: none">• Accepted: message accepted by the receiver• Rejected: message rejected by the receiver• Failed: SWIFT failed to deliver the message	String	--	M
Sw:AckSwiftTime	The SWIFT acceptance time of the request ("Accepted", "Rejected") or generation time of the delivery notification request ("Failed") in UTC. Format: YYYY-MM-DDTHH:MM:SSZ	String	--	M
Sw:AckDescription	Provides information about the acknowledgement. Free text.	String	--	O

Element	Description	Type	From	To
	<p>In case the Sw:AcceptStatus is "Failed" (delivery notification generated by SWIFT), the Sw:AckDescription contains the following:</p> <ul style="list-style-type: none"> • Message has expired (code SwGbl.MessageExpired) • Message delivery attempts exceeded system threshold (code SwGbl.MaxRetryExceeded) 			
Sw:AckInfo	<p>Provides information about the acknowledgement.</p> <p>Structured data that the client can analyse.</p> <p>In case the Sw:AcceptStatus is "Failed" (delivery notification generated by SWIFT), the Sw:AckInfo contains the following:</p> <p>SwRejectCode=<reject code></p> <p>Where the reject code is:</p> <ul style="list-style-type: none"> • SwGbl.MessageExpired • SwGbl.MaxRetryExceeded 	String	--	O

An example of this can be found in the DeliveryReport listed in "File Transfer Examples".

SwInt:ValidationDescriptor

Element	Description	Type	From	To
SwInt:ValResult	<p>Indicates the result of validation.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Success • Warning • Fatal (not currently used) 	String	--	M
SwInt:ValStatus	<p>This contains the details of error(s) found.</p> <p>More than one SwGbl:StatusAttributes can be present.</p> <p>Present if SwInt:ValResult is different from Success.</p>	SwGbl:Status	--	O

Example:

```

<SwInt:ValResult>Warning</SwInt:ValResult>
<SwInt:ValStatus>
  <SwGbl:StatusAttributes>
    <SwGbl:Severity>Warning</SwGbl:Severity>
    <SwGbl:Code><!--SWIFTStandards error code--></SwGbl:Code>
    <SwGbl:Text><!--additional diagnostic information--></SwGbl:Text>
  </SwGbl:StatusAttributes>
</SwInt:ValStatus>

```

A.2.6.2 Message Emission Flow

A.2.6.2.1 Creation of an Emission Appendix

Description

An appendix holds the details of the emission or the reception of a message. This appendix is used to generate the Transmission Notification as described earlier in the Intervention Text of the TransmissionReport.

Creation of an Emission Appendix with this Information

For each attempt to send a message, an emission appendix is created containing the following information:

- IAPP name: SWIFTNet Network
- Appendix type: Emission
- Session Holder: The Emission Profile name
- Session Number: The Session Number
- Sequence Number: The Sequence Number
- Receiver delivery status:
 - if no reconciliation: '-'
 - if reconciliation: "Delivered to receiver"
- Network Delivery Status: Network ACK

Generation of a Pseudo SWIFT Acknowledgement (ACKNAK)

Upon unsuccessful emission the reason code is filled in the emission appendix in a Pseudo SWIFT acknowledgement described as follows.

The ACKNAK element is not defined in the XSD specified in "Structure of the DataPDU". The Intervention Text being of type Any can contain any kind of information or free text message.

Reason	Code	Text
Transmission error	T02	This contains all items where in <SwGbl>Status>, <SwGbl:Severity> Fatal or Transient and <SwGbl:Code> equals Sw.Gbl.NetworkTransmissionError. The text of the <SwGbl.Details><SwGbl:Code> (first occurrence) is put in the text of the appendix. If the <SwGbl.Details> is not present, then the text is empty.
Unknown	T03	All other cases: The text of the <SwGbl.Details><SwGbl:Code> (first occurrence) is put in the text of the appendix. If the <SwGbl.Details> is not present, then the text is empty.

Upon (successful or unsuccessful) transmission response, the ack/nak text field of the emission appendix is updated and the <SwGbl>Status> is appended to the PseudoAckNack as follows:

```
<AckNack><PseudoAckNack>{1:F21<BIC8(Sender_X1)>A<Branch(Sender_X1)
<SessionNbr><SequenceNbr>}{4:{177:<LocalTime(YYMMDDHHMM)>}
{451:0(Ack)/1(Nack)}[{405:<Code>}]{311:ACK/NAK\r\n<Text>}
{108:<Message_User_Reference(1..16)>}}</PseudoAckNack>
<SwGbl>Status>...</SwGbl>Status></AckNack>
```

Transmission to Back Office

Transmission notification is transmitted to the Back-Office through a TransmissionReport.

A.2.6.2.2 User Delivery Notifications from SWIFTNet Store-and-forward

Description

After successful emission to the store-and-forward central system, the following delivery notification can be received:

- Successful delivery notification (optional): A User Delivery Report message (DELIVERED) is created and routed to the Traffic Reconciliation component.
- Failed delivery notification: A User Delivery Report message (REJECTED) is created and routed to the Traffic Reconciliation component.

Delivery notifications are reconciled with the original request.

If the original message is found, then the emission appendix is updated with the delivery status.

If TRS is configured to generate a delivery notification (Traffic recon - Delivery Notif), a pseudo User Delivery notification message (internal to Alliance Access) is created in the _TR_NOTIF routing point (with message nature NETWORK_MSG, Sender = DYLRXXXXXX (in case of delivery notification) or ABLRXXXXXX (in case of delayed NAK or abort notification), unit = None), and routed to the _TR_REC routing point with "Delivered" (positive delivery notification) or "Undelivered" (failed delivery notification) as processing result through an updated internal routing rule.

Details of the delivery notification, as contained in the SWIFTNet data element NotifySnFRequestHandle of the received delivery notification, are also added as an intervention of category Deliveryreport to the original message instance by the standard TRREC functionality.

The NotifySnFRequestHandle structure for SWIFTNet release 6.0.0 is shown in the following example (note the structure of this element can evolve with future releases of SWIFTNet):

```
<Sw:NotifySnFRequestHandle>
  <Sw:SnFRef>SWITCH90-2005-05-25T15:51:14.9525.238697Z</Sw:SnFRef>
  <Sw:SnFRefType>InterAct</Sw:SnFRefType>
  <Sw:AcceptStatus>Accepted</Sw:AcceptStatus>
  <Sw:AckSwiftTime>2005-05-25T15:48:33Z</Sw:AckSwiftTime>
  <Sw:AckInfo>Acked</Sw:AckInfo>
</Sw:NotifySnFRequestHandle>
```

If the original message is not found, the notification is only journalised.

Transmission to Back-Office

The Alliance Delivery Notification instance created by TRREC is transmitted to the Back Office through a Delivery Report. Reconciliation at the back office can be done based on the UserReference.

A.2.6.2.3 Business Response for SWIFTNet Real-Time

Generation of a Transmission Response Intervention

In real-time delivery mode, the response can be a business response. In such a case, the response payload (if any) is stored as an Intervention of a new category "Transmission response" and is appended to the original instance.

If a Transmission Notification is created then it contains the date-time and sequence number of this intervention.

Transmission to Back-Office

The business response can be transmitted to the back-office application through Transmission Report.

It is the back-office responsibility to process the intervention accordingly.

A.2.6.3 Message Reception Flow

A.2.6.3.1 Real-Time Reception

Description

Messages are created in the _SI_from_SWIFTNet routing point and are immediately made available for processing (routed) to the back office.

An empty InterAct response is generated for each message.

Reception Appendix

A reception appendix is created with the following key information:

- IAPP Name: SWIFTNet Network
- Appendix Type: Reception
- Session Holder: SWIFTNet Link Endpoint on which the message was received (present in the SWIFTNet Link header)
- Session Number: Current Session Number
- Sequence Number: Current Sequence Number
- Network Delivery Status: <empty>
- Receiver Delivery Status: Receiver ACKed

A.2.6.3.2 Store-and-forward Reception

Description

Store-and-forward messages can be received as soon as the queue is Active (acquired).

Upon reception:

- Messages are created in the _SI_from_SWIFTNet routing point and are immediately made available for processing (routed) to the back office.
- Each message is acknowledged positively in the response sent to the central store-and-forward engine.

Reception Appendix

A reception appendix is created for a requests delivery notification with the following key information:

- IAPP Name: SWIFTNet Network
- Appendix Type: Reception
- Session Holder: Store-and-forward queue name

- Session Number: Session Number taken from the store-and-forward Session Identifier
- Sequence Number: Sequence Number taken from the store-and-forward output sequence number
- Network Delivery Status: ACKed

A.2.6.4 File Transfer Examples

Introduction

The following sections show DataPDU examples for:

- Store-and-forward:
 - Message sent by an application to Alliance Access
 - Transmission Report sent by Alliance Access to the application (ACK)
 - Transmission Report sent by Alliance Access to the application (Nack)
This was triggered by putting an unknown tag in the message payload, causing a Message Validation error (MVal error)
 - Transmission Report (ACK) including the original message sent by Alliance Access to the application
 - Delivery Report sent by Alliance Access to the application
 - Message sent by Alliance Access to the application
- Real time:
 - Message sent by an application to Alliance Access
 - Transmission Report Sent by Alliance Access to the application (including a real-time business response)

A.2.6.4.1 Store-and-forward

Message sent by an application to Alliance Access

```
<?xml version="1.0" encoding="utf-8"?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01">
  <Saa:Message>
    <Saa:MessageFormat>MX</Saa:MessageFormat>
    <Saa:MessageSubFormat>Input</Saa:MessageSubFormat>
    <Saa:Sender>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Sender>
    <Saa:Receiver>
      <Saa:FullName>
        <Saa:X1>SAADBEBBXXX</Saa:X1>
      </Saa:FullName>
    </Saa:Receiver>
    <Saa:MessageNature>FinancialNature</Saa:MessageNature>
    <Saa:MessageLPI>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbabb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbabb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.if.ia</Saa:Service>
        <Saa:RequestType>setr.016.001.02</Saa:RequestType>
```

```

<Saa:NRIndicator>true</Saa:NRIndicator>
</Saa:SWIFTNetRequestAttribute>
</Saa:NetworkAttribute>
<Saa:SecurityAttribute>
  <Saa:SWIFTNetSecurityAttribute>
    <Saa:SigningRequired>true</Saa:SigningRequired>
  </Saa:SWIFTNetSecurityAttribute>
</Saa:SecurityAttribute>
</Saa:MessageLPI>
<Saa:MessageTPI>
  <Saa:NetworkDelivNotify>true</Saa:NetworkDelivNotify>
  <Saa:NetworkPriority>Normal</Saa:NetworkPriority>
</Saa:MessageTPI>
<Saa:MessageSRI>
  <Saa:UserReference>Sample-XMLv1-0609141402</Saa:UserReference>
</Saa:MessageSRI>
<Saa:MessageText>
  <AppHdr xmlns="urn:swift:xsd:$ahV10">
    <MsgRef>Sample-XMLv1-0609141402</MsgRef>
    <CrDate>2006-09-14T02:02:11.414</CrDate>
  </AppHdr>
  <Document xmlns="urn:swift:xsd:swift.if.ia$setr.016.001.02">
    <setr.016.001.02>
      <RltdRef>
        <Ref>Ref123-1</Ref>
      </RltdRef>
      <IndvOrdrDtlsRpt>
        <Sts>PACK</Sts>
        <OrdrRef>Ref123-1</OrdrRef>
      </IndvOrdrDtlsRpt>
    </setr.016.001.02>
  </Document>
</Saa:MessageText>
</Saa:Message>
</Saa:DataPDU>

```

Transmission Report sent by Alliance Access to the application (Ack)

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv1-0609141402</
  Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>ApplicationInterface</Saa:CBTApplication>
        <Saa:MessagePartner>MXInput</Saa:MessagePartner>
        <Saa:SessionNr>0005</Saa:SessionNr>
        <Saa:SeqNr>000001</Saa:SeqNr>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:OriginalRelatedMessage>true</Saa:OriginalRelatedMessage>
      <Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
      <Saa:BackToNonOriginator>true</Saa:BackToNonOriginator>
    </Saa:ReportLPI>
    <Saa:TransmissionReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>

```

```

<Saa:Service>swift.if.ia</Saa:Service>
<Saa:RequestType>setr.016.001.02</Saa:RequestType>
<Saa:NonRepType>SvcMand</Saa:NonRepType>
<Saa:SwiftRef>SWITCH90-2006-09-14T13:21:26.25214.2015075Z</Saa:SwiftRef>
<Saa:SwiftRequestRef>SNL10391-2006-09-14T13:21:24.55820.000505Z
  </Saa:SwiftRequestRef>
<Saa:CBTReference>a7e67cde-e52a-4b0c-a3ad-af3f97dbaa6e</Saa:CBTReference>
<Saa:SnFInputTime>0102:2006-09-14T13:13:12</Saa:SnFInputTime>
</Saa:SWIFTNetRequestAttribute>
<Saa:SWIFTNetResponseAttribute>
  <Saa:ResponderDN>cn=messaging,o=swift,o=swift</Saa:ResponderDN>
  <Saa:SwiftResponseRef>snp00006-2006-09-14T13:21:48.25306.002002Z
    </Saa:SwiftResponseRef>
</Saa:SWIFTNetResponseAttribute>
</Saa:NetworkAttribute>
<Saa:NetworkSessionNr>000005</Saa:NetworkSessionNr>
<Saa:NetworkSeqNr>00000001</Saa:NetworkSeqNr>
<Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
<Saa:Interventions>
  <Saa:Intervention>
    <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
    <Saa:CreationTime>060914152112</Saa:CreationTime>
    <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
    <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
    <Saa:Text>
      <AckNack>
        <PseudoAckNack>{1:F21SAADBEBBAXXX000005000000001}{4:{177:0609141521}
{451:0}{311:ACK}{108:Sample-XMLv1-0609141402}}</PseudoAckNack>
      </AckNack>
    </Saa:Text>
  </Saa:Intervention>
</Saa:Interventions>
</Saa:TransmissionReport>
</Saa:Report>
</Saa:DataPDU>

```

Transmission Report sent by Alliance Access to the application (Nack)

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv10609141402
  </Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>ApplicationInterface</Saa:CBTApplication>
        <Saa:MessagePartner>MXInput</Saa:MessagePartner>
        <Saa:SessionNr>0005</Saa:SessionNr>
        <Saa:SeqNr>000001</Saa:SeqNr>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:OriginalRelatedMessage>true</Saa:OriginalRelatedMessage>
      <Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
      <Saa:BackToNonOriginator>true</Saa:BackToNonOriginator>
    </Saa:ReportLPI>
    <Saa:TransmissionReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>

```

```

<Saa:Service>swift.if.ia</Saa:Service>
<Saa:RequestType>setr.016.001.02</Saa:RequestType>
<Saa:CBTReference>a7e67cde-e52a-4b0c-a3ad-af3f97dbaa6e</Saa:CBTReference>
</Saa:SWIFTNetRequestAttribute>
<Saa:SWIFTNetResponseAttribute/>
</Saa:NetworkAttribute>
<Saa:NetworkSessionNr>000002</Saa:NetworkSessionNr>
<Saa:NetworkSeqNr>00000008</Saa:NetworkSeqNr>
<Saa:NetworkDeliveryStatus>NetworkNacked</Saa:NetworkDeliveryStatus>
<Saa:Interventions>
  <Saa:Intervention>
    <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
    <Saa:CreationTime>061011143408</Saa:CreationTime>
    <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
    <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
    <Saa:Text>
      <AckNack>
        <PseudoAckNack>{1:F21SAADBEBBAXXX000002000000008}{4:{177:0610111435}
{451:1}{405:T02}{311:NAK Sw.WFE.eMVALError}{108:Sample-XMLv1-0609141402}}</
PseudoAckNack>
        <SwGbl:Status>
          <SwGbl:StatusAttributes>
            <SwGbl:Severity>Transient</SwGbl:Severity>
            <SwGbl:Code>Sw.Gbl.NetworkTransmissionError</SwGbl:Code>
            <SwGbl:Parameter>16899</SwGbl:Parameter>
            <SwGbl:Parameter>message validation failed with error</
SwGbl:Parameter>
          <SwGbl:Text>Network Transmission Error</SwGbl:Text>
          <SwGbl:Details>
            <SwGbl:Code>Sw.WFE.eMVALError</SwGbl:Code>
            <SwGbl:Text>MVAL component error., message validation failed with
error</SwGbl:Text>
          </SwGbl:Details>
          <SwGbl:Details>
            <SwGbl:Code>Sw.WFE.ExecuteRequestFail</SwGbl:Code>
            <SwGbl:Text>Execute Request failed in WFE , MVAL</SwGbl:Text>
          </SwGbl:Details>
          <SwGbl:Details>
            <SwGbl:Code>Sw.WFE.ExecuteRequestFail</SwGbl:Code>
            <SwGbl:Text>Execute Request failed in WFE </SwGbl:Text>
          </SwGbl:Details>
          <SwGbl:StatusAttributes>
            <SwGbl:Severity>Fatal</SwGbl:Severity>
            <SwGbl:Code>Sw.MVAL.SyntaxException</SwGbl:Code>
            <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]/IndvOrdrDtlsRpt1[1]</SwGbl:Parameter>
            <SwGbl:Text>unexpected content "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}IndvOrdrDtlsRpt1"; expected "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}MstrRef" or "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}IndvOrdrDtlsRpt" or "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}OrdrDtlsRpt" or "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}RltdRef"</SwGbl:Text>
          </SwGbl:StatusAttributes>
          <SwGbl:StatusAttributes>
            <SwGbl:Severity>Fatal</SwGbl:Severity>
            <SwGbl:Code>Sw.MVAL.SyntaxException</SwGbl:Code>
            <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]/IndvOrdrDtlsRpt1[1]
          </SwGbl:Parameter>
          <SwGbl:Text>no declaration for element "{urn:swift:xsd:swift.if.ia
$setr.016.001.02}IndvOrdrDtlsRpt1"</SwGbl:Text>
        </SwGbl:StatusAttributes>
        <SwGbl:StatusAttributes>
          <SwGbl:Severity>Fatal</SwGbl:Severity>
          <SwGbl:Code>Sw.MVAL.SyntaxException</SwGbl:Code>

```

```

        <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]/IndvOrdrDtlsRpt1[1]/Sts[1]</SwGbl:Parameter>
        <SwGbl:Text>no declaration for element "{urn:swift:xsd:swift.if.ia
$setr.016.001.02}Sts"</SwGbl:Text>
        </SwGbl:StatusAttributes>
        <SwGbl:StatusAttributes>
        <SwGbl:Severity>Fatal</SwGbl:Severity>
        <SwGbl:Code>Sw.MVAL.SyntaxError</SwGbl:Code>
        <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]/IndvOrdrDtlsRpt1[1]/OrdrRef[1]</SwGbl:Parameter>
        <SwGbl:Text>no declaration for element "{urn:swift:xsd:swift.if.ia
$setr.016.001.02}OrdrRef"</SwGbl:Text>
        </SwGbl:StatusAttributes>
        <SwGbl:StatusAttributes>
        <SwGbl:Severity>Fatal</SwGbl:Severity>
        <SwGbl:Code>Sw.MVAL.SyntaxError</SwGbl:Code>
        <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]</SwGbl:Parameter>
        <SwGbl:Text>unexpected end of content</SwGbl:Text>
        </SwGbl:StatusAttributes>
        </SwGbl:Status>
        </AckNack>
        </Saa:Text>
        </Saa:Intervention>
        </Saa:Interventions>
        </Saa:TransmissionReport>
        </Saa:Report>
</Saa:DataPDU>

```

Transmission Report (Ack) including the original message

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>Full</Saa:OrigMessageFields>
    <Saa:OrigMessage>
      <Saa:MessageFormat>MX</Saa:MessageFormat>
      <Saa:MessageSubFormat>Input</Saa:MessageSubFormat>
      <Saa:Sender>
        <Saa:X1>SAADBEBBXXX</Saa:X1>
      </Saa:Sender>
      <Saa:Receiver>
        <Saa:FullName>
          <Saa:X1>SAADBEBBXXX</Saa:X1>
        </Saa:FullName>
      </Saa:Receiver>
      <Saa:LiveMessage>true</Saa:LiveMessage>
      <Saa:MessageNature>FinancialNature</Saa:MessageNature>
      <Saa:MessageLPI>
        <Saa:OriginalMessage>false</Saa:OriginalMessage>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.if.ia</Saa:Service>
          <Saa:RequestType>setr.016.001.02</Saa:RequestType>
          <Saa:NonRepType>SvcMand</Saa:NonRepType>
          <Saa:SwiftRef>SWITCH90-2006-09-14T13:21:26.25214.2015075Z</Saa:SwiftRef>
          <Saa:SwiftRequestRef>SNL10391-2006-09-14T13:21:24.55820.000505Z
        </Saa:SwiftRequestRef>
    
```

```

<Saa:CBTReference>a7e67cde-e52a-4b0c-a3ad-af3f97dbaa6e</
Saa:CBTReference>
  <Saa:SnFInputTime>0102:2006-09-14T13:13:12</Saa:SnFInputTime>
  </Saa:SWIFTNetRequestAttribute>
  <Saa:SWIFTNetResponseAttribute>
    <Saa:ResponderDN>cn=messaging,o=swift,o=swift</Saa:ResponderDN>
    <Saa:SwiftResponseRef>snp00006-2006-09-14T13:21:48.25306.002002Z
    </Saa:SwiftResponseRef>
  </Saa:SWIFTNetResponseAttribute>
  </Saa:NetworkAttribute>
  <Saa:SecurityAttribute>
    <Saa:SWIFTNetSecurityAttribute>
      <Saa:SignerDN>cn=rma2,o=saadbebb,o=swift</Saa:SignerDN>
    </Saa:SWIFTNetSecurityAttribute>
  </Saa:SecurityAttribute>
  <Saa:MessageOrigin>
    <Saa:CBTApplication>ApplicationInterface</Saa:CBTApplication>
    <Saa:MessagePartner>MXInput</Saa:MessagePartner>
    <Saa:SessionNr>0005</Saa:SessionNr>
    <Saa:SeqNr>000001</Saa:SeqNr>
  </Saa:MessageOrigin>
  <Saa:CBTRoutingInfo>MXAck</Saa:CBTRoutingInfo>
  </Saa:MessageLPI>
  <Saa:MessageTPI>
    <Saa:Network>SwiftNetNetwork</Saa:Network>
    <Saa:NetworkPriority>Normal</Saa:NetworkPriority>
    <Saa:NetworkSessionNr>000005</Saa:NetworkSessionNr>
    <Saa:NetworkSeqNr>00000001</Saa:NetworkSeqNr>
  </Saa:MessageTPI>
  <Saa:MessageSRI>
    <Saa:UserReference>Sample-XMLv1-0609141402</Saa:UserReference>
  </Saa:MessageSRI>
  <Saa:MessageText>
    <AppHdr xmlns="urn:swift:xsd:$ahV10">
      <MsgRef>Sample-XMLv1-0609141402</MsgRef>
      <CrDate>2006-09-14T02:02:11.414</CrDate>
    </AppHdr>
    <Document xmlns="urn:swift:xsd:swift.if.ia$setr.016.001.02">
      <setr.016.001.02>
        <RltdRef>
          <Ref>Ref123-1</Ref>
        </RltdRef>
        <IndvOrdrDtlsRpt>
          <Sts>PACK</Sts>
          <OrdrRef>Ref123-1</OrdrRef>
        </IndvOrdrDtlsRpt>
      </setr.016.001.02>
    </Document>
  </Saa:MessageText>
  </Saa:OrigMessage>
  <Saa:ReportLPI>
    <Saa:MessageOrigin>
      <Saa:CBTApplication>ApplicationInterface</Saa:CBTApplication>
      <Saa:MessagePartner>MXInput</Saa:MessagePartner>
      <Saa:SessionNr>0005</Saa:SessionNr>
      <Saa:SeqNr>000001</Saa:SeqNr>
    </Saa:MessageOrigin>
    <Saa:Modified>false</Saa:Modified>
    <Saa:OriginalRelatedMessage>true</Saa:OriginalRelatedMessage>
    <Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
    <Saa:BackToNonOriginator>true</Saa:BackToNonOriginator>
  </Saa:ReportLPI>
  <Saa:TransmissionReport>
    <Saa:Network>SwiftNetNetwork</Saa:Network>
    <Saa:NetworkAttribute>
      <Saa:SWIFTNetRequestAttribute>
        <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>

```

```

<Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
<Saa:Service>swift.if.ia</Saa:Service>
<Saa:RequestType>setr.016.001.02</Saa:RequestType>
<Saa:NonRepType>SvcMand</Saa:NonRepType>
<Saa:SwiftRef>SWITCH90-2006-09-14T13:21:26.25214.2015075Z</Saa:SwiftRef>
<Saa:SwiftRequestRef>SNL10391-2006-09-14T13:21:24.55820.000505Z
</Saa:SwiftRequestRef>
<Saa:CBTReference>a7e67cde-e52a-4b0c-a3ad-af3f97dbaa6e</Saa:CBTReference>
<Saa:SnFInputTime>0102:2006-09-14T13:13:12</Saa:SnFInputTime>
</Saa:SWIFTNetRequestAttribute>
<Saa:SWIFTNetResponseAttribute>
<Saa:ResponderDN>cn=messaging,o=swift,o=swift</Saa:ResponderDN>
<Saa:SwiftResponseRef>snp00006-2006-09-14T13:21:48.25306.002002Z
</Saa:SwiftResponseRef>
</Saa:SWIFTNetResponseAttribute>
</Saa:NetworkAttribute>
<Saa:NetworkSessionNr>000005</Saa:NetworkSessionNr>
<Saa:NetworkSeqNr>00000001</Saa:NetworkSeqNr>
<Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
<Saa:Interventions>
<Saa:Intervention>
<Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
<Saa:CreationTime>060914152112</Saa:CreationTime>
<Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
<Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
<Saa:Text>
<AckNack>
<PseudoAckNack>{1:F21SAADBEBBAXXX00005000000001}{4:{177:0609141521}
{451:0}{311:ACK}{108:Sample-XMLv1-0609141402}}</PseudoAckNack>
</AckNack>
</Saa:Text>
</Saa:Intervention>
</Saa:Interventions>
</Saa:TransmissionReport>
</Saa:Report>
</Saa:DataPDU>

```

Delivery Report sent by Alliance Access to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>ApplicationInterface</Saa:CBTApplication>
        <Saa:MessagePartner>MXInput</Saa:MessagePartner>
        <Saa:SessionNr>0005</Saa:SessionNr>
        <Saa:SeqNr>00001</Saa:SeqNr>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:OriginalRelatedMessage>true</Saa:OriginalRelatedMessage>
      <Saa:ReportingApplication>Traffic Recon</Saa:ReportingApplication>
      <Saa:BackToNonOriginator>true</Saa:BackToNonOriginator>
    </Saa:ReportLPI>
    <Saa:DeliveryReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>

```

```

<Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
<Saa:Service>swift.if.ia</Saa:Service>
<Saa:RequestType>setr.016.001.02</Saa:RequestType>
<Saa:NonRepType>SvcMand</Saa:NonRepType>
<Saa:SwiftRef>SWITCH90-2006-09-14T13:21:26.25214.2015075Z</Saa:SwiftRef>
<Saa:SwiftRequestRef>SNL10391-2006-09-14T13:21:24.55820.000505Z
</Saa:SwiftRequestRef>
<Saa:CBTReference>a7e67cde-e52a-4b0c-a3ad-af3f97dbaa6e</Saa:CBTReference>
<Saa:SnFInputTime>0102:2006-09-14T13:13:12</Saa:SnFInputTime>
</Saa:SWIFTNetRequestAttribute>
<Saa:SWIFTNetResponseAttribute>
<Saa:ResponderDN>cn=messaging,o=swift,o=swift</Saa:ResponderDN>
<Saa:SwiftResponseRef>snp00006-2006-09-14T13:21:48.25306.002002Z
</Saa:SwiftResponseRef>
</Saa:SWIFTNetResponseAttribute>
</Saa:NetworkAttribute>
<Saa:NetworkSessionNr>000005</Saa:NetworkSessionNr>
<Saa:NetworkSeqNr>00000001</Saa:NetworkSeqNr>
<Saa:ReceiverDeliveryStatus>RcvDelivered</Saa:ReceiverDeliveryStatus>
<Saa:Interventions>
<Saa:Intervention>
<Saa:IntvCategory>DeliveryReport</Saa:IntvCategory>
<Saa:CreationTime>060914152453</Saa:CreationTime>
<Saa:ApplicationOrigin>TRS</Saa:ApplicationOrigin>
<Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
<Saa:Text>
<Sw:NotifySnFRequestHandle>
<Sw:SnFRef>SWITCH90-2006-09-14T13:21:26.25214.2015075Z</Sw:SnFRef>
<Sw:SnFRefType>InterAct</Sw:SnFRefType>
<Sw:AcceptStatus>Accepted</Sw:AcceptStatus>
<Sw:AckSwiftTime>2006-09-14T13:21:50Z</Sw:AckSwiftTime>
<Sw:AckInfo>Acked</Sw:AckInfo>
</Sw:NotifySnFRequestHandle>
</Saa:Text>
</Saa:Intervention>
</Saa:Interventions>
</Saa:DeliveryReport>
</Saa:Report>
</Saa:DataPDU>

```

Message sent by Alliance Access to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>OSAADBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Message>
    <Saa:MessageFormat>MX</Saa:MessageFormat>
    <Saa:MessageSubFormat>Output</Saa:MessageSubFormat>
    <Saa:Sender>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Sender>
    <Saa:Receiver>
      <Saa:FullName>
        <Saa:X1>SAADBEBBXXX</Saa:X1>
      </Saa:FullName>
    </Saa:Receiver>
    <Saa:LiveMessage>true</Saa:LiveMessage>
    <Saa:MessageNature>FinancialNature</Saa:MessageNature>
    <Saa:MessageLPI>
      <Saa:OriginalMessage>true</Saa:OriginalMessage>
    <Saa:NetworkAttribute>
      <Saa:SWIFTNetRequestAttribute>
        <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
        <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>

```

```

<Saa:Service>swift.if.ia</Saa:Service>
<Saa:RequestType>setr.016.001.02</Saa:RequestType>
<Saa:NonRepType>SvcMand</Saa:NonRepType>
<Saa:SwiftRef>SWITCH90-2006-09-14T13:21:26.25214.2015075Z</Saa:SwiftRef>
<Saa:SwiftRequestRef>SNL10391-2006-09-14T13:21:24.55820.000505Z
</Saa:SwiftRequestRef>
<Saa:CBTReference>e6af835e-1dd1-11b2-9214-092595955b82</Saa:CBTReference>
<Saa:SNLEndPoint>sni_sms6560</Saa:SNLEndPoint>
<Saa:SnFQueueName>saadbebb_ifia</Saa:SnFQueueName>
<Saa:ValidationDescriptor>
  <SwInt:ValResult>Success</SwInt:ValResult>
</Saa:ValidationDescriptor>
<Saa:AuthResult>Success</Saa:AuthResult>
<Saa:AuthValue>
  <SwSec:CryptoInternal>

<SwSec:CipherKey>UEVNRkBQcm9jLVR5cGU6IDQsTUlDLU90TFkNCkNvbnRlbnQtRG9tYWluOibSR
kM4MjINCKvudHJ1c3RGaWx1LVZ1cnNpb246IDIuMA0KT3JpZ2luYXRvc1ETjogY249cm1hMixvPXN
hYWRiZWJiLG89c3dpZnQNCK9yaWctU046IDEExNDc3ODU1NjYNCK1JQy1JbmZvOibTSEEExLCBSU0EsD
QogcnhjSVaZWEjRVd0WnBTYj0Y2tjenFOc25nMG5rRk15R0FrSDhkRHZhM203M1R1ellQUj11VF1
mRNWUb1VTZA0KIH1VR3ROVkV1eWFkM21tbla5akJiQvhjN0c4ekpmVUlnaWgyWVgwcWc0QTF6UFV5T
EJXcmVOOGdNWFBiVndKd1YNCiBEdXFKK0svdk9PM2VwY2VeeFYzWkhIS1BKY000Y0NSYkFMQXB1Yw1
1ZGxyUWRLZVV5Q3lsOTHpOHNuNFQ4UWhpDQogUjB3VFZJeWk0RTNnY3FFSC9ubFV5M082ZnBtNF1CN
k16TWYxNVEzVVZONHdMVnhCNEpkSjJveGVpelBIY1vqVg0KIEAbUNmSEg5dTBSb0pWTjd4TlpKWXh
sRmRybjFPd2J1c3RETT1TSmNPUjY10Fg5WFhKV3NWWXphT08xQTg1cCsNCiAwNFFzU0k2N1VZR2Zx
m1TaStIVVRnPT0NCg==</SwSec:CipherKey>
  <SwSec: CryptoProtocol>4.0:3.0</SwSec: CryptoProtocol>
</SwSec: CryptoInternal>
<SwSec: CryptoDescriptor>
  <SwSec: MemberRef>RequestPayload</SwSec: MemberRef>
  <SwSec: MemberRef>RequestHeader</SwSec: MemberRef>
  <SwSec: MemberRef>RequestDescriptor.SwiftRequestRef</SwSec: MemberRef>
  <SwSec: SignDN>cn=rma2,o=saadbebb,o=swift</SwSec: SignDN>
  <SwSec: CertPolicyId>1.3.21.6.2</SwSec: CertPolicyId>
</SwSec: CryptoDescriptor>
</Saa:AuthValue>
</Saa:SWIFTNetRequestAttribute>
<Saa:SWIFTNetResponseAttribute/>
</Saa:NetworkAttribute>
<Saa:SecurityAttribute>
  <Saa:SWIFTNetSecurityAttribute>
    <Saa:SignerDN>cn=rma2,o=saadbebb,o=swift</Saa:SignerDN>
  </Saa:SWIFTNetSecurityAttribute>
</Saa:SecurityAttribute>
<Saa:MessageOrigin>
  <Saa:CBTApplication>SwiftnetInterface</Saa:CBTApplication>
</Saa:MessageOrigin>
<Saa:CBTRoutingInfo>MXRecv</Saa:CBTRoutingInfo>
</Saa:MessageLPI>
<Saa:MessageTPI>
  <Saa:Network>SwiftNetNetwork</Saa:Network>
  <Saa:NetworkPriority>Normal</Saa:NetworkPriority>
  <Saa:NetworkSessionNr>979896</Saa:NetworkSessionNr>
  <Saa:NetworkSeqNr>000001559</Saa:NetworkSeqNr>
  <Saa:DuplCreation>PDE</Saa:DuplCreation>
</Saa:MessageTPI>
<Saa:MessageSRI>
  <Saa:UserReference>Sample-XMLv1-0609141402</Saa:UserReference>
</Saa:MessageSRI>
<Saa:MessageText>
  <AppHdr xmlns="urn:swift:xsd:$ahV10">
    <MsgRef>Sample-XMLv1-0609141402</MsgRef>
    <CrDate>2006-09-14T02:02:11.414</CrDate>
  </AppHdr>
<Document xmlns="urn:swift:xsd:swift.if.ia$setr.016.001.02">
  <setr.016.001.02>
    <RltdRef>

```

```

<Ref>Ref123-1</Ref>
</RltdRef>
<IndvOrdrDtlsRpt>
<Sts>PACK</Sts>
<OrdrRef>Ref123-1</OrdrRef>
</IndvOrdrDtlsRpt>
</setr.016.001.02>
</Document>
</Saa:MessageText>
</Saa:Message>
</Saa:DataPDU>

```

A.2.6.4.2 Real time

Message sent by an application to Alliance Access

```

<?xml version="1.0" encoding="utf-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01">
  <Saa:Message>
    <Saa:MessageFormat>MX</Saa:MessageFormat>
    <Saa:MessageSubFormat>Input</Saa:MessageSubFormat>
    <Saa:Sender>
      <Saa:X1>SAASBEBBXXX</Saa:X1>
    </Saa:Sender>
    <Saa:Receiver>
      <Saa:FullName>
        <Saa:X1>SAATBEBBXXX</Saa:X1>
      </Saa:FullName>
    </Saa:Receiver>
    <Saa:MessageNature>FinancialNature</Saa:MessageNature>
    <Saa:MessageLPI>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saasbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>cn=beso,cn=tg229,o=saatbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.cashrepv1</Saa:Service>
          <Saa:RequestType>getaccount</Saa:RequestType>
        </Saa:SWIFTNetRequestAttribute>
      </Saa:NetworkAttribute>
    </Saa:MessageLPI>
    <Saa:MessageTPI>
      <Saa:NetworkPriority>Normal</Saa:NetworkPriority>
    </Saa:MessageTPI>
    <Saa:MessageSRI>
      <Saa:UserReference>REF-1-0609181711</Saa:UserReference>
    </Saa:MessageSRI>
    <Saa:MessageText>
      <Ah:AppHdr xmlns:Ah="urn:swift:xsd:$ahV10">
        <Ah:MsgRef>SCRRQ01</Ah:MsgRef>
        <Ah:CrDate>2006-09-18T17:11:28.359</Ah:CrDate>
      </Ah:AppHdr>
      <Doc:Document xmlns:Doc="urn:swift:xsd:swift.cashrepv1$getaccount" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Doc:getaccount>
          <Doc:NstrAcctSchCrit>
            <Doc:AcctId>
              <Doc:DmstAcct>789DA123</Doc:DmstAcct>
            </Doc:AcctId>
            <Doc:BalTp>AVLB</Doc:BalTp>
          </Doc:NstrAcctSchCrit>
          <Doc:QryPrcg>
            <Doc:QryRef>
              <Doc:Ref>SCRRQ01</Doc:Ref>
            </Doc:QryRef>
          </Doc:QryPrcg>
        </Doc:getaccount>
      </Doc:Document>
    </Saa:MessageText>
  </Saa:Message>
</Saa:DataPDU>

```

```

</Saa:MessageText>
</Saa:Message>
</Saa:DataPDU>

```

Transmission Report sent by Alliance Access to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAATBEBBXXMX REF-1-0609181711</Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAATBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>ApplicationInterface</Saa:CBTApplication>
        <Saa:MessagePartner>MXFileInput</Saa:MessagePartner>
        <Saa:SessionNr>0017</Saa:SessionNr>
        <Saa:SeqNr>000001</Saa:SeqNr>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:OriginalRelatedMessage>true</Saa:OriginalRelatedMessage>
      <Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
      <Saa:BackToNonOriginator>true</Saa:BackToNonOriginator>
    </Saa:ReportLPI>
    <Saa:TransmissionReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saasbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>cn=beso,cn=tg229,o=saatbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.cashrepv1</Saa:Service>
          <Saa:RequestType>getaccount</Saa:RequestType>
          <Saa:SwiftRef>SWITCH90-2006-09-18T15:12:41.24521.1424140Z</Saa:SwiftRef>
          <Saa:SwiftRequestRef>SNL00229-2006-09-18T15:12:39.5656.000017Z
        </Saa:SwiftRequestRef>
        <Saa:CBTReference>b12ba774-c3bf-47df-9e8a-924282c3235c</Saa:CBTReference>
      </Saa:SWIFTNetRequestAttribute>
      <Saa:SWIFTNetResponseAttribute>
        <Saa:ResponderDN>cn=beso,cn=tg229,o=saatbebb,o=swift</Saa:ResponderDN>
        <Saa:NonRepType>SvcMand</Saa:NonRepType>
        <Saa:SwiftResponseRef>SNL00229-2006-09-18T15:12:41.5304.000011Z
      </Saa:SwiftResponseRef>
      <Saa:AuthResult>Success</Saa:AuthResult>
      <Saa:AuthValue>
        <SwSec: CryptoInternal>

        <SwSec: CipherKey>UEVNRkBQcm9jLVR5cGU6IDQsTUlDLU90TFkNCKnVbnRlbnQtRG9tYWluOiBSR
          kM4MjINCKvudHJ1c3RGaWx1LVZ1cnNpb246IDIuMA0KT3JpZ2luYXRvc1ETjogY249cm1hNCxvPXN
          hYXRiZWJiLG89c3dpZnQNCK9yaWctU046IDExNDE5Mzg1MjINCK1JQy1JbmZvOiBTSEExLCBSU0EsD
          QogVmFTNlpqMC9rYnQrZVF0dHRhNmQvcnpPdVhmL3prc1NTeXBSc1RGWUxQOHAzaZFLSDFOVnZacGF
          XWDhoVTY4bg0K1Fo4a1h3a2g1Q3VYNFgvenNQZUdtS1pKWTBvWVZXM3c1cmdyYm5YMjVzQm15cURVc
          y9MYlRxc18wV0d1aUI4ZwQNCiBzR0xRenFRNFh3VmxFGrmlUN0FxWjErUHovQURmQ1Fmemd2N1JibWp
          HWWxrTk54NVnPmUk4ajz5VjU3bnBpSCTvDQogM21MWmhuUFNvcThZbEZ1EhzS3dCOExWNko025yb
          zd1NWRVc2ZjZUVqbUVZeeERGK21qaX1wSytXaUdTVWz1Wg0KIE01R21nUk9rb0k5N2k4STZ4d2J4QUd
          1L3UrZ0M4enJ5NUd1SHVtTE1XcHpRUEsvejVGWmRSTEpqajNGaXJKZW0NCiAyU2pucXo50XNEWUf1b
          WJBT0E5N25RPT0NCg==</SwSec: CipherKey>
        <SwSec: CryptoProtocol>4.0:3.0</SwSec: CryptoProtocol>
      </SwSec: CryptoInternal>
      <Saa:MemberRef>
        <Saa:ResponsePayload></Saa:ResponsePayload>
        <Saa:ResponseHeader></Saa:ResponseHeader>
        <Saa:ResponseDescriptor>SwiftResponseRef</Saa:ResponseDescriptor>
        <Saa:SignDN>cn=rma4,o=saatbebb,o=swift</Saa:SignDN>
      </Saa:MemberRef>
    </Saa:MemberRef>
  </Saa:MemberRef>
</Saa:DataPDU>

```

```

        <SwSec:CertPolicyId>1.3.21.6.2</SwSec:CertPolicyId>
        </SwSec:CryptoDescriptor>
        </Saa:AuthValue>
        </Saa:SWIFTNetResponseAttribute>
        </Saa:NetworkAttribute>
        <Saa:NetworkSessionNr>000005</Saa:NetworkSessionNr>
        <Saa:NetworkSeqNr>00000002</Saa:NetworkSeqNr>
        <Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
        <Saa:Interventions>
        <Saa:Intervention>
        <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
        <Saa:CreationTime>060918171236</Saa:CreationTime>
        <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
        <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
        <Saa:Text>
        <AckNack>
        <PseudoAckNack>{1:F21SAASBEBBAXXX000005000000002}{4:{177:0609181712}
{451:0}{311:ACK}{108:REF-1-0609181711}}</PseudoAckNack>
        </AckNack>
        </Saa:Text>
        </Saa:Intervention>
        <Saa:Intervention>
        <Saa:IntvCategory>TransmissionResponse</Saa:IntvCategory>
        <Saa:CreationTime>060918171242</Saa:CreationTime>
        <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
        <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
        <Saa:Text>
        <Ah:AppHdr xmlns:Ah="urn:swift:xsd:$ahV10">
        <Ah:MsgRef>ra01</Ah:MsgRef>
        <Ah:CrDate>2006-09-18T17:12:30</Ah:CrDate>
        </Ah:AppHdr>
        <Doc:Document xmlns:Doc="urn:swift:xsd:swift.cashrepv1$returnaccount"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Doc:returnaccount>
        <Doc:QryRef>
        <Doc:Ref>SCRRQ01</Doc:Ref>
        </Doc:QryRef>
        <Doc:RtrRef>
        <Doc:Ref>RS01</Doc:Ref>
        </Doc:RtrRef>
        <Doc:Accts>
        <Doc:AcctRpt>
        <Doc:AcctId>
        <Doc:DmstAcct>789DA123</Doc:DmstAcct>
        </Doc:AcctId>
        <Doc:Acct>
        <Doc:Ccy>EUR</Doc:Ccy>
        <Doc:Bal>
        <Doc:Amt>99733.03</Doc:Amt>
        <Doc:CdtDbtInd>CRDT</Doc:CdtDbtInd>
        <Doc:ValDt>
        <Doc:Dt>2006-09-18</Doc:Dt>
        </Doc:ValDt>
        <Doc:Tp>AVLB</Doc:Tp>
        </Doc:Bal>
        </Doc:Acct>
        </Doc:AcctRpt>
        </Doc:Accts>
        </Doc:returnaccount>
        </Doc:Document>
        </Saa:Text>
        </Saa:Intervention>
        </Saa:Interventions>
        </Saa:TransmissionReport>
        </Saa:Report>
        </Saa:DataPDU>

```

A.2.6.5 MQSA Examples

Introduction

The following sections show DataPDU examples for:

- **Store-and-forward**

- Message sent by an application to Alliance Access
- Transmission Report sent by Alliance Access to the application (ACK)
- Transmission Report sent by Alliance Access to the application (Nack)

This was triggered by putting an unknown tag in the message payload, causing a Message Validation error (MVal error).

- Transmission Report (ACK) including the original message
- Delivery Report sent by Alliance Access to the application
- Message sent by Alliance Access to the application

- **Real time**

- Message sent by an application to Alliance Access
- Transmission Report sent by Alliance Access to the application (including a real-time business response)

A.2.6.5.1 Store-and-forward

Message sent by an application to MQSA

```
<?xml version="1.0" encoding="utf-8"?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01">
  <Saa:Message>
    <Saa:MessageFormat>MX</Saa:MessageFormat>
    <Saa:MessageSubFormat>Input</Saa:MessageSubFormat>
    <Saa:Sender>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Sender>
    <Saa:Receiver>
      <Saa:FullName>
        <Saa:X1>SAADBEBBXXX</Saa:X1>
      </Saa:FullName>
    </Saa:Receiver>
    <Saa:MessageNature>FinancialNature</Saa:MessageNature>
    <Saa:MessageLPI>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.if.ia</Saa:Service>
          <Saa:RequestType>setr.016.001.02</Saa:RequestType>
          <Saa:NRIndicator>true</Saa:NRIndicator>
        </Saa:SWIFTNetRequestAttribute>
      </Saa:NetworkAttribute>
      <Saa:SecurityAttribute>
        <Saa:SWIFTNetSecurityAttribute>
          <Saa:SigningRequired>true</Saa:SigningRequired>
        </Saa:SWIFTNetSecurityAttribute>
      </Saa:SecurityAttribute>
    </Saa:MessageLPI>
  <Saa:MessageTPI>
```

```

<Saa:NetworkDelivNotify>true</Saa:NetworkDelivNotify>
<Saa:NetworkPriority>Normal</Saa:NetworkPriority>
</Saa:MessageTPI>
<Saa:MessageSRI>
  <Saa:UserReference>Sample-XMLv1-0609141402</Saa:UserReference>
</Saa:MessageSRI>
<Saa:MessageText>
  <AppHdr xmlns="urn:swift:xsd:$ahV10">
    <MsgRef>Sample-XMLv1-0609141402</MsgRef>
    <CrDate>2006-09-14T02:02:11.414</CrDate>
  </AppHdr>
  <Document xmlns="urn:swift:xsd:swift.if.ia$setr.016.001.02">
    <setr.016.001.02>
      <RltdRef>
        <Ref>Ref123-1</Ref>
      </RltdRef>
      <IndvOrdrDtlsRpt>
        <Sts>PACK</Sts>
        <OrdrRef>Ref123-1</OrdrRef>
      </IndvOrdrDtlsRpt>
    </setr.016.001.02>
  </Document>
</Saa:MessageText>
</Saa:Message>
</Saa:DataPDU>

```

Logical reply sent by MQSA to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:LogicalReply>
    <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv1-0609141402
    </Saa:SenderReference>
    <Saa:SuccessIndication>true</Saa:SuccessIndication>
  </Saa:LogicalReply>
</Saa:DataPDU>

```

Transmission Report sent by MQSA to the application (Ack)

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:OrigSenderReference>QU1RIFFNLkJFV1gxMjQgII00D0UgAA0B
      </Saa:OrigSenderReference>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>Other</Saa:CBTApplication>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
      <Saa:DuplEmission>false</Saa:DuplEmission>
    </Saa:ReportLPI>
    <Saa:TransmissionReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>

```

```

<Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
<Saa:Service>swift.if.ia</Saa:Service>
<Saa:RequestType>setr.016.001.02</Saa:RequestType>
<Saa:NonRepType>SvcMand</Saa:NonRepType>
<Saa:SwiftRef>SWITCH90-2006-09-19T12:38:41.25857.1220138Z</Saa:SwiftRef>
<Saa:SwiftRequestRef>SNL10391-2006-09-19T12:38:41.6596.000073Z
</Saa:SwiftRequestRef>
<Saa:CBTReference>39d39f5a-fc26-4e5d-92f8-3bb42f4352f6</Saa:CBTReference>
<Saa:SnFInputTime>0102:2006-09-19T12:30:25</Saa:SnFInputTime>
</Saa:SWIFTNetRequestAttribute>
<Saa:SWIFTNetResponseAttribute />
</Saa:NetworkAttribute>
<Saa:NetworkSessionNr>000003</Saa:NetworkSessionNr>
<Saa:NetworkSeqNr>000000001</Saa:NetworkSeqNr>
<Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
<Saa:Interventions>
<Saa:Intervention>
<Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
<Saa:CreationTime>060919143839</Saa:CreationTime>
<Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
<Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
<Saa:Text>
<AckNack>
<PseudoAckNack>{1:F21SAADBEBBAXXX000003000000001}{4:{177:0609191438}
{451:0}{311:ACK}{108:Sample-XMLv1-0609141402}</PseudoAckNack>
</AckNack>
</Saa:Text>
</Saa:Intervention>
</Saa:Interventions>
</Saa:TransmissionReport>
</Saa:Report>
</Saa:DataPDU>

```

Transmission Report sent by Alliance Access to the application (Nack)

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xs:saamxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAAIBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:OrigSenderReference>QU1RIFFNLk1YUyAgICAgIHTRLUgACIC
      </Saa:OrigSenderReference>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>Other</Saa:CBTApplication>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
      <Saa:DuplEmission>false</Saa:DuplEmission>
    </Saa:ReportLPI>
    <Saa:TransmissionReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.if.ia</Saa:Service>
          <Saa:RequestType>setr.016.001.02</Saa:RequestType>
          <Saa:CBTReference>0201e4e5-c347-4ed3-a96a-2c0eab280749</Saa:CBTReference>
        </Saa:SWIFTNetRequestAttribute>
        <Saa:SWIFTNetResponseAttribute />
      </Saa:NetworkAttribute>
    </Saa:TransmissionReport>
  </Saa:Report>
</Saa:DataPDU>

```

```

</Saa:NetworkAttribute>
<Saa:NetworkSessionNr>000001</Saa:NetworkSessionNr>
<Saa:NetworkSeqNr>000000001</Saa:NetworkSeqNr>
<Saa:NetworkDeliveryStatus>NetworkNacked</Saa:NetworkDeliveryStatus>
<Saa:Interventions>
  <Saa:Intervention>
    <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
    <Saa:CreationTime>061011153702</Saa:CreationTime>
    <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
    <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
    <Saa:Text>
      <AckNack>
        <PseudoAckNack>{1:F21SAAIBEBBAXXX000001000000001}{4:{177:0610111538}
{451:1}{405:T02}{311:NAK Sw.WFE.eMVALError}{108:Sample-XMLv1-0609141402}}
        </PseudoAckNack>
      <SwGbl:Status>
        <SwGbl:StatusAttributes>
          <SwGbl:Severity>Transient</SwGbl:Severity>
          <SwGbl:Code>Sw.Gbl.NetworkTransmissionError</SwGbl:Code>
          <SwGbl:Parameter>3979</SwGbl:Parameter>
          <SwGbl:Parameter>message validation failed with error</
SwGbl:Parameter>
          <SwGbl:Text>Network Transmission Error</SwGbl:Text>
          <SwGbl:Details>
            <SwGbl:Code>Sw.WFE.eMVALError</SwGbl:Code>
            <SwGbl:Text>MVAL component error., message validation failed with
error</SwGbl:Text>
          </SwGbl:Details>
          <SwGbl:Details>
            <SwGbl:Code>Sw.WFE.ExecuteRequestFail</SwGbl:Code>
            <SwGbl:Text>Execute Request failed in WFE , MVAL</SwGbl:Text>
          </SwGbl:Details>
          <SwGbl:Details>
            <SwGbl:Code>Sw.WFE.ExecuteRequestFail</SwGbl:Code>
            <SwGbl:Text>Execute Request failed in WFE</SwGbl:Text>
          </SwGbl:Details>
        </SwGbl:StatusAttributes>
        <SwGbl:StatusAttributes>
          <SwGbl:Severity>Fatal</SwGbl:Severity>
          <SwGbl:Code>Sw.MVAL.SyntaxException</SwGbl:Code>
        <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.016.001.02[1]/
IndvOrdrDtlsRpt1[1]</SwGbl:Parameter>
          <SwGbl:Text>unexpected content "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}IndvOrdrDtlsRpt1"; expected "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}MstrRef" or "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}IndvOrdrDtlsRpt" or "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}OrdrDtlsRpt" or "{urn:swift:xsd:swift.if.ia$setr.
016.001.02}RltdRef"</SwGbl:Text>
          </SwGbl:StatusAttributes>
        <SwGbl:StatusAttributes>
          <SwGbl:Severity>Fatal</SwGbl:Severity>
          <SwGbl:Code>Sw.MVAL.SyntaxException</SwGbl:Code>
          <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]/IndvOrdrDtlsRpt1[1]</SwGbl:Parameter>
          <SwGbl:Text>no declaration for element "{urn:swift:xsd:swift.if.ia
$setr.016.001.02}IndvOrdrDtlsRpt1"</SwGbl:Text>
          </SwGbl:StatusAttributes>
        <SwGbl:StatusAttributes>
          <SwGbl:Severity>Fatal</SwGbl:Severity>
          <SwGbl:Code>Sw.MVAL.SyntaxException</SwGbl:Code>
          <SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]/IndvOrdrDtlsRpt1[1]/Sts[1]</SwGbl:Parameter>
          <SwGbl:Text>no declaration for element "{urn:swift:xsd:swift.if.ia
$setr.016.001.02}Sts"</SwGbl:Text>
          </SwGbl:StatusAttributes>
        <SwGbl:StatusAttributes>
          <SwGbl:Severity>Fatal</SwGbl:Severity>

```

```

<SwGbl:Code>Sw.MVAL.SyntaxError</SwGbl:Code>
<SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.
016.001.02[1]/IndvOrdrDtlsRpt1[1]/OrdrRef[1]</SwGbl:Parameter>
<SwGbl:Text>no declaration for element "{urn:swift:xsd:swift.if.ia
$setr.016.001.02}OrdrRef"</SwGbl:Text>
</SwGbl:StatusAttributes>
<SwGbl:StatusAttributes>
<SwGbl:Severity>Fatal</SwGbl:Severity>
<SwGbl:Code>Sw.MVAL.SyntaxError</SwGbl:Code>
<SwGbl:Parameter>SwInt:RequestPayload//Document[1]/setr.016.001.02[1]
</SwGbl:Parameter>
<SwGbl:Text>unexpected end of content</SwGbl:Text>
</SwGbl:StatusAttributes>
</SwGbl:Status>
</AckNack>
</Saa:Text>
</Saa:Intervention>
</Saa:Interventions>
</Saa:TransmissionReport>
</Saa:Report>
</Saa:DataPDU>

```

Transmission Report (Ack) including the original message

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>Full</Saa:OrigMessageFields>
    <Saa:OrigMessage>
      <Saa:MessageFormat>MX</Saa:MessageFormat>
      <Saa:MessageSubFormat>Input</Saa:MessageSubFormat>
    <Saa:Sender>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Sender>
    <Saa:Receiver>
      <Saa:FullName>
        <Saa:X1>SAADBEBBXXX</Saa:X1>
      </Saa:FullName>
    </Saa:Receiver>
    <Saa:LiveMessage>true</Saa:LiveMessage>
    <Saa:MessageNature>FinancialNature</Saa:MessageNature>
    <Saa:MessageLPI>
      <Saa:OriginalMessage>false</Saa:OriginalMessage>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.if.ia</Saa:Service>
          <Saa:RequestType>setr.016.001.02</Saa:RequestType>
          <Saa:NonRepType>SvcMand</Saa:NonRepType>
          <Saa:SwiftRef>SWITCH90-2006-10-18T09:13:49.15784.012942Z</Saa:SwiftRef>
          <Saa:SwiftRequestRef>SNL10391-2006-10-18T09:13:48.3040.001280Z
        </Saa:SwiftRequestRef>
        <Saa:CBTReference>0aad3ea0-2d15-4d2d-8ce5-e6dfe47cdb4c
      </Saa:CBTReference>
      <Saa:SnFInputTime>0102:2006-10-18T09:05:21</Saa:SnFInputTime>
    </Saa:SWIFTNetRequestAttribute>
    <Saa:SWIFTNetResponseAttribute />
  </Saa:NetworkAttribute>
  <Saa:SecurityAttribute>

```

```

<Saa:SWIFTNetSecurityAttribute>
  <Saa:SignerDN>cn=rma2,o=saadbebb,o=swift</Saa:SignerDN>
</Saa:SWIFTNetSecurityAttribute>
</Saa:SecurityAttribute>
<Saa:MessageOrigin>
  <Saa:CBTApplication>Other</Saa:CBTApplication>
</Saa:MessageOrigin>
<Saa:CBTRoutingInfo>SMQS_To_MQSeries</Saa:CBTRoutingInfo>
<Saa:DuplEmission>false</Saa:DuplEmission>
</Saa:MessageLPI>
<Saa:MessageTPI>
  <Saa:Network>SwiftNetNetwork</Saa:Network>
  <Saa:NetworkPriority>Normal</Saa:NetworkPriority>
  <Saa:NetworkSessionNr>000003</Saa:NetworkSessionNr>
  <Saa:NetworkSeqNr>000000001</Saa:NetworkSeqNr>
</Saa:MessageTPI>
<Saa:MessageSRI>
  <Saa:UserReference>Sample-XMLv1-0609141402</Saa:UserReference>
</Saa:MessageSRI>
<Saa:MessageText>
  <AppHdr xmlns="urn:swift:xsd:$ahV10">
    <MsgRef>Sample-XMLv1-0609141402</MsgRef>
    <CrDate>2006-09-14T02:02:11.414</CrDate>
  </AppHdr>
  <Document xmlns="urn:swift:xsd:swift.if.ia$setr.016.001.02">
    <setr.016.001.02>
      <RltdRef>
        <Ref>Ref123-1</Ref>
      </RltdRef>
      <IndvOrdrDtlsRpt>
        <Sts>PACK</Sts>
        <OrdrRef>Ref123-1</OrdrRef>
      </IndvOrdrDtlsRpt>
    </setr.016.001.02>
  </Document>
</Saa:MessageText>
</Saa:OrigMessage>
<Saa:ReportLPI>
<Saa:OrigSenderReference>QU1RIFFNLk1YUyAgICAgII7oNUUgAF8E
</Saa:OrigSenderReference>
<Saa:MessageOrigin>
  <Saa:CBTApplication>Other</Saa:CBTApplication>
</Saa:MessageOrigin>
<Saa:Modified>false</Saa:Modified>
<Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
<Saa:DuplEmission>false</Saa:DuplEmission>
</Saa:ReportLPI>
<Saa:TransmissionReport>
  <Saa:Network>SwiftNetNetwork</Saa:Network>
<Saa:NetworkAttribute>
  <Saa:SWIFTNetRequestAttribute>
    <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
    <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
    <Saa:Service>swift.if.ia</Saa:Service>
    <Saa:RequestType>setr.016.001.02</Saa:RequestType>
    <Saa:NonRepType>SvcMand</Saa:NonRepType>
    <Saa:SwiftRef>SWITCH90-2006-10-18T09:13:49.15784.012942Z</Saa:SwiftRef>
    <Saa:SwiftRequestRef>SNL10391-2006-10-18T09:13:48.3040.001280Z
  </Saa:SwiftRequestRef>
  <Saa:CBTReference>0aad3ea0-2d15-4d2d-8ce5-e6df4e47cdb4c</Saa:CBTReference>
  <Saa:SnFInputTime>0102:2006-10-18T09:05:21</Saa:SnFInputTime>
</Saa:SWIFTNetRequestAttribute>
  <Saa:SWIFTNetResponseAttribute />
</Saa:NetworkAttribute>
<Saa:NetworkSessionNr>000003</Saa:NetworkSessionNr>
<Saa:NetworkSeqNr>000000001</Saa:NetworkSeqNr>
<Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>

```

```

<Saa:Interventions>
  <Saa:Intervention>
    <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
    <Saa:CreationTime>061018111349</Saa:CreationTime>
    <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
    <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
    <Saa:Text>
      <AckNack>
        <PseudoAckNack>{1:F21SAADBEBBAXXX000003000000001}{4:{177:0610181113}
{451:0}{311:ACK}{108:Sample-XMLv1-0609141402}}</PseudoAckNack>
      </AckNack>
    </Saa:Text>
  </Saa:Intervention>
</Saa:Interventions>
</Saa:TransmissionReport>
</Saa:Report>
</Saa:DataPDU>

```

Delivery Report sent by MQSA to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAADBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:OrigSenderReference>QU1R1FFNLkJFV1gxMjQgII00D0UgAA0B
      </Saa:OrigSenderReference>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>Other</Saa:CBTApplication>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:ReportingApplication>Traffic Recon</Saa:ReportingApplication>
      <Saa:DuplEmission>false</Saa:DuplEmission>
    </Saa:ReportLPI>
    <Saa:DeliveryReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.if.ia</Saa:Service>
          <Saa:RequestType>setr.016.001.02</Saa:RequestType>
          <Saa:NonRepType>SvcMand</Saa:NonRepType>
          <Saa:SwiftRef>SWITCH90-2006-09-19T12:38:41.25857.1220138Z</Saa:SwiftRef>
          <Saa:SwiftRequestRef>SNL10391-2006-09-19T12:38:41.6596.000073Z
        </Saa:SwiftRequestRef>
          <Saa:CBTReference>39d39f5a-fc26-4e5d-92f8-3bb42f4352f6</Saa:CBTReference>
          <Saa:SnFInputTime>0102:2006-09-19T12:30:25</Saa:SnFInputTime>
        </Saa:SWIFTNetRequestAttribute>
        <Saa:SWIFTNetResponseAttribute />
      </Saa:NetworkAttribute>
      <Saa:NetworkSessionNr>000003</Saa:NetworkSessionNr>
      <Saa:NetworkSeqNr>000000001</Saa:NetworkSeqNr>
    <Saa:ReceiverDeliveryStatus>RcvDelivered</Saa:ReceiverDeliveryStatus>
    <Saa:Interventions>
      <Saa:Intervention>
        <Saa:IntvCategory>DeliveryReport</Saa:IntvCategory>
        <Saa:CreationTime>060919143932</Saa:CreationTime>
        <Saa:ApplicationOrigin>TRS</Saa:ApplicationOrigin>
        <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
      </Saa:Intervention>
    </Saa:Interventions>
  </Saa:DeliveryReport>
</Saa:DataPDU>

```

```

<Saa:Text>
  <Sw:NotifySnFRequestHandle>
    <Sw:SnFRef>SWITCH90-2006-09-19T12:38:41.25857.1220138Z</Sw:SnFRef>
    <Sw:SnFRefType>InterAct</Sw:SnFRefType>
    <Sw:AcceptStatus>Accepted</Sw:AcceptStatus>
    <Sw:AckSwiftTime>2006-09-19T12:39:34Z</Sw:AckSwiftTime>
    <Sw:AckInfo>Acked</Sw:AckInfo>
  </Sw:NotifySnFRequestHandle>
</Saa:Text>
</Saa:Intervention>
</Saa:Interventions>
</Saa:DeliveryReport>
</Saa:Report>
</Saa:DataPDU>

```

Message sent by MQSA to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>OSAADBEBBXXX016Sample-XMLv1-0609141402
  </Saa:SenderReference>
  <Saa:Message>
    <Saa:MessageFormat>MX</Saa:MessageFormat>
    <Saa:MessageSubFormat>Output</Saa:MessageSubFormat>
    <Saa:Sender>
      <Saa:X1>SAADBEBBXXX</Saa:X1>
    </Saa:Sender>
    <Saa:Receiver>
      <Saa:FullName>
        <Saa:X1>SAADBEBBXXX</Saa:X1>
      </Saa:FullName>
    </Saa:Receiver>
    <Saa:LiveMessage>true</Saa:LiveMessage>
    <Saa:MessageNature>FinancialNature</Saa:MessageNature>
    <Saa:MessageLPI>
      <Saa:OriginalMessage>true</Saa:OriginalMessage>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=saadbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>o=saadbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.if.ia</Saa:Service>
          <Saa:RequestType>setr.016.001.02</Saa:RequestType>
          <Saa:NonRepType>SvcMand</Saa:NonRepType>
        <Saa:SwiftRef>SWITCH90-2006-09-19T12:38:41.25857.1220138Z</Saa:SwiftRef>
        <Saa:SwiftRequestRef>SNL10391-2006-09-19T12:38:41.6596.000073Z
      </Saa:SwiftRequestRef>
      <Saa:CBTReference>79793722-19ac-4d6d-ad7e-a755349285ed</Saa:CBTReference>
      <Saa:SNLEndPoint>sni_bewx124</Saa:SNLEndPoint>
      <Saa:SnFQueueName>saadbebb_ifia</Saa:SnFQueueName>
      <Saa:ValidationDescriptor>
        <SwInt:ValResult>Success</SwInt:ValResult>
      </Saa:ValidationDescriptor>
      <Saa:AuthResult>Success</Saa:AuthResult>
      <Saa:AuthValue>
        <SwSec: CryptoInternal>
          <SwSec:CipherKey>UEVNRkBQcm9jLVR5cGU6IDQsTULDLU90TFkNCkNvbRlbnQtRG9tYWluOibSR
          kM4MjINCKvudHJ1c3RGaWx1LVZ1cnNpb246IDIuMA0KT3JpZ2luYXRvcilETjogY249cm1hMixvPZN
          hYWRizWJiLG89c3dpZnQNCk9yaWctU046IDExNDC3ODU1NjYNCk1JQy1JbmZvOiBTSEExLCBSU0EsD
          OogdUlTY2tYSkV1akFUQSt5bWFnaWJRU1I3b3B5Q3JheGV0L0ExZ2OzRy9mQkdyT0JZZmc1LzZ1bzY
          4S1hjdjFyRg0KIDQ5aHgxWWRWeDlyME1LMHZld2xHRnBVRUErdzhUcktzMG95QTFDbXd3am5iR1I5T
          U92aWtGK01hNTQ2N3dXSHMNCiAxZU50dk5zY0tNVHYYb2grU0RrcW9xS1hUy8zQXpNNFphL2NCR25
          PYUN2MEFocXFaQUFTazFneTE3c3dZMURLDQogNzhYYi9tdnMvRVZBT1o0RnY4MUhzWWhnM21wNHRUO
          EV1YnVNdFpvZDMycVkwemFLVVMrcUtGL2VwVjRQM2syMA0KIGMvaWJJc3ZKc1pCTTlQbzAyT1JyNxB
        </SwSec: CryptoInternal>
      </Saa:AuthValue>
    </Saa:NetworkAttribute>
  </Saa:MessageLPI>
  <Saa:CBTReference>79793722-19ac-4d6d-ad7e-a755349285ed</Saa:CBTReference>
  <Saa:SNLEndPoint>sni_bewx124</Saa:SNLEndPoint>
  <Saa:SnFQueueName>saadbebb_ifia</Saa:SnFQueueName>
  <Saa:ValidationDescriptor>
    <SwInt:ValResult>Success</SwInt:ValResult>
  </Saa:ValidationDescriptor>
  <Saa:AuthResult>Success</Saa:AuthResult>
  <Saa:AuthValue>
    <SwSec: CryptoInternal>
      <SwSec:CipherKey>UEVNRkBQcm9jLVR5cGU6IDQsTULDLU90TFkNCkNvbRlbnQtRG9tYWluOibSR
      kM4MjINCKvudHJ1c3RGaWx1LVZ1cnNpb246IDIuMA0KT3JpZ2luYXRvcilETjogY249cm1hMixvPZN
      hYWRizWJiLG89c3dpZnQNCk9yaWctU046IDExNDC3ODU1NjYNCk1JQy1JbmZvOiBTSEExLCBSU0EsD
      OogdUlTY2tYSkV1akFUQSt5bWFnaWJRU1I3b3B5Q3JheGV0L0ExZ2OzRy9mQkdyT0JZZmc1LzZ1bzY
      4S1hjdjFyRg0KIDQ5aHgxWWRWeDlyME1LMHZld2xHRnBVRUErdzhUcktzMG95QTFDbXd3am5iR1I5T
      U92aWtGK01hNTQ2N3dXSHMNCiAxZU50dk5zY0tNVHYYb2grU0RrcW9xS1hUy8zQXpNNFphL2NCR25
      PYUN2MEFocXFaQUFTazFneTE3c3dZMURLDQogNzhYYi9tdnMvRVZBT1o0RnY4MUhzWWhnM21wNHRUO
      EV1YnVNdFpvZDMycVkwemFLVVMrcUtGL2VwVjRQM2syMA0KIGMvaWJJc3ZKc1pCTTlQbzAyT1JyNxB
    </SwSec: CryptoInternal>
  </Saa:AuthValue>
</Saa:NetworkAttribute>
</Saa:MessageLPI>
</Saa:Message>
</Saa:SenderReference>
</Saa:DataPDU>

```

```

s1p1elVsS2tYcWhyZ1J6V0g1UEJoNEDjd0hqa0JFTTQ4dXVOQS96bUgNCiBCRnZSc0Q1ZVBuY0lsN
nM2ZHgwOXZnPT0NCg==</SwSec:CipherKey>
  <SwSec:CryptoProtocol>4.0:3.0</SwSec:CryptoProtocol>
</SwSec:CryptoInternal>
<SwSec:CryptoDescriptor>
  <SwSec:MemberRef>RequestPayload</SwSec:MemberRef>
  <SwSec:MemberRef>RequestHeader</SwSec:MemberRef>
  <SwSec:MemberRef>RequestDescriptor.SwiftRequestRef</SwSec:MemberRef>
  <SwSec:SignDN>cn=rma2,o=saadbebb,o=swift</SwSec:SignDN>
  <SwSec:CertPolicyId>1.3.21.6.2</SwSec:CertPolicyId>
</SwSec:CryptoDescriptor>
</Saa:AuthValue>
</Saa:SWIFTNetRequestAttribute>
<Saa:SWIFTNetResponseAttribute />
</Saa:NetworkAttribute>
<Saa:SecurityAttribute>
  <Saa:SWIFTNetSecurityAttribute>
    <Saa:SignerDN>cn=rma2,o=saadbebb,o=swift</Saa:SignerDN>
  </Saa:SWIFTNetSecurityAttribute>
</Saa:SecurityAttribute>
<Saa:MessageOrigin>
  <Saa:CBTApplication>SwiftnetInterface</Saa:CBTApplication>
</Saa:MessageOrigin>
<Saa:CBTRoutingInfo>SMQS_To_MQSeries</Saa:CBTRoutingInfo>
<Saa:DuplEmission>false</Saa:DuplEmission>
</Saa:MessageLPI>
<Saa:MessageTPI>
  <Saa:Network>SwiftNetNetwork</Saa:Network>
  <Saa:NetworkPriority>Normal</Saa:NetworkPriority>
  <Saa:NetworkSessionNr>003389</Saa:NetworkSessionNr>
  <Saa:NetworkSeqNr>000001560</Saa:NetworkSeqNr>
  <Saa:DuplCreation>PDE</Saa:DuplCreation>
</Saa:MessageTPI>
<Saa:MessageSRI>
  <Saa:UserReference>Sample-XMLv1-0609141402</Saa:UserReference>
</Saa:MessageSRI>
<Saa:MessageText>
  <AppHdr xmlns="urn:swift:xsd:$ahV10">
    <MsgRef>Sample-XMLv1-0609141402</MsgRef>
    <CrDate>2006-09-14T02:02:11.414</CrDate>
  </AppHdr>
  <Document xmlns="urn:swift:xsd:swift.if.ia$setr.016.001.02">
    <setr.016.001.02>
      <RltdRef>
        <Ref>Ref123-1</Ref>
      </RltdRef>
      <IndvOrdrDtlsRpt>
        <Sts>PACK</Sts>
        <OrdrRef>Ref123-1</OrdrRef>
      </IndvOrdrDtlsRpt>
    </setr.016.001.02>
  </Document>
</Saa:MessageText>
</Saa:Message>
</Saa:DataPDU>

```

A.2.6.5.2 Real time

Message sent by an application to MQSA

```

<?xml version="1.0" encoding="utf-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01">
  <Saa:Message>
    <Saa:MessageFormat>MX</Saa:MessageFormat>
    <Saa:MessageSubFormat>Input</Saa:MessageSubFormat>
    <Saa:Sender>
      <Saa:X1>SAASBEBBXXX</Saa:X1>

```

```

</Saa:Sender>
<Saa:Receiver>
<Saa:FullName>
  <Saa:X1>SAATBEBBXXX</Saa:X1>
</Saa:FullName>
</Saa:Receiver>
<Saa:MessageNature>FinancialNature</Saa:MessageNature>
<Saa:MessageLPI>
<Saa:NetworkAttribute>
<Saa:SWIFTNetRequestAttribute>
  <Saa:RequestorDN>o=saasbebb,o=swift</Saa:RequestorDN>
  <Saa:ResponderDN>cn=beso,cn=tg229,o=saatbebb,o=swift</Saa:ResponderDN>
  <Saa:Service>swift.cashrepv1</Saa:Service>
  <Saa:RequestType>getaccount</Saa:RequestType>
</Saa:SWIFTNetRequestAttribute>
</Saa:NetworkAttribute>
</Saa:MessageLPI>
<Saa:MessageTPI>
  <Saa:NetworkPriority>Normal</Saa:NetworkPriority>
</Saa:MessageTPI>
<Saa:MessageSRI>
  <Saa:UserReference>REF-1-0609181711</Saa:UserReference>
</Saa:MessageSRI>
<Saa:MessageText>
<Ah:AppHdr xmlns:Ah="urn:swift:xsd:$ahV10">
  <Ah:MsgRef>SCRRQ01</Ah:MsgRef>
  <Ah:CrDate>2006-09-18T17:11:28.359</Ah:CrDate>
</Ah:AppHdr>
<Doc:Document xmlns:Doc="urn:swift:xsd:swift.cashrepv1$getaccount"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Doc:getaccount>
    <Doc:NstrAcctSchCrit>
      <Doc:AcctId>
        <Doc:DmstAcct>789DA123</Doc:DmstAcct>
      </Doc:AcctId>
      <Doc:BalTp>AVLB</Doc:BalTp>
    </Doc:NstrAcctSchCrit>
    <Doc:QryPrcg>
      <Doc:QryRef>
        <Doc:Ref>SCRRQ01</Doc:Ref>
      </Doc:QryRef>
    </Doc:QryPrcg>
  </Doc:getaccount>
</Doc:Document>
</Saa:MessageText>
</Saa:Message>
</Saa:DataPDU>

```

Logical reply sent by MQSA to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:LogicalReply>
    <Saa:SenderReference>ISAATBEBBXXXMX REF-1-0609181711</Saa:SenderReference>
    <Saa:SuccessIndication>true</Saa:SuccessIndication>
  </Saa:LogicalReply>
</Saa:DataPDU>

```

Transmission Report sent by MQSA to the application

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:xsd:saa.mxs.01"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:SenderReference>ISAATBEBBXXMX REF-1-0609181711</Saa:SenderReference>
  <Saa:Report>
    <Saa:Addressee>
      <Saa:X1>SAATBEBBXXX</Saa:X1>
    </Saa:Addressee>
    <Saa:OrigMessageFields>NoOriginal</Saa:OrigMessageFields>
    <Saa:ReportLPI>
      <Saa:OrigSenderReference>QU1R1FFNLkJFV1gxMjQgIH1WEUUGAYC
      </Saa:OrigSenderReference>
      <Saa:MessageOrigin>
        <Saa:CBTApplication>Other</Saa:CBTApplication>
      </Saa:MessageOrigin>
      <Saa:Modified>false</Saa:Modified>
      <Saa:ReportingApplication>SWIFTNet Interface</Saa:ReportingApplication>
      <Saa:DuplEmission>false</Saa:DuplEmission>
    </Saa:ReportLPI>
    <Saa:TransmissionReport>
      <Saa:Network>SwiftNetNetwork</Saa:Network>
      <Saa:NetworkAttribute>
        <Saa:SWIFTNetRequestAttribute>
          <Saa:RequestorDN>o=sasbebb,o=swift</Saa:RequestorDN>
          <Saa:ResponderDN>cn=beso,cn=tg229,o=saatbebb,o=swift</Saa:ResponderDN>
          <Saa:Service>swift.cashrepv1</Saa:Service>
          <Saa:RequestType>getaccount</Saa:RequestType>
          <Saa:SwiftRef>SWITCH90-2006-09-20T15:03:30.22745.2556517Z</Saa:SwiftRef>
          <Saa:SwiftRequestRef>SNL00229-2006-09-20T15:03:29.7900.000004Z
          </Saa:SwiftRequestRef>
          <Saa:CBTReference>9c2392bf-63d9-4a1c-bd27-a7c9d0c1b1b1</Saa:CBTReference>
        </Saa:SWIFTNetRequestAttribute>
        <Saa:SWIFTNetResponseAttribute>
          <Saa:ResponderDN>cn=beso,cn=tg229,o=saatbebb,o=swift</Saa:ResponderDN>
          <Saa:SwiftResponseRef>SNL00229-2006-09-20T15:03:31.5004.000005Z
          </Saa:SwiftResponseRef>
          <Saa:AuthResult>Success</Saa:AuthResult>
          <Saa:AuthValue>
            <SwSec: CryptoInternal>
              <SwSec: CipherKey>UEVNRkBQcm9jLVR5cGU6IDQsTUlDLU90TFkNckNvbnR1bnQtRG9tYWluOiBSR
kM4MjINCKvudHJ1c3RGaWx1LVz1cnNpb246IDIuMA0KT3JpZ2luYXRvcileTjogY249cm1hNCxvPXB
hYXRiZWJ1LG89c3dpZnQNCk9yaWctU046IDEExNDE5Mzg1MjINCK1JQy1JbmZvOiBTSEExLCBSU0EsD
QogZEF4b3VROFRFbldNNW03T2V0czZDdC8vTjFzOU9tU1o0cTFPdWI4ZnppT2xIQS95RDJhc2h5L21
KU2V0cjbUy0KIHpJUNv5M09Lcz1TUlxt2p3MnVKSEZvb0hKYmtQTUdPOGTIZG91clo4K0tVeGFHM
E5QSwtCTVJKY1Z0alRVdGgNCiBvCe1TU1SE5wcGtuN09VY2FUenFMT1ZQSnZ4Z2NrRut4d25CNzd
5THRuay83Y1RMVFhRR3FOVks2N0ROVs9rDQogcHZWz1UwWGxxNVVQWGoxtMTVvWndxUS9HVzVHcGMxb
1hBYXpWdVJMTTFpa054UHRXejg0Sm9iT0FTV1R1VjFQYw0KIG9nNmRmUkRySGtSZWt2elh1V0pzazR
sQjFiWGYrOVpCWTFOaWNIUCtiaTd2akV5bDZ5Mk1CalDWWXVGvzJ4TwSNcibjMTEzam5EQjhad255T
2kzMU5jV3ZBPT0NCg==</SwSec: CipherKey>
            <SwSec: CryptoProtocol>4.0:3.0</SwSec: CryptoProtocol>
          </SwSec: CryptoInternal>
          <SwSec: CryptoDescriptor>
            <SwSec: MemberRef>ResponsePayload</SwSec: MemberRef>
            <SwSec: MemberRef>ResponseHeader</SwSec: MemberRef>
            <SwSec: MemberRef>ResponseDescriptor.SwiftResponseRef</SwSec: MemberRef>
            <SwSec: SignDN>cn=rma4,o=saatbebb,o=swift</SwSec: SignDN>
            <SwSec: CertPolicyId>1.3.21.6.2</SwSec: CertPolicyId>
          </SwSec: CryptoDescriptor>
        </Saa:AuthValue>
      </Saa:SWIFTNetResponseAttribute>
    </Saa:NetworkAttribute>
    <Saa:NetworkSessionNr>000003</Saa:NetworkSessionNr>
    <Saa:NetworkSeqNr>000000002</Saa:NetworkSeqNr>
    <Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
  </Saa:Report>
</Saa:DataPDU>

```

```

<Saa:Interventions>
  <Saa:Intervention>
    <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
    <Saa:CreationTime>060920170319</Saa:CreationTime>
    <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
    <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
    <Saa:Text>
      <AckNack>
        <PseudoAckNack>{1:F21SAASBEBBAXXX000003000000002}{4:{177:0609201703}
{451:0}{311:ACK}{108:REF-1-0609181711}}</PseudoAckNack>
      </AckNack>
    </Saa:Text>
  </Saa:Intervention>
  <Saa:Intervention>
    <Saa:IntvCategory>TransmissionResponse</Saa:IntvCategory>
    <Saa:CreationTime>060920170326</Saa:CreationTime>
    <Saa:ApplicationOrigin>SWIFTNet Interface</Saa:ApplicationOrigin>
    <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
    <Saa:Text>
      <Ah:AppHdr xmlns:Ah="urn:swift:xsd:$ahV10">
        <Ah:MsgRef>ra01</Ah:MsgRef>
        <Ah:CrDate>2006-09-18T17:12:30</Ah:CrDate>
      </Ah:AppHdr>
      <Doc:Document xmlns:Doc="urn:swift:xsd:swift.cashrepv1$returnaccount"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Doc:returnaccount>
          <Doc:QryRef>
            <Doc:Ref>SCRRQ01</Doc:Ref>
          </Doc:QryRef>
          <Doc:RtrRef>
            <Doc:Ref>RS01</Doc:Ref>
          </Doc:RtrRef>
          <Doc:Accts>
            <Doc:AcctRpt>
              <Doc:AcctId>
                <Doc:DmstAcct>789DA123</Doc:DmstAcct>
              </Doc:AcctId>
              <Doc:Acct>
                <Doc:Ccy>EUR</Doc:Ccy>
                <Doc:Bal>
                  <Doc:Amt>99733.03</Doc:Amt>
                  <Doc:CdtDbtInd>CRDT</Doc:CdtDbtInd>
                  <Doc:ValDt>
                    <Doc:Dt>2006-09-18</Doc:Dt>
                  </Doc:ValDt>
                  <Doc:Tp>AVLB</Doc:Tp>
                </Doc:Bal>
              </Doc:Acct>
            </Doc:AcctRpt>
            </Doc:Accts>
          </Doc:returnaccount>
        </Doc:Document>
      </Saa:Text>
    </Saa:Intervention>
  </Saa:Interventions>
</Saa:TransmissionReport>
</Saa:Report>
</Saa:DataPDU>

```

A.2.7 XML Version 2 (XMLv2)

Introduction

The following sections describe the format of the Protocol Data Units (PDUs) exchanged between Alliance Access and the application.

Examples of Message Formats

You can find examples of the XML version 2 message format in the following directory:

- Windows: %alliance%\SWIFT\SERVER\MXS\batch_examples
- UNIX or Linux: \$ALLIANCE/MXS/batch_examples

A.2.7.1 New Format Changes

A.2.7.1.1 Versioning

Summary

Since Alliance Access 6.2, a new approach to the versioning of the XML format is used for message exchange with back-office applications. In addition to the existing versioning of an XML schema, several revisions of the same version can exist.

Taking into account the consequent revisions, the existing XMLv2 evolves as 2.0.1, 2.0.2, and so on.

A.2.7.1.2 Schema Definition

Changes in the definition of the XMLv2 schema for revisions greater than zero

- The version element is added to the schema definition for information purposes (the element is not used for format validation).

Specifically, xs:schema:version element is added, indicating the revision of the schema.

For example, for revision 2.0.1, the schema definition is (changes are in bold):

```
<xs:schema version="2.0.1" elementFormDefault="qualified"
  xmlns="urn:swift:saa:xsd:saa.2.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:swift:saa:xsd:saa.2.0">
```

- The DataPDU:Revision element is added to the definition of DataPDU type.

The presence of the Revision element is mandatory for the revisions greater than zero. Absence of the Revision element indicates that the document has revision 0 ("zero").

For example, for revision 2.0.1 the definition of the DataPDU type is as follows (changes are in bold):

```
<xs:complexType name="DataPDU">
  <xs:sequence>
    <xs:element name="Revision" type="SWString" fixed="2.0.1"/>
    <xs:element name="Header" type="Header" />
    <xs:element name="Body" type="SwAny" minOccurs="0" />
  </xs:sequence>
</xs:complexType>
```

The schema file name contains the revision number, if applicable.

A.2.7.1.3 Changes in Revision 2.0.1

Overview

This section provides a brief overview of the changes to the data element in revision 2.0.1.

Changes to the data element Message

The format sub-element of Message can accept the value "AnyXML".

AnyXML format messages can be sent and received by back-office applications, providing they are well-formed XML documents. No special licence option is required to process messages using this format.

RoutingCode available for all instances

The RoutingCode element in the InterfaceInfo data element is available for all types of message instances.

AddressInfo can contain X as Sender

The BIC12 in the AddressInfo data element can contain the value "X" as the 9th character of the logical terminal Terminal Code.

SAAInfo added to data elements

A data element, SAAInfo, of the type SAAInfo has been added to the following data elements:

- Message
- DeliveryNotification
- HistoryReport
- TransmissionReport
- DeliveryReport
- MessageStatus

New Auxiliary type SAAInfo

An auxiliary type, SAAInfo, has been added for use with the MQ Host Adapter:

Element	Description	Type	From	To
InstanceName	The instance name of the Alliance Access that sends the message to a back-office application. It is followed by "/" and the exit point where the message was processed, or the queue to which the message was routed. From: the value is ignored	String	O	M
UserName	The OS user that runs the Alliance Access server. From: the value is ignored	String	O	M
Unit	The Alliance Access Unit to which the message belongs. From: the value is ignored	String	O	M

Changes to data sub-element of InterfaceInfo

Element	Description	Type	From	To
RoutingCode	Information which is used for routing in Alliance Access. The code entered here is visible through the routing keyword 'Routing_code' (see "RoutingInstruction").	String	O	O

Element	Description	Type	From	To
	The limitation that only an Original instance or Copy instance can have this field has been removed. Any instance type can contain this element.			

The limitation that only Original or Copy message instances can have the RoutingCode field present is removed. The field can be optionally present for any type of message instance.

Changes to sub-element SWIFTNetNetworkInfo

Request type has been added for TARGET2 standard support:

Changes to sub-element SWIFTNetNetworkInfo

Element	Description	Type	From	To
RequestType	Contains the Request Type of the message. If the request type is not present, then for AnyXML messages, the request type is assumed to be the same as the message identifier. For MX messages, it corresponds to the namespace URI of the XML document in the body of the message.	String	O	O

A.2.7.1.4 Changes in Revision 2.0.2

Overview

This section provides a brief overview of the changes to the data elements in revision 2.0.2.

Changes to the data element Message

The sub-element FileLogicalName has been added to support FileAct.

The Format element can now have the value "File".

The length of the SenderReference element is increased from 50 to 70 to accommodate the UMID + suffix.

In the NetworkInfo element, the IsNotificationRequested sub-element can also be used for Real-Time FileAct.

In the InterfaceInfo element, the ProductInfo sub-element has been added to support the ProductList element.

In the SWIFTNetSecurityInfo element, the FileDigestAlgorithm and FileDigestValue sub-elements have been added to support FileAct.

In the SWIFTNetNetworkInfo element:

- The SnFDeliveryTime sub-element has been added
- To support the payload attributes, the sub-elements PayloadAttributes and ResponsePayloadAttributes have been added
- To support FileAct, the following sub-elements have been added: CreationTime, IsCopyRequested, IsAuthNotificationRequested, CopyInfo, TransferRef, SnFTransferRef, TransferDescription, TransferInfo, FileDescription, FileInfo, HeaderInfo, NotificationResponderDN, NotificationRequestType, FileStartTime, FileEndTime.
- To support the Overdue Warning feature of SWIFTNet 6.3, the OverdueWarningTime and OverdueWarningDelay sub-elements have been added.

Changes to the data element SessionStatus

The sub-elements AcceptedFromMessagePartner, RejectedFromMessagePartner, AcceptedToMessagePartner, and RejectedToMessagePartner have been added, in relation to the introduction of the SOAP host adapter.

The Format element can now have the value "File".

The length of the Sender element is increased from 50 to 70 to accommodate the UMID + suffix.

New Auxiliary type PayloadAttribute

Element	Description	Type	From	To
Name	Name of the attribute associated to the payload of the SWIFTNet request, or response.	String	M	M
Value	Value of the attribute associated to the payload of the SWIFTNet request, or response.	String	M	M

New Auxiliary type PayloadAttributeList

Element	Description	Type	From	To
PayloadAttribute	The list of occurrences of the name, and value of an attribute.	PayloadAttribute [1..N]	O	O

New Auxiliary type Product

Element	Description	Type	From	To
VendorName	Name of the vendor of the back-office application.	String	O	O
ProductName	Name of the back-office application.	String	O	O
ProductVersion	Version of the back-office application.	String	O	O

New Auxiliary type ProductList

Element	Description	Type	From	To
Product	The list of occurrences of the VendorName, ProductName, and ProductVersion.	Product [0..3]	O	--

New Auxiliary type Digest

Element	Description	Type	From	To
DigestRef	Identification of a digest.	DigestRef	M	M
DigestValue	Value of a digest identified by DigestRef.	DigestValue [0..1]	O	O

New Auxiliary type DigestList

Element	Description	Type	From	To
Digest	The list of occurrences of the Digest.	Digest [1..8]	O	O

A.2.7.1.5 Changes in Revision 2.0.3

Overview

This section provides a brief overview of the changes to the data elements in revision 2.0.3.

Changes to the data element Message

In the SWIFTNetNetworkInfo element:

- The following sub-elements have been added to support the message and file distribution feature:
 - RecipientList
 - IsRecipientListPublic
 - DistributionInfo

In the FINNetworkInfo element:

- The following sub-element has been added and contains the full FIN user header:
 - FINUserHeader

The ThirdPartyList sub-element has been added to support the message and file dynamic copy feature.

New Auxiliary type RecipientList

Element	Description	Type	From	To
RecipientDN	The DN which identifies the recipient for the distribution of a message or file.	RecipientDN [1..1000]	O	O

New Auxiliary type ThirdPartyList

Element	Description	Type	From	To
ThirdPartyDN	The DN which identifies the third party for the copy of a message or file.	ThirdPartyDN [1..30]	O	O

A.2.7.1.6 Changes in Revision 2.0.4

Overview

This section provides a brief overview of the changes to the data elements in revision 2.0.4.

New field tags

Element	Description	Type	From	To
ExpiryDateTime	Used in the Message tag of XMLv2 FileAct or InterAct messages. The field applies only to message partners whose connection method is based on XMLv2. When present in a FileAct or InterAct message received from the back office, this field must contain a valid absolute date and time (expressed in UTC) in the standard date/time format used internally by Alliance Access. However, Alliance Access does not	YYYYMMDDHHMMSS	O	O

	check at reception time whether the date and time that the field contains are in the future. This information is applicable to input SWIFTNet messages only.			
RetrievallInfo	Used in the context of InterAct retrievals, this field contains the following information: <ul style="list-style-type: none"> retrieval direction (that is, whether the original message is an input message or an output message) reference of the retrieval request (either xsys.015.001.01 or an O2M request) position of the retrieved message within the batch of retrieved messages whether a message is the last message within the batch of retrieved messages 	XML fragment	O	O

A.2.7.1.7 Changes in Revision 2.0.5

Overview

This section provides a brief overview of the change to the data elements in revision 2.0.5.

New field tag

Element	Description	Type	From	To
CustomDigestValue	This new field tag supports the IPLA custom digest used by Alliance Access for duplicate check.	String	O	O

A.2.7.1.8 Changes in Revision 2.0.6

Overview

A new XML field tag supporting local authentication (LAU) data has been implemented. This tag is useful if you need to use LAU, but you have not configured your File Transfer or Websphere MQ message partners to use the XMLv2 binary prefix.

The content of this tag is described in the W3C DSig Specification.

The following W3C DSig methods are used:

Algorithm	URL
CanonicalizationMethod	http://www.w3.org/2001/10/xml-exc-c14n#
SignatureMethod	http://www.w3.org/2001/04/xmldsig-more#hmac-sha256
Transform	http://www.w3.org/2000/09/xmldsig#enveloped-signature
Transform	http://www.w3.org/2001/10/xml-exc-c14n#

Algorithm	URL
DigestMethod	http://www.w3.org/2001/04/xmlenc#sha256

New field tag

Element	Description	Type	From	To
LAU	This new field tag provides authentication information as an alternative to a message partner using an XMLv2 binary prefix. However, if both a binary prefix and this tag are present, the LAU data in both must match.	W3C Signature element	O	O

A.2.7.2 Protocol Data Units

Description

The application and Alliance Access exchange PDUs that are sequences of bytes with the following structure:

Prefix	Length	Signature	DataPDU
--------	--------	-----------	---------

- **Prefix** (1 byte): the character 0x1f.
- **Length** (6 bytes): length (in bytes) of the Signature and DataPDU fields: this length is base-10 encoded as six ASCII characters, and is left-padded with zeros, if needed.
- **Signature** (24 bytes): signature computed on the DataPDU using the HMAC-SHA256 algorithm, base64-encoded (see "Computing the Signature of a DataPDU" on page 741).

This signature authenticates the originator of the DataPDU (the application or Alliance Access) and guarantees the integrity of the DataPDU. This action is referred to as local authentication (LAU). If Alliance Access is configured to not require LAU, then the field must contain NULL characters.

- **DataPDU**: XML structure containing the information relevant for processing (message or report) encoded in UTF-8 format.

The first byte of this field must be the character, < (0x3C). A byte-order marker is not supported.

The structure of the DataPDU is described in the rest of this section.

A DataPDU field has an overall XML structure that looks like:

```
<?xml version="1.0" encoding="utf-8"?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
...
</Saa:DataPDU>
```

A DataPDU field that Alliance Access sends to the application may contain structured data that is received from SWIFTNet. Therefore, the field may contain the following additional namespace declarations:

```
xmlns:Sw="urn:swift:snl:ns.Sw"
xmlns:SwInt="urn:swift:snl:ns.SwInt".
xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
xmlns:SwSec="urn:swift:snl:ns.SwSec"
```

The signature is computed on the complete DataPDU field, that includes the string <?xml version="1.0" encoding="utf-8"?>. The XML representation must not be altered between the signature computation and the verification. The namespace includes a version number (2.0).

A batch file that is exchanged using File Transfer can contain one or more consecutive PDUs. A batch file that is exchanged using the MQ Host Adapter or the SOAP Host Adapter can have only one PDU.

A.2.7.3 Structure of the DataPDU

Introduction

This section describes the various XML elements that can be present in the DataPDU field. The description uses a table format.

The corresponding schema is located in the following directory in the Alliance Access release tree:

On Windows: **\MXS\xsd\SAA_XML_v2_0.xsd**

On UNIX or Linux: **/MXS/xsd/SAA_XML_v2_0.xsd**

The columns "From" and "To" indicate whether the element is mandatory ('M'), optional ('O'), or not applicable ('--') for the corresponding direction of a message or report exchange. The directions are defined as follows:

- "From": from the application to Alliance Access
- "To": to the application from Alliance Access.

A.2.7.3.1 DataPDU

DataPDU elements

Element	Description	Type	From	To
Revision	The revision to a version of an XML schema. Absence of the Revision element indicates that the document has revision 0 ("zero")	String	M ⁽¹⁾	M
Header	Contains all information relevant to the processing of Alliance Access .	Header	M	M
Body	Contains the message "text". Present in a DataPDU carrying either a message, a delivery notification, or a report that includes the original message. For an MX message: this element contains the Application Header (if required ⁽²⁾) and the Business Document as defined in the Solutions documentation. No encoding is	Any	M	O

Element	Description	Type	From	To
	<p>required since these structures contain XML data.</p> <p>For an MT message: this element contains the FIN block 4, base64-encoded (because this block does not contain XML data)⁽³⁾.</p>			
LAU	Provides authentication information as an alternative to a message partner using an XMLv2 binary prefix. However, if both a binary prefix and this tag are present, the LAU data in both must match.	W3C Signature element	O	O

- (1) Mandatory for revisions greater than zero.
- (2) If an Application Header is required, then the schema of the Application Header for each Standard that is part of a Solution is listed in the Implementor section of the Standards Handbook for that specific SWIFTStandard.
- (3) Example: a FIN block 4 containing { 4 : 20 : TRN MSG1000 : 79 : MESSAGE TEXT } is included as follows in the Body element : 20 : TRN MSG1000 : 79 : MESSAGE TEXT, base64-encoded.

The Header type is defined as a union of the following types:

- **Message**: when the DataPDU carries a message sent by the application to Alliance Access or by Alliance Access to the application.
- **HistoryReport**: when the DataPDU carries a report used by Alliance Access to send a History or Information Notification to the application.
- **TransmissionReport**: when the DataPDU carries a report used by Alliance Access to send a Transmission Notification to the application.
- **DeliveryNotification**: when the DataPDU carries a Delivery Notification sent by Alliance Access to the application.
- **DeliveryReport**: when the DataPDU carries a report used by Alliance Access to send a reconciled Delivery Notification to the application. Alliance Access sends such a report only if the Traffic Reconciliation component of Alliance Access is used to reconcile Delivery Notifications with original messages.
- **MessageStatus**: when the DataPDU carries the status of the message processing sent by Alliance Access to the application. In case of error, it contains an error code that indicates why the message was rejected by Alliance Access.
- **SessionStatus**: when the DataPDU carries the status of a session sent by Alliance Access to the application. This is not applicable to MQSA.

Element	Description	Type	From	To
(Message 	See "Message".	Message	M	M
HistoryReport 	See "HistoryReport".	HistoryReport	--	M
TransmissionReport 	See "TransmissionReport".	TransmissionReport	--	M
DeliveryNotification 	See "DeliveryNotification".	DeliveryNotification	--	M

Element	Description	Type	From	To
DeliveryReport 	See "DeliveryReport".	DeliveryReport	--	M
MessageStatus 	See "MessageStatus".	MessageStatus	--	M
SessionStatus)	See "SessionStatus".	SessionStatus	--	M

A.2.7.3.2 Message

Message elements

Element	Description	Type	From	To
SenderReference	Reference provided by the application for reconciliation (see "Message Reconciliation Scenario") of a DataPDU carrying a message with the corresponding report DataPDUs. Length is 70 characters.	String	M	M
MessageIdentifier	The identification of the message. For an MT message, the format is: <code>fin apc.<msgtype>[.<mug variant>]⁽¹⁾</code> For example, fin.103, fin.103.REMIT or fin.202, fin.202.COV For an MX message, the format is: <code><bus. area>.<msg type>.<variant>.<version></code> For example, ifds.001.001.01 The MessageIdentifier is used as the Request Type of the InterAct or FileAct message. It corresponds to the namespace URI of the XML Document in the Body which has the following structure: <code>urn-prefix: [[service name] \$]MessageIdentifier</code>	String	M	M
Format	The message format: <ul style="list-style-type: none">• for an MT message: MT• for an MX message: MX• for an FpML message: FpML• for a File message: File• for any message in an XML format not included in a deployment package installed on Alliance Access: AnyXML	String	M	M

Element	Description	Type	From	To
	<p>Note This list is not exhaustive. New values may be introduced by new or updated deployment packages installed on Alliance Access .</p>			
SubFormat	<p>The message sub-format.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Input (default value) • Output <p>Both values can be used for the "From" as well as the "To" direction.</p>	Enumeration ⁽²⁾	O	M
Sender	The address of the message sender (see "AddressInfo").	AddressInfo	M	M
Receiver	The address of the message receiver (see "AddressInfo").	AddressInfo	M	M
InterfaceInfo	General information managed by Alliance Access (see "InterfaceInfo").	InterfaceInfo	O	O
NetworkInfo	Network-related information managed by Alliance Access (see "NetworkInfo").	NetworkInfo	O/M ⁽³⁾	O
SecurityInfo	Security-related information managed by Alliance Access (see "SecurityInfo").	SecurityInfo	O	O
SAInfo	Information about the Alliance Access instance that processes the message.	SAInfo	O	O
FileLogicalName	Logical name of the file (1 to 254 characters).	String	O	O

(1) Message User Group

(2) When the type Enumeration is used, possible values are defined in the Description column.

(3) Optional for an MT message, mandatory for an MX message (contains the Service).

A.2.7.3.2.1 InterfaceInfo

InterfaceInfo elements

This structure contains all the network-related information managed by Alliance Access to process messages.

Element	Description	Type	From	To
UserReference	<p>The Message User Reference.</p> <p>For FIN, this corresponds to the MUR (field 108 of block 3).</p> <p>For SWIFTNet, this is the RequestRef (part of the InterAct RequestHeader).</p>	String	O	O
RoutingCode	Information to influence routing in Alliance Access. The code entered here is visible	String	O	O

Element	Description	Type	From	To
	through the routing keyword 'Routing_code' (see "RoutingInstruction").			
ValidationLevel	<p>Requested message validation level.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • None • Minimum • Extract routing keywords from message text • Intermediate • MT messages: Minimum + syntax validation • MX messages: same as Minimum • Maximum • Same as Intermediate <p>If specified, has precedence over the Alliance Access configuration.</p>	Enumeration	O	--
IsModificationAllowed	<p>If set to true, then the message can be modified using the Message Modification application or using Message Management (available on Alliance Web Platform).</p> <p>If set to false, then the message cannot be changed.</p> <p>Default value: as defined in the configuration.</p>	Boolean	O	--
RoutingInstruction	<p>Specifies where the message has to be created (see "RoutingInstruction").</p> <p>If specified, has precedence over the message partner configuration.</p> <p>Currently not applicable to MQSA: if present, it is ignored.</p>	RoutingInstruction	O	--
MessageCreator	<p>The component that created the message.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • ApplicationInterface • SWIFTNetInterface • FINInterface • Workstation • Messenger • Other <p>Only present for Original or Copy instances.</p> <p>From: the value is ignored⁽¹⁾.</p>	Enumeration	O	O

Element	Description	Type	From	To
MessageContext	<p>The message instance type:</p> <ul style="list-style-type: none"> • Original • Copy • Report <p>From: the value is ignored⁽¹⁾.</p>	Enumeration	O	M
MessageNature	<p>The message nature.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Financial • Text • Network • Security • Service <p>For MX messages, the value Financial must be used.</p> <p>From: only for Output messages.</p>	Enumeration	O	M
ProductInfo	Information about the back-office applications sending the messages.	ProductList	O	--

(1) This field is optional in the From direction to allow a DataPDU received from Alliance Access to be sent to Alliance Access again without changing it. However, Alliance Access ignores its value.

A.2.7.3.2.2 NetworkInfo

NetworkInfo elements

This structure contains all the network-related information managed by Alliance Access to process messages.

Element	Description	Type	From	To
Priority	<p>The Network priority.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Normal • Urgent • System (FIN only) <p>Default value: Normal.</p>	Enumeration	O	M
IsPossibleDuplicate	<p>From: the application indicates that the message is a PDE (Possible Duplicate Emission).</p> <p>To: Alliance Access indicates that the message was locally marked (within Alliance Access, either by means of a manual operation or by the interface) as a possible duplicate, or that it has possibly</p>	Boolean	O	M

Element	Description	Type	From	To
	been delivered already to the application, or that it has been received with a PDE/ PDM indication. In the latter case, the element DuplicateHistory is also present. Default value: false.			
DuplicateHistory	History details of the possible duplicates (PDEs and PDMS). From: for Output messages only.	PDEPDM [1..N]	O	O
IsNotificationRequested	Indicates whether a positive delivery notification is requested. Can also be used for Real-time FileAct. Default value: false.	Boolean	O	O
Service	The SWIFTNet service name. Mandatory for SWIFTNet. For FIN, the value must be 'swift.fin' when specified.	String	O	M
Network	The network over which the message has been transmitted. Possible values are: <ul style="list-style-type: none">• Application• SWIFTNet• FIN• Other From: for Output messages only.	Enumeration	O	M
SessionNr	The network session number. From: for Output messages only.	Integer	O	M
SeqNr	The network sequence number. From: for Output messages only.	Integer	O	M
(SWIFTNetNetworkInfo 	SWIFTNet-specific network information (see "SWIFTNetNetworkInfo").	SWIFTNetNetworkInfo	O	O
FINNetworkInfo)	FIN-specific network information (see "FINNetworkInfo").	FINNetworkInfo	O	O

A.2.7.3.2.2.1 SWIFTNetNetworkInfo

SWIFTNetNetworkInfo elements

Element	Description	Type	From	To
RequestType	Contains the request type of the message. If the request type is not present, then for AnyXML messages, the request type is assumed to be the same as the message identifier. For MX messages, it corresponds to the namespace URI of the XML document in the body of the message.	String	O	O

Element	Description	Type	From	To
SWIFTRef	<p>The reference generated by the central SWIFT infrastructure.</p> <p>Always present for Output messages, Transmission Reports with delivery status Acked, and Delivery Reports, for InterAct traffic. FileAct messages do not use this element.</p> <p>Format:</p> <p>SWITCHid-YYYY-MM- DDTHH:MM:SS.procid.digitsZ</p> <p>Where:</p> <ul style="list-style-type: none"> • <code>SWITCHid</code> is the ID of the switch that generated the reference • <code>procid</code> is the process ID of the process that created the reference • <code>digits</code> makes the reference unique within a given second • the timestamp is the time of generation of the reference in UTC <p>From: for Output messages only.</p>	String	O	O
SNLRef	<p>The reference generated by the emitting SWIFTNet Link.</p> <p>Always present for Output messages, Transmission Reports with delivery status Acked, and Delivery Reports.</p> <p>Format:</p> <p>SNLid-YYYY-MM- DDTHH:MM:SS.procid.digitsZ</p> <p>Where <code>SNLid</code> is the ID of the SWIFTNet Link that generated the reference.</p> <p>The other parts are identical to the format of "SWIFTRef".</p> <p>From: for Output messages only.</p>	String	O	O
Reference	<p>The reference generated by Alliance Access (for messages sent) or by the correspondent application (for messages received).</p> <p>From: for Output messages only.</p>	String	O	O
SNLEndPoint	<p>The SWIFTNet Link endpoint.</p> <p>Real-time messages only.</p> <p>From: for Output messages only.</p>	String	O	O
SnFQueueName	<p>The store-and-forward queue name.</p> <p>Store-and-forward messages only.</p> <p>From: for Output messages only.</p>	String	O	O
SnFIInputTime	SWIFTNet storage location and time of a store-and-forward request (UTC).	String	O	O

Element	Description	Type	From	To
	<p>Format:</p> <p>nnnn:YYYY-MM-DDTHH:MM:SS</p> <p>Where <code>nnnn</code> is the SWIFT internal storage identifier.</p>			
SnFDeliveryTime	<p>The time (UTC) when the message was acknowledged by the receiver.</p> <p>Format:</p> <p>YYYY-MM-DDTHH:MM:SSZ</p>	String	O	O
CreationTime	<p>The time (local system time in UTC) when the initial message request was created.</p> <p>Format:</p> <p>YYYY-MM-DDTHH:MM:SSZ</p> <p>The CreationTime is only meaningful for an output message.</p>	String	O	O
ValidationDescriptor	<p>MVal processing result.</p> <p>From: for Output messages only.</p>	Any	O	O
ResponseResponderDN	<p>The responder DN of the response.</p> <p>Real-time messages only.</p>	String	--	O
ResponseSWIFTRef	<p>The response reference generated by the central SWIFT infrastructure.</p> <p>Format:</p> <p>SWITCHid-YYYY-MM-DDTHH:MM:SS.procid.digitsZ</p> <p>Where:</p> <ul style="list-style-type: none"> • <code>SWITCHid</code> is the ID of the switch that generated the reference • <code>procid</code> is the process ID of the process that created the reference • <code>digits</code> makes the reference unique within a given second • the timestamp is the time of generation of the reference in UTC <p>Real-time messages only.</p>	String	--	O
ResponseSNLRef	<p>The reference generated by the SWIFTNet Link of the responding application.</p> <p>Format:</p> <p>SNLid-YYYY-MM-DDTHH:MM:SS.procid.digitsZ</p> <p>Where <code>SNLid</code> is the ID of the SWIFTNet Link that generated the reference.</p> <p>The other parts are identical to the format of "SWIFTRef".</p> <p>Real-time messages only.</p>	String	--	O

Element	Description	Type	From	To
ResponseReference	The reference generated by the responding application. Format: see " <i>SwiftReference</i> " in SWIFTNetNetworkInfo. Real-time messages only.	String	--	O
IsPossibleDuplicateResponse	Indicates whether the response is a possible duplicate. Real-time messages only. Default value: false.	Boolean	--	O
ResponseValidationDescriptor	MVal processing result of the response. Real-time messages only.	Any	--	O
PayloadAttributes	List of names and values associated to attributes of SWIFTNet message requests. Example: the attribute "type" on the SwInt:RequestPayload.	PayloadAttributeList	-	O
ResponsePayloadAttributes	List of names and values associated with attributes of SWIFTNet message responses. Example: the attribute "type" on the SwInt:ResponsePayload.	PayloadAttributeList	-	O
IsCopyRequested	True when the SWIFTNet copy feature is optional for that service and a copy must be made. When absent, a copy is only made when the copy feature is defined as mandatory for the service. If the copy service is defined as mandatory, then this value cannot be False.	Boolean	O	O
IsAuthNotificationRequested	Request a positive Authorisation Notification for Y-Copy service.	Boolean	O	-
CopyInfo	Provides copy-processing related information. From: for Output messages only.	Sw:Copy	O	O
TransferRef	The unique reference of the file transfer. From: for Output messages only.	String	O	O
StoredTransferRef	The unique reference of the file transfer notification. For Reception only on store and forward.	String	-	O
OrigSnFRef	Present if a notification relates to a copy. For Reception only on store and forward.	String	-	O
TransferDescription	Information about the file transfer (free text).	String	O	O
TransferInfo	Structured data that the receiver can use for automatic processing of the file transfer.	String	O	O
FileDescription	Information about the file (free text).	String	O	O
FileInfo	Structured data that the receiver can use for automatic processing of the file.	String	O	O
HeaderInfo	Sw:HeaderInfo in end-to-end control data.	XML	O	O

Element	Description	Type	From	To
	Sometimes this element is mandatory. See "The HeaderInfo element" on page 704.			
NotificationResponderDN	Delivery Notification Receiver DN (for Real-time FileAct). Not present for Output messages.	String	O	O
NotificationRequestType	Delivery Notification Request Type (for Real-time FileAct).	String	O	O
FileStartTime	The time when the file transfer was started. From: for Output messages only. Format: YYYYMMDDHHMMSS	String	O	O
FileEndTime	The time when the file transfer ended. From: for Output messages only. Format: YYYYMMDDHHMMSS	String	O	O
OverdueWarningTime	Time and date in UTC after which store and forward has to generate an overdue warning if the message/file remains undelivered. Cannot be in the past or more than 14 days in the future. If present, no OverdueWarningDelay can be specified. Format: YYYY-MM-DDTHH:MM:SSZ	String	O	O
OverdueWarningDelay	Number of minutes after which store and forward has to generate an overdue warning if the message/file remains undelivered. Minimum 5, maximum 1440 (1 day). If present, no OverdueWarningTime can be specified.	String	O	O
RecipientList	The list of recipients to which the message/file must be distributed. The content of the element RecipientList of an input message is placed in the element RecipientDNList of the related output message. The element RecipientDNList is included in the element DistributionInfo.	RecipientList	O	--
ThirdPartyList	The list of third party recipients to which the message or file must be copied in case of dynamic T- or Y-Copy.	ThirdPartyList	O	O
IsRecipientListPublic	This element, when absent or equal to TRUE, indicates that the RecipientList is public and has to be forwarded to all Recipients.	Boolean	O	--
DistributionInfo	Distribution information provided to the recipient of a distributed message or file. From: for output messages only.	Sw:DistributionInfo	O	O

The HeaderInfo element

Sometimes, the `HeaderInfo` element is mandatory. The Application Service Profile defines the mandatory elements for a service, or for a particular solution. You can specify these key mandatory elements in the `HeaderInfo` element and therefore, the content of `HeaderInfo` differs for each service.

The `HeaderInfo` is placed in the FileAct header and verified by the SWIFTNet central system or back-office application based on the service that uses it. The SWIFTNet central system verifies the presence, syntax and semantic meaning of the elements. If the verification fails, then the message is rejected.

The FileAct Header information is mandated for the following services that SWIFT administers:

Service	Request Types	General FileAct Header Documentation	Solution-specific FileAct Header requirements
swift.remit.fast	All	Standards MX - General Information Guide	SWIFTRemit Standards MX Message Implementation Guidelines
swift.remit.fast!p			
swift.remit.fast!x			

Note SWIFTNet Copy Services can copy the content of the `HeaderInfo` element and send it to a Copy destination.

The following connection methods support the use of the `HeaderInfo` element:

- "File Transfer" on page 554
- "SOAP" on page 576
- "WebSphere MQ" on page 605

A.2.7.3.2.2.2 FINNetworkInfo

FINNetworkInfo elements

Element	Description	Type	From	To
UserPriority	FIN User Header field 113; Banking Priority	String	O	O
CopyService	Value-added service ID	String	O	O
MessageSyntaxVersion	The syntax version (for example, 0505). From: Output messages only.	String	O	M
IsRetrieved	Indicates whether the message is a retrieved message. Default value: false. Output messages only.	Boolean	O	O
ReleaseInfo	FIN User Header field 115: information from Central Institution to the receiver of payment message. Output messages only.	String	O	O
ValidationIdentifier	FIN User Header field 119: Validation Identifier Cannot be present if the MessageIdentifier contains the optional Message User Group (see "Message").	String	O	O

Element	Description	Type	From	To
CorrespondentInputReference	The sender logical terminal, session, and sequence numbers used by the correspondent to send the message. Output messages only.	String	O	O
CorrespondentInputTime	Time and date the message was sent by the correspondent. Output messages only.	String	O	O
LocalOutputTime	Time and date the message was received by this interface. Output messages only.	String	O	O
SystemOriginated	SYS trailer Output messages only.	String	O	O
DelayedMessage	Delayed Message trailer Output messages only.	String	O	O
FINUserHeader	Full FIN user header (block 3 of FIN message)	String	O	O

A.2.7.3.2.3 SecurityInfo

SecurityInfo elements

This structure contains all the security-related information managed by Alliance Access to process messages.

Element	Description	Type	From	To
IsSigningRequested	Indicates whether signing of the message is required upon emission: <ul style="list-style-type: none"> SWIFTNet: if specified, overrides the Alliance Access emission profile configuration. FIN: if specified, the value is ignored. 	Boolean	O	--
RMAResult	The result of the Authorisation verification. Possible values are: <ul style="list-style-type: none"> Success Bypassed NoRecord NotEnabled InvalidPeriod Unauthorised Not present when message is not subject to RMA authorisation. From: Output messages only.	Enumeration	O	O
(SWIFTNetSecurityInfo	SWIFTNet-specific security information (see "SWIFTNetSecurityInfo").	SWIFTNetSecurityInfo	O	O

Element	Description	Type	From	To
FINSecurityInfo				
)	FIN-specific security information (see "FINSecurityInfo").	FINSecurityInfo	O	O

A.2.7.3.2.3.1 SWIFTNetSecurityInfo

SWIFTNetSecurityInfo elements

Element	Description	Type	From	To
IsNRRequested	Indicates whether non-repudiation is requested. Default value: as defined in the Alliance Access emission profile configuration.	Boolean	O	--
SignerDN	The Signer DN. From: Output messages only.	String	O	O
NRTYPE	Non-repudiation processing information (Type). Possible values are: <ul style="list-style-type: none">• SvcOpt• SvcMand From: Output messages only.	Enumeration	O	O
NRWarning	Non-repudiation processing information (Warning).	String	O	O
SignatureResult	The signature result. Possible values are: <ul style="list-style-type: none">• Success• Bypassed• Failed From: Output messages only.	Enumeration	O	O
SignatureValue	The signature value. From: Output messages only.	Any	O	O
ResponseNRTYPE	Non-repudiation processing information (Type) for the response. Possible values are: <ul style="list-style-type: none">• SvcOpt• SvcMand Real-time messages only.	Enumeration	--	O
ResponseNRWarning	Non-repudiation processing information for the response (Warning). Real-time messages only.	String	--	O
ResponseSignatureResult	The signature result for the response.	Enumeration	--	O

Element	Description	Type	From	To
	<p>Possible values are:</p> <ul style="list-style-type: none"> • Success • Bypassed • Failed <p>Real-time messages only.</p>			
ResponseSignatureValue	The signature value for the response. Real-time messages only.	Any	--	O
FileDigestAlgorithm	Name of the file digest algorithm ("SHA-1" or "SHA-256"). 1 to 20 characters.	String	O	O
FileDigestValue	Value of the file digest. 1 to 50 characters.	String	O	O
DigestList	<p>Allows to override the usual digest(s) used for MX and File messages. Optional and composed of up to 8 digests.</p> <p>Composed of 2 elements:</p> <ul style="list-style-type: none"> • DigestRef (mandatory) • DigestValue (optional). 	DigestList	O	O
ThirdPartySignerDn	The Third Party Signer DN if the digest on Sw:ThirdPartyToSenderInfo is received in a second signature. From: for Output messages only.	String	O	O

A.2.7.3.2.3.2 FINSecurityInfo

FINSecurityInfo elements

Element	Description	Type	From	To
ChecksumResult	<p>The result of the FIN checksum validation.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Success • Failed <p>From: Output messages only.</p>	Enumeration	O	O
ChecksumValue	The value of the FIN checksum. From: Output messages only.	String	O	O
PACResult	<p>The result of the PAC verification.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Success • SuccessFuture • SuccessOld • Bypassed 	Enumeration	O	O

Element	Description	Type	From	To
	<ul style="list-style-type: none"> • NoKey • Failed • InvalidDigest • InvalidSignerDN • InvalidCertPolicyID <p>From: Output messages only.</p>			
PACValue	<p>PAC value:</p> <ul style="list-style-type: none"> • From: MT 097 Input message (FINCopy server) and Output messages. • To: Present if the message is subject to FINCopy. <p>Depending on the Alliance Access configuration for message partner or MQSA, the value can be a "dummy" value (00000000).</p>	String	O	O
MACResult	<p>The result of the MAC verification.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Success • SuccessFuture • SuccessOld • Bypassed • NoKey • Failed • InvalidDigest • InvalidSignerDN • InvalidCertPolicyID <p>From: Output messages only.</p>	Enumeration	O	O
MACValue	<p>MAC value.</p> <p>Present if the message requires authentication.</p> <p>Depending on the Alliance Access configuration for message partner or MQSA, the value can be a "dummy" value (00000000).</p> <p>From: Output messages only.</p>	String	O	O
MACSignatureValue	<p>Signature of the MAC equivalent digest (also includes the PAC1⁽¹⁾ equivalent digest if required).</p> <p>From: Output messages only.</p>	Any	O	O

Element	Description	Type	From	To
PAC2SignatureValue	Signature of the PAC2 ⁽²⁾ equivalent digest. From: Output messages only.	Any	O	O

(1) Used for authentication between the Sender of the message and the Central Institution.

(2) Used for authentication between the Central Institution and the Receiver of the message.

A.2.7.3.3 HistoryReport

HistoryReport elements

Alliance Access uses a HistoryReport to send a "History Notification" or "Information Notification" to the application.

The Print connection method supports the transmission of a history notification of both input and output messages.

The connection method that uses XML version 2 supports the transmission of a history notification only for input messages.

For a History Notification, the report contains a list of all interventions belonging to the related instance, up to the routing point where the History Notification was created.

For an Information Notification, the report only contains the interventions that were created at the routing point where the Information Notification was created.

Element	Description	Type	From	To
SenderReference	SenderReference that the application has provided when sending the corresponding message.	String	--	M
OriginalInstanceAddressee	The address of the receiver of the original instance (see "AddressFullName").	AddressFullName	--	M
ReportingApplication	The Alliance Access component that generated the report Possible values are: <ul style="list-style-type: none">• ApplicationInterface• FINInterface• SWIFTNetInterface• TrafficReconciliation• Other	Enumeration	--	M
SAInfo	Information about the Alliance Access instance that processes the message.	SAInfo	-	O
Interventions	The list of interventions.	HistoryIntervention [1..N]	--	M

Element	Description	Type	From	To
IsRelatedInstanceOriginal	<p>Indicates whether this report is about an Original or a Copy instance:</p> <ul style="list-style-type: none"> • true: RelatedInstanceAddressee is not present • false: RelatedInstanceAddressee is possibly present 	Boolean	--	M
RelatedInstanceAddressee	<p>If this report concerns a Copy instance, then this field contains the address of the receiver of the Copy (see "AddressFullName").</p> <p>Present if the element IsRelatedInstanceOriginal (previous element) has a value of false.</p>	AddressFullName	--	O
MessageCreator	<p>The Alliance Access component that created the message.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • ApplicationInterface • SWIFTNetInterface • FINInterface • Workstation • Messenger • Other 	Enumeration	--	M
IsMessageModified	Indicates whether the message has been modified within Alliance Access.	Boolean	--	M
MessageFields	<p>The level of detail that Alliance Access provides about the original Message (next element), as defined in the Alliance Access configuration.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • NoOriginal <p>The next element Message will not be present.</p> <p>Used when the Message Partner or queue profile is configured to never send the original message for notifications.</p> <p>When the Message Partner or queue profile is configured to include the original message in the report, the following values allow defining the elements of the original message that are present in the next element Message:</p> <ul style="list-style-type: none"> • MinimumInfo 	Enumeration	--	M

Element	Description	Type	From	To
	<p>The next element Message contains the element Header, but not the element Body. The Header will not contain the InterfaceInfo, NetworkInfo, SecurityInfo elements.</p> <p>Corresponds to a configuration specifying "Minimum Info".</p> <ul style="list-style-type: none"> • HeaderOnly <p>The next element Message contains the complete element Header but not the element Body. Corresponds to a configuration specifying "Headers Only"</p> <ul style="list-style-type: none"> • HeaderAndBody <p>The next element Message contains its complete structure.</p> <p>Corresponds to a configuration specifying "Complete Text" or "Expanded".</p>			
Message	The original Message (see "Message"). The content of this element depends on the value of MessageFields.	Message	--	O

A.2.7.3.4 TransmissionReport

TransmissionReport elements

Alliance Access uses a TransmissionReport to send a Transmission Notification to the application. The report contains an intervention of type TransmissionReport, and optionally, an intervention of type TransmissionResponse. A transmission response can appear for real-time input messages for which the real-time server generates a business response.

A Transmission Notification instance is created by the Alliance Access network interface components (for example, SWIFT Interface for MT, SWIFTNet Interface for MX) when an attempt is made to transmit the message.

Element	Description	Type	From	To
SenderReference	SenderReference that has been provided by the application when sending the corresponding message.	String	--	M
ReconciliationInfo	<p>Used by the application to reconcile a Delivery Notification with the original message through a Report (see "Message Reconciliation Scenario").</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • MIR of the message for FIN • SwiftRef of the message for SWIFTNet <p>Only present when element NetworkDeliveryStatus has value NetworkAcked.</p>	String	--	O

Element	Description	Type	From	To
NetworkDeliveryStatus	<p>The network delivery status.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • NetworkAcked • NetworkNacked • NetworkRejectedLocally <p>The message has been rejected by Alliance Access before emission.</p> <ul style="list-style-type: none"> • NetworkAborted <p>The message emission has been aborted due to a communication error or a user abort of the session.</p> <ul style="list-style-type: none"> • NetworkTimedOut <p>The acknowledgement for the message was not received within the allowed time (SWIFTNet only).</p> <ul style="list-style-type: none"> • NetworkWaitingAck <p>Transient state.</p> <p>Unless the Alliance Access routing is configured to do so, the last 3 values are not reported to the application.</p>	Enumeration	--	M
OriginalInstanceAddressee	The address of the receiver of the original instance (see "AddressFullName").	AddressFullName	--	M
ReportingApplication	<p>The Alliance Access component that generated the report.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • ApplicationInterface • FINInterface • SWIFTNetInterface • TrafficReconciliation • Other 	Enumeration	--	M
NetworkInfo	Network-related information managed by Alliance Access (see "NetworkInfo").	NetworkInfo	--	M
SAInfo	Information about the Alliance Access instance that processes the message.	SAInfo	-	O
Interventions	The list of interventions.	Intervention [1..N]	--	M

Element	Description	Type	From	To
IsRelatedInstanceOriginal	Indicates whether this report is about an Original or a Copy instance: <ul style="list-style-type: none"> • true: RelatedInstanceAddressee is not present • false: RelatedInstanceAddressee is possibly present 	Boolean	--	M
RelatedInstanceAddressee	If this report concerns a Copy instance, then this field contains the address of the receiver of the Copy (see "AddressFullName"). Present if the element IsRelatedInstanceOriginal (previous element) has a value of false.	AddressFullName	--	O
MessageCreator	The Alliance Access component that created the message. Possible values are: <ul style="list-style-type: none"> • ApplicationInterface • SWIFTNetInterface • FINInterface • Workstation • Messenger • Other 	Enumeration	--	M
IsMessageModified	Indicates whether the message has been modified within Alliance Access.	Boolean	--	M
MessageFields	See the definition of MessageFields in "HistoryReport".	Enumeration	--	M
Message	The original Message (see "Message"). The content of this element depends on the value of MessageFields.	Message	--	O

A.2.7.3.5 DeliveryNotification

DeliveryNotification elements

Alliance Access uses a DeliveryNotification to send a Delivery Notification to the application.
The report contains an intervention of type DeliveryReport.

Element	Description	Type	From	To
ReconciliationInfo	Reconciliation information. Value: <ul style="list-style-type: none"> • MIR of the original message for FIN • SwiftRef of the original message for SWIFTNet. 	String	-	M

Element	Description	Type	From	To
	<p>This element contains the information that the application requires, to reconcile the DeliveryNotification with the TransmissionReport (through the ReconciliationInfo element present in the TransmissionReport), then with the original Message (through the SenderReference element of the TransmissionReport and of the original Message).</p> <p>See "Message Reconciliation Scenario" for an explanation of the reconciliation scenario.</p>			
ReceiverDeliveryStatus	<p>The Delivery Notification status.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • RcvDelivered • RcvAborted • RcvDelayedNak <p>FIN: the message has been rejected by FIN and has not been received by the correspondent</p> <p>SWIFTNet store-and-forward: the message has been rejected by the correspondent.</p> <ul style="list-style-type: none"> • RcvFCPReleased <p>The message has been released by the Central Institution (FIN only).</p> <ul style="list-style-type: none"> • RcvOverdue <p>Can occur only when the related message had Priority set to Urgent.</p> <ul style="list-style-type: none"> • RcvUnknown <p>Can occur, for instance, when InterAct or FileAct messages are sent in the context of a distribution to several recipients.</p>	Enumeration	--	M
MessageIdentifier	<p>The identification of the message.</p> <p>For an MT message, the format is:</p> <p><code>fin apc.<msgtype>[.<mug⁽¹⁾>]</code></p> <p>For example, <code>fin.103, fin.103.REMIT</code></p> <p>Otherwise, the value is the string "Delivery Notification".</p>	String	--	M
Receiver	<p>The address of the receiver of the Delivery Notification (see "AddressInfo").</p> <p>FIN only.</p>	AddressInfo	--	O
InterfaceInfo	General information managed by Alliance Access (see "InterfaceInfo").	InterfaceInfo	--	O

Element	Description	Type	From	To
NetworkInfo	Network-related information managed by Alliance Access (see "NetworkInfo").	NetworkInfo	--	O
SecurityInfo	Security-related information managed by Alliance Access (see "SecurityInfo"). FIN only.	SecurityInfo	--	O
SAAInfo	Information about the Alliance Access instance that processes the message.	SAAInfo	-	O

(1) Message User Group

A.2.7.3.6 DeliveryReport

DeliveryReport elements

Alliance Access uses a DeliveryReport to send a Delivery Notification to the application when the Traffic Reconciliation component of Alliance Access is used. The report contains an intervention of type DeliveryReport.

Element	Description	Type	From	To
SenderReference	SenderReference that the application has provided when sending the corresponding message.	String	--	M
ReceiverDeliveryStatus	The Delivery Notification status. Possible values are: <ul style="list-style-type: none">• RcvDelivered• RcvAborted• RcvDelayedNak• RcvFCPReleased• RcvOverdue See "DeliveryNotification".	String	--	M
OriginalInstanceAddressee	The address of the receiver of the original instance (see "AddressFullName").	AddressFullName	--	M
ReportingApplication	The Alliance Access component that generated the report. Possible values are: <ul style="list-style-type: none">• ApplicationInterface• FINInterface• SWIFTNetInterface• TrafficReconciliation• Other	Enumeration	--	M
NetworkInfo	Network-related information managed by Alliance Access (see "NetworkInfo").	NetworkInfo	--	M

Element	Description	Type	From	To
SAAInfo	Information about the Alliance Access instance that processes the message.	SAAInfo	-	O
Interventions	The list of interventions.	Intervention [1..N]	--	M
IsRelatedInstanceOriginal	Indicates whether this report is about an Original or a Copy instance Possible values are: <ul style="list-style-type: none">• true: RelatedInstanceAddressee is not present• false: RelatedInstanceAddressee is possibly present	Boolean	--	M
RelatedInstanceAddressee	If this report concerns a Copy instance, then this field contains the address of the receiver of the Copy (see "AddressFullName"). Present if the element IsRelatedInstanceOriginal has a value of false.	AddressFullName	--	O
MessageCreator	The Alliance Access component that created the message. Possible values are: <ul style="list-style-type: none">• ApplicationInterface• SWIFTNetInterface• FINInterface• Workstation• Messenger• Other	Enumeration	--	M
IsMessageModified	Indicates whether the message has been modified within Alliance Access.	Boolean	--	M
MessageFields	See the definition of MessageFields in "HistoryReport".	Enumeration	--	M
Message	The original Message (see "Message"). The content of this element depends on the value of MessageFields.	Message	--	O

A.2.7.3.7 MessageStatus

MessageStatus elements

Element	Description	Type	From	To
SenderReference	Sender reference that had been provided by the application when sending the corresponding Message.	String	--	O

Element	Description	Type	From	To
SeqNr	The sequence number of the concerned DataPDU in the file. Not applicable to MQSA.	Integer	--	O
IsSuccess	Indicates the result of the processing of the DataPDU by Alliance Access: <ul style="list-style-type: none"> • true if the DataPDU was processed successfully by Alliance Access • false if an error occurred during the processing of the DataPDU. 	Boolean	--	M
ErrorCode	Code identifying the error. Only present if the element IsSuccess has value false.	String	--	O
ErrorText	Text associated with the error code. Only present if the element IsSuccess has value false.	String	--	O
SAAInfo	Information about the Alliance Access instance that processes the message.	SAAInfo	-	O

A.2.7.3.8 SessionStatus

SessionStatus elements

Not applicable to MQSA.

Element	Description	Type	From	To
MessagePartner	The name of the message partner.	String	M	M
CreationTime	Date and Time the SessionStatus DataPDU was generated. Format: 'YYYYMMDDHHMMSS'	String	M	M
SessionNr	The session number.	Integer	M	M
InputFile	The name of the input file.	String	--	O
IsSuccess	Indicates the result of the processing by Alliance Access: <ul style="list-style-type: none"> • false if the session was aborted by Alliance Access during the processing of the file (no PDU contained in the file has been processed by Alliance Access). • true otherwise. 	Boolean	M	M
ErrorCode	Code identifying the error. Only present if the element IsSuccess has a value of false.	String	O	O
ErrorText	Text associated with the error code. Only present if the element IsSuccess has a value of false.	String	O	O

Element	Description	Type	From	To
SessionDirection	<p>The direction of the message flow:</p> <ul style="list-style-type: none"> FromMessagePartner: message from the message partner to Alliance Access. ToMessagePartner: message to the message partner from Alliance Access. ToAndFromMessagePartner: message to the message partner from Alliance Access and message from the message partner to Alliance Access. <p>Only present for SOAP adapters.</p>	String	O	O
Accepted	<p>Depends of the SessionDirection setting:</p> <ul style="list-style-type: none"> FromMessagePartner: the number of messages accepted by Alliance Access. ToMessagePartner: the number of messages sent by Alliance Access and accepted by the message partner. <p>If the element SessionDirection is not present, then the number of messages accepted by Alliance Access.</p>	Integer	O	O
Rejected	<p>Depends of the SessionDirection setting:</p> <ul style="list-style-type: none"> FromMessagePartner: the number of messages rejected by Alliance Access. ToMessagePartner: the number of messages sent by Alliance Access and accepted by the message partner. <p>If the element SessionDirection is not present, then the number of messages rejected by Alliance Access.</p> <p>Only present if the element IsSuccess has a value of "true".</p>	Integer	O	O
AcceptedFromMessagePartner	<p>The number of messages accepted by Alliance Access.</p> <p>Only present if the element IsSuccess has a value of true and for the SOAP connection method.</p>	Integer	O	O
RejectedFromMessagePartner	<p>The number of messages rejected by Alliance Access.</p> <p>Only present if the element IsSuccess has a value of true and for the SOAP connection method.</p>	Integer	O	O
AcceptedToMessagePartner	<p>The number of messages sent by Alliance Access and accepted by the message partner.</p> <p>Only present if the element IsSuccess has a value of true and for the SOAP connection method.</p>	Integer	O	O

Element	Description	Type	From	To
RejectedToMessagePartner	The number of messages sent by Alliance Access and rejected by the message partner. Only present if the element IsSuccess has a value of true and for the SOAP connection method.	Integer	O	O

A.2.7.3.9 Auxiliary Types

A.2.7.3.9.1 AddressInfo

AddressInfo elements

Element	Description	Type	From	To
(BIC12 	Sender: The first 9 characters identify the Sender logical terminal. "X" is accepted as 9th character in a BIC12. If the logical terminal is not defined in Alliance Access, then the message is rejected with an error (see "Error Codes"). Receiver: the 9th char must always be "X". FIN only.	String	M	M
Nickname 	The correspondent nickname. Only for a Receiver address. FIN only. Currently not applicable to MQSA.	String	M	--
) DN	The DN identifying the sender or receiver of the message. SWIFTNet only. If the FullName element (below) is not present, the DN content is used as follows to build the correspondent parts used for the correspondent lookup in Alliance Access. Example: DN = cn=name,ou=payment,o=bank,o=swift <ul style="list-style-type: none"> • bank is mapped to a correspondent X1 part: the institution BIC11. The character X is added to obtain a string of 11 characters, that is, bankXXXXXXXX. • payment is mapped to a correspondent X2 part: the department or application name • name is mapped to a correspondent X3 part: if the correspondent type is Application, then it contains routing information. If the correspondent type is Individual, then it contains the last name. 	String	M	M

Element	Description	Type	From	To
FullName	<p>Detailed address information (see "AddressFullName").</p> <p>Alliance Access always sends this to the application if present in the Correspondent Information File.</p> <p>Cannot be specified if the element Nickname is present.</p>	AddressFullName	O	O

A.2.7.3.9.2 AddressFullName

AddressFullName elements

Element	Description	Type	From	To
X1	<p>The correspondent X1 part: the Institution BIC11.</p> <p>The format used for SWIFTNet system messages (and that is used when receiving such messages) is SWIFTXXXXXX.</p> <p>For FIN system messages the format is SWFTXXXXXX.</p>	String	M	M
X2	<p>The correspondent X2 part: Department or Application name.</p> <p>Present if correspondent is of type Department or Application or Individual.</p>	String	O	O
X3	<p>The correspondent X3 part: if the correspondent type is Application, then it contains routing information; if the correspondent type is Individual, then it contains the last name.</p> <p>Present if the correspondent is of type Application or Individual.</p>	String	O	O
X4	<p>The correspondent X4 part: the firstname.</p> <p>Present if the correspondent is of type Individual.</p>	String	O	O
FinancialInstitution	Name of the institution.	String	O	O
BranchInformation	Branch information.	String	O	O
CityName	City name.	String	O	O
Location	Location.	String	O	O
CountryCode	Country code.	String	O	O

A.2.7.3.9.3 RoutingInstruction

RoutingInstruction elements

Element	Description	Type	From	To
RoutingFunction	<p>The routing function to be performed on the message.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> Route 	Enumeration	M	--

Element	Description	Type	From	To
	<p>the target routing point is determined by the routing rules of Alliance Access</p> <ul style="list-style-type: none"> • DisposeToRoutingPoint the target routing point is specified by the value of the next element • DisposeToRoutingStep the target routing point is specified by the value of the RoutingStep element 			
RoutingPoint	<p>The target routing point.</p> <p>Present if the element RoutingFunction has value "DisposeToRoutingPoint".</p>	String	O	--
RoutingStep	<p>The requested message disposition state. The corresponding routing point name is listed between parentheses.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Verify (_MP_verification) • Authorise (_MP_authorisation) • Modify (_MP_mod_text) • ReadyToSend (based on the preferred network settings of the Receiver in the Alliance Access Correspondent Information File) <p>Present if the element RoutingFunction has a value of "DisposeToRoutingStep".</p>	Enumeration	O	--

A.2.7.3.9.4 PDEPDM

PDEPDM elements

Element	Description	Type	From	To
(PDE 	FIN only: the PDE value.	String	O	M
) PDM	FIN: the PDM value. SWIFTNet: the store and forward PDM history.	String	O	M

A.2.7.3.9.5 Intervention

Intervention elements

This type is only used in the elements of type TransmissionReport and DeliveryReport.

Element	Description	Type	From	To
IntvCategory	Intervention category.	Enumeration	--	M

Element	Description	Type	From	To
	<p>Possible values are:</p> <ul style="list-style-type: none"> • TransmissionReport present if TransmissionReport • DeliveryReport present if DeliveryReport • TransmissionResponse only present in TransmissionReport or HistoryReport for MX Input messages. 			
CreationTime	The intervention creation date and time. Format: "YYYYMMDDHHMMSS".	String	--	M
OperatorOrigin	The name of the operator that triggered the intervention creation.	String	--	M
Contents	The intervention contents.	Any	-	M

A.2.7.3.9.6 HistoryIntervention

HistoryIntervention elements

This type is only used in the element HistoryReport. The difference with the type Intervention (see "Intervention") is that the contents of the intervention (element Text) is passed as a String (escaped). The format of the intervention contents in a HistoryReport can indeed be a combination of free-format text and of XML.

Element	Description	Type	From	To
IntvCategory	<p>Intervention category.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • TransmissionReport present if TransmissionReport • DeliveryReport present if DeliveryReport • TransmissionResponse only present in TransmissionReport or HistoryReport for MX Input messages • Security • Routing • MesgAsTransmitted • MesgAsReceived • MesgModified • Other 	Enumeration	--	M

Element	Description	Type	From	To
CreationTime	The intervention creation date and time. Format: "YYYYMMDDHHMMSS".	String	--	M
OperatorOrigin	The name of the operator that triggered the intervention creation.	String	--	M
Text	The intervention text.	String	--	M

A.2.7.3.9.7 SAAInfo

SAAInfo elements

The SAAInfo element is an optional element. However, if you do include it, then you must specify all of its sub-elements:

Element	Description	Type	From	To
InstanceName	The instance name of the Alliance Access that sends the message to a back-office application. It is followed by "/" and the exit point where the message was processed, or the queue to which the message was routed. From: the value is ignored.	String	O	M
UserName	The OS user that runs the Alliance Access server. From: the value is ignored.	String	O	M
Unit	The Alliance Access Unit to which the message belongs. From: the value is ignored.	String	O	M

A.2.7.3.10 Additional Information

Introduction

The elements described in this section are not included in the DataPDU schema described in "DataPDU":

- AckNack
- SwGbl:Status
- Sw:SnFPDMHistory
- Sw:NotifSnFRequestHandle
- SwInt:ValidationDescriptor

These are Alliance Access or SWIFTNet-specific data elements that Alliance Access provides to the application for completeness. Further processing of these elements is not required, but their structure is listed. Note that the structure of these elements can evolve with future releases of SWIFTNet.

ACK/NAK

Element	Description	Type	From	To
PseudoAckNack	Alliance Access-generated Pseudo SWIFT Acknowledgement.	String	--	M
SwGbl:Status	Optional SWIFTNet report status.	SwGbl:Status	--	O

Generation of a Pseudo SWIFT Acknowledgement (ACKNAK)

The Pseudo SWIFT Acknowledgement has the following structure:

```

<AckNack>
  <PseudoAckNack>
    {1:F21BIC8(Sender_X1)}ABranch(Sender_X1)
    SessionNbrSequenceNbr}{4:{177:LocalTime(YYMMDDHHMM)}
    {451:0(Ack)/1(Nack)}{405:Code}{311:ACK/NAK\r\nText}
    {108:Message_User_Reference(1..16)}}
  </PseudoAckNack>
  <SwGbl:Status>
    ...
  </SwGbl:Status>
</AckNack>

```

Note White spaces have been added for readability.

Parts that are in bold are placeholders that are substituted with their actual value as follows:

- **BIC8(Sender_X1)**: the BIC8 of the sender X1, for instance SAAABEBB
- **Branch(Sender_X1)**: the branch of the sender X1, for instance XXX
- **SessionNbr**: the emission session number, for instance 000012
- **SequenceNbr**: the emission sequence number, for instance 00000001
- **LocalTime**: the local time in YYMMDDHHMM format, for instance 0611061025
- **0(Ack)/1(Nack)**: 0 in case of ACK or 1 in case of NACK
- **ACK/NAK**: either ACK or NACK
- **Message_User_Reference**: the message user reference

The **Code** and **Text** parts are optional. They are present on unsuccessful emission of a message on the network.

The Code and Text values are filled as follows:

Code	Text	Description
T02	Value of the first occurrence of <SwGbl:Details><SwGbl:Code> if present	Transmission error When the value of the element <SwGbl:Severity> is either Fatal or Transient, and the value of the element <SwGbl:Code> is Sw.Gbl.NetworkTransmissionError.
T04	File marked as duplicate by correspondent	In the context of FileAct, the file sent is marked as duplicate by the correspondent.
T05	File rejected by correspondent	In the context of FileAct, the file sent is rejected by the correspondent.

Code	Text	Description
T06	File aborted by correspondent (remote abort) or File aborted by <user> (local abort)	In the context of FileAct, the file transfer has been aborted either remotely by the correspondent during reception, or locally by the user sending the file.
T03	Value of the first occurrence of <SwGbl:Details><SwGbl:Code>	All other cases.
LEN	-	In the context of FIN, the total FIN message length exceeds 10k.
COR	-	In the context of FIN, the correspondent specified in the FIN messages is marked as inactive in the Correspondent File.
AUT	-	In the context of FIN, there is no valid RMA authorisation to send the FIN message.
ADR	-	In the context of FIN, there is an inconsistency between the message and the sender/receiver: A live message has a T&T destination as sender. A live message has a T&T destination as receiver. The message is not live and the sender is a LIVE destination (except for messages MT 076, 087, and 092).
OTH	-	In the context of FIN, any other reason.

Example:

```
<AckNack><PseudoAckNack>{1:F21SAAABEBBAXXX00001200000001}{4:{177:0611061025}
{451:1}{405:T02}{311:NAK
Sw.SPX.TpCall1TPENOENT}{108:REF-1-0610311645}}</PseudoAckNack>
<SwGbl:Status>...</SwGbl:Status></AckNack>
```

SwGbl:Status

Element	Description	Type	From	To
SwGbl:StatusAttributes	Report status of top-level processing of called function. Can occur multiple times when the function does iterative processing (for example, a message validation function may return all syntax errors).	SwGbl:StatusAttributes [1..N]	--	M

SwGbl:StatusAttributes

Element	Description	Type	From	To
SwGbl:Severity	Possible values: <ul style="list-style-type: none"> • Fatal • Transient • Logic • Success • Warning 	String	--	M
SwGbl:Code	Status code. The list of error codes is available in SWIFTNet Link Error Codes	String	--	M

Element	Description	Type	From	To
	(part of the SWIFTNet Link documentation set).			
SwGbl:Parameter	Content depends on the error.	Any [0..N]	--	O
SwGbl:Text	Textual description. No processing, except display/print for information, must be performed on this element.	String	--	O
SwGbl:Action	Proposed corrective action.	String	--	O
SwGbl:Details	Lower level detailed report.	SwGbl:Details [0..N]	--	O

SwGbl:Details

Element	Description	Type	From	To
SwGbl:Code	Status code.	String	--	M
SwGbl:Text	Textual description.	String	--	O
SwGbl:Action	Proposed corrective action.	String	--	O

Sw:SnFPDMHistory

Element	Description	Type	From	To
Sw:SnFPDMHistory	In case of previous delivery attempts, gives the delivery attempt history.	Sw:SnFDeliveryHistory	--	M

Sw:SnFDeliveryHistory

Element	Description	Type	From	To
Sw:SnFDeliveryInfo	Message delivery information. In case of disaster take-over (SWIFT side), all messages present in the queue at the moment of the disaster are flagged for possible duplicate delivery, but without delivery information.	Sw:SnFDeliveryInfo [0..N]	--	O

Sw:SnFDeliveryInfo

Element	Description	Type	From	To
Sw:SwiftTime	SWIFT time of the delivery attempt (UTC). Format: YYYY-MM-DDTHH:MM:SSZ	String	--	O
SwSec:UserDN	Authoriser DN of the session owner.	String	--	O
Sw:SnFSessionId	Store-and-forward session identifier when the message was delivered. Format: <queue>:(d p):<6 digit session number>	String	--	O
SwInt:SNLId	SNL ID of the physical SWIFTNet Link where message was delivered.	String	--	O
Sw:RetryReason	Reason why the message failed delivery.	SwGbl:Status [0..1]	--	O

Sample SnFPDMHistory structure for SWIFTNet release 6.0, as described in the previous tables:

```

<Sw:SnFPDMHistory>
  <Sw:SnFDeliveryInfo>
    <Sw:SwiftTime>2005-07-19T08:58:37Z</Sw:SwiftTime>
    <SwSec:UserDN>ou=zurich,o=bankwxyz,o=swift</SwSec:UserDN>
    <Sw:SnFSessionId>bankwxyz_applicql:p:000458</Sw:SnFSessionId>
    <SwInt:SNLId>SNL00835D1</SwInt:SNLId>
    <Sw:RetryReason>
      <SwGbl:Status>
        <SwGbl:StatusAttributes>
          <SwGbl:Severity>Transient</SwGbl:Severity>
          <SwGbl:Code>See Error Guide</SwGbl:Code>
          <SwGbl:Text>One liner error description</SwGbl:Text>
          <SwGbl:Action>Retry Message</SwGbl:Action>
        </SwGbl:StatusAttributes>
      </SwGbl:Status>
    </Sw:RetryReason>
  </Sw:SnFDeliveryInfo>
</Sw:SnFPDMHistory>

```

Sw:NotifSnFRequestHandle

Element	Description	Type	From	To
Sw:SnFRef	Store-and-forward message reference of the notification. Contains the SwiftRef of the original message (see "SWIFTNetRequestAttribute" on page 644).	String	--	M
Sw:SnFRefType	Type of message for which this notification is provided. Possible value: <ul style="list-style-type: none">• InterAct	String	--	M
Sw:AcceptStatus	Type of store-and-forward notification. Possible values: <ul style="list-style-type: none">• Accepted message accepted by the receiver• Rejected message rejected by the receiver• Failed SWIFT failed to deliver the message	String	--	M
Sw:AckSwiftTime	The SWIFT acceptance time of the request ("Accepted", "Rejected") or generation time of the delivery notification request ("Failed") in UTC. Format: YYYY-MM-DDTHH:MM:SSZ	String	--	M
Sw:AckDescription	Provides information about the acknowledgement. Free text. In case the Sw:AcceptStatus is "Failed" (delivery notification generated by SWIFT),	String	--	O

Element	Description	Type	From	To
	<p>the Sw:AckDescription contains the following:</p> <ul style="list-style-type: none"> • Message has expired (code SwGbl.MessageExpired) • Message delivery attempts exceeded system threshold (code SwGbl.MaxRetryExceeded) 			
Sw:AckInfo	<p>Provides information about the acknowledgement.</p> <p>Structured data that the client can analyse.</p> <p>In case the Sw:AcceptStatus is "Failed" (delivery notification generated by SWIFT), the Sw:AckInfo contains the following:</p> <p>SwRejectCode=<reject code></p> <p>Where reject code is:</p> <p>SwGbl.MessageExpired SwGbl.MaxRetryExceeded</p>	String	--	O

SwInt:ValidationDescriptor

Element	Description	Type	From	To
SwInt:ValResult	<p>Indicates the result of validation.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Success • Warning • Fatal (not currently used) 	String	--	M
SwInt:ValStatus	<p>This contains the details of error(s) found.</p> <p>More than one SwGbl:StatusAttributes can be present.</p> <p>Present if SwInt:ValResult is Warning.</p>	SwGbl:Status	--	O

Example:

```

<SwInt:ValResult>Warning</SwInt:ValResult>
<SwInt:ValStatus>
  <SwGbl:StatusAttributes>
    <SwGbl:Severity>Warning</SwGbl:Severity>
    <SwGbl:Code><!--SWIFTStandards error code--></SwGbl:Code>
    <SwGbl:Text><!--additional diagnostic information--></SwGbl:Text>
  </SwGbl:StatusAttributes>
</SwInt:ValStatus>

```

A.2.7.4 Message Reconciliation Scenario

Overview

This section describes how a message sent by an application can be reconciled with its network ACK and with the (optional) Delivery Notification subsequently sent by Alliance Access to the application.

Process

1. When sending the message to Alliance Access, the application assigns a unique reference to the message which it puts in the element SenderReference of the Message DataPDU that contains the message.
2. After receiving and processing the Message DataPDU, Alliance Access sends the message over the network. When Alliance Access receives the network ACK (or NAK), it sends a TransmissionReport DataPDU to the application.

This TransmissionReport DataPDU contains:

- an element SenderReference containing the unique reference that was provided by the application in the original Message DataPDU
 - an element ReconciliationInfo containing the Message Input Reference (for an MT message) or the SWIFTRef (for an MX message); the contents of this element are used by the application for future reconciliation with the Delivery Notification (step 4).
3. When receiving a TransmissionReport DataPDU, the application can reconcile it with the original Message DataPDU through the contents of its element SenderReference. At this stage, the contents of the elements ReconciliationInfo, and SenderReference contained in the Transmission Report DataPDU must be stored together for future reconciliation of the Delivery Notification. Note that Alliance Access can possibly send the message multiple times; the application must be able to handle multiple TransmissionReports for the same message.
 4. When Alliance Access receives a Delivery Notification for a message that has been sent and ACK'ed, two scenarios are possible:
 - If the Traffic Reconciliation component of Alliance Access is used to reconcile the Delivery Notification with the original message, then Alliance Access sends a DeliveryReport DataPDU to the application. The DeliveryReport contains an element SenderReference with the unique reference as the original message. In this scenario, the application can reconcile the DeliveryReport DataPDU with the original Message DataPDU through the contents of its element SenderReference.
 - If the Traffic Reconciliation component of Alliance Access is not used or cannot perform the reconciliation because the original message is no longer present in the Alliance Access database (due to archiving), then Alliance Access sends a DeliveryNotification DataPDU to the application. In this scenario, the application:
 - can reconcile the DeliveryNotification carried in the Message DataPDU the corresponding TransmissionReport DataPDU by matching the contents of its element ReconciliationInfo with the ReconciliationInfo it has stored when it received the TransmissionReport DataPDU from Alliance Access (step 3),
 - can then find back the original Message DataPDU from the TransmissionReport PDU through the SenderReference stored with the ReconciliationInfo (step 3).

Note

For MT messages, the DeliveryNotification DataPDU can be received by the application before the TransmissionReport DataPDU. A FIN Delivery Notification is a system message: system messages are processed by Alliance Access with a higher priority. The design of the application must take this into account.

A.2.7.5 Examples

A.2.7.5.1 Exchange of MT Messages

A.2.7.5.1.1 Emission Flow DataPDUs

Introduction

The following sections contain examples of DataPDUs exchanged between an application and Alliance Access during the emission flow of an MT message.

Message Sent by an Application to Alliance Access

The following shows an example of Message DataPDU sent by an application to Alliance Access:

```
<?xml version="1.0" encoding="utf-8" ?>
<DataPDU xmlns="urn:swift:saa:xsd:saa.2.0">
  <Header>
    <Message>
      <SenderReference>REF10610311637</SenderReference>
      <MessageIdentifier>fin.199</MessageIdentifier>
      <Format>MT</Format>
      <Sender>
        <BIC12>SAARBEBBAXXX</BIC12>
        <FullName>
          <X1>SAARBEBBXXX</X1>
        </FullName>
      </Sender>
      <Receiver>
        <BIC12>SAARBEBBXXXX</BIC12>
        <FullName>
          <X1>SAARBEBBXXX</X1>
        </FullName>
      </Receiver>
      <InterfaceInfo>
        <UserReference>REF10610311637</UserReference>
      </InterfaceInfo>
      <NetworkInfo>
        <IsNotificationRequested>true</IsNotificationRequested>
        <FINNetworkInfo />
      </NetworkInfo>
      <SecurityInfo>
        <FINSecurityInfo />
      </SecurityInfo>
    </Message>
  </Header>
  <Body>DQo6MjA6VFJOIE1TRzEwMDANCjo3OTpNRVNTQUdFIFRFWFQ=</Body>
</DataPDU>
```

MessageStatus Sent by Alliance Access to the Application

The following shows the MessageStatus DataPDU sent by Alliance Access to the application and the important information in this DataPDU is identified in bold:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:Header>
    <Saa:MessageStatus>
      <Saa:SenderReference>REF10610311637</Saa:SenderReference>
      <Saa:SeqNr>000001</Saa:SeqNr>
      <Saa:.IsSuccess>true</Saa:.IsSuccess>
    </Saa:MessageStatus>
  </Saa:Header>
</Saa:DataPDU>
```

```

</Saa:Header>
</Saa:DataPDU>

```

TransmissionReport Sent by Alliance Access to the Application

The following table shows the TransmissionReport DataPDU sent by Alliance Access to the application upon reception of the ACK.

The important information in this DataPDU is identified in bold:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:Header>
    <Saa:TransmissionReport>
      <Saa:SenderReference>REF10610311637</Saa:SenderReference>
      <Saa:ReconciliationInfo>061102SAARBEBBAXXX0023000049</Saa:ReconciliationInfo>
      <Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
      <Saa:OriginalInstanceAddressee>
        <Saa:X1>SAARBEBBAXXX</Saa:X1>
      </Saa:OriginalInstanceAddressee>
      <Saa:ReportingApplication>FINInterface</Saa:ReportingApplication>
      <Saa:NetworkInfo>
        <Saa:Priority>Normal</Saa:Priority>
        <Saa:IsPossibleDuplicate>true</Saa:IsPossibleDuplicate>
        <Saa:IsNotificationRequested>true</Saa:IsNotificationRequested>
        <Saa:Service>swift.fin</Saa:Service>
        <Saa:Network>FIN</Saa:Network>
        <Saa:SessionNr>0023</Saa:SessionNr>
        <Saa:SeqNr>000049</Saa:SeqNr>
        <Saa:FINNetworkInfo>
          <Saa:MessageSyntaxVersion>0605</Saa:MessageSyntaxVersion>
        </Saa:FINNetworkInfo>
      </Saa:NetworkInfo>
      <Saa:Interventions>
        <Saa:Intervention>
          <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
          <Saa:CreationTime>20061102093841</Saa:CreationTime>
          <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
          <Saa:Contents>{1:F21SAARBEBBAXXX0023000049}{4:{177:0611020938}{451:0}
{108:REF10610311637}}</Saa:Contents>
        </Saa:Intervention>
      </Saa:Interventions>
      <Saa:IsRelatedInstanceOriginal>true</Saa:IsRelatedInstanceOriginal>
      <Saa:MessageCreator>ApplicationInterface</Saa:MessageCreator>
      <Saa:IsMessageModified>false</Saa:IsMessageModified>
      <Saa:MessageFields>HeaderAndBody</Saa:MessageFields>
      <Saa:Message>
        <Saa:SenderReference>REF10610311637</Saa:SenderReference>
        <Saa:MessageIdentifier>fin.199</Saa:MessageIdentifier>
        <Saa:Format>MT</Saa:Format>
        <Saa:SubFormat>Input</Saa:SubFormat>
        <Saa:Sender>
          <Saa:BIC12>SAARBEBBAXXX</Saa:BIC12>
          <Saa:FullName>
            <Saa:X1>SAARBEBBAXXX</Saa:X1>
          </Saa:FullName>
        </Saa:Sender>
        <Saa:Receiver>
          <Saa:BIC12>SAARBEBBXXXX</Saa:BIC12>
          <Saa:FullName>
            <Saa:X1>SAARBEBBAXXX</Saa:X1>
          </Saa:FullName>
        </Saa:Receiver>
        <Saa:InterfaceInfo>
          <Saa:UserReference>REF10610311637</Saa:UserReference>

```

```

<Saa:MessageCreator>ApplicationInterface</Saa:MessageCreator>
<Saa:MessageContext>Report</Saa:MessageContext>
<Saa:MessageNature>Financial</Saa:MessageNature>
</Saa:InterfaceInfo>
<Saa:NetworkInfo>
  <Saa:Priority>Normal</Saa:Priority>
  <Saa:IsPossibleDuplicate>true</Saa:IsPossibleDuplicate>
  <Saa:IsNotificationRequested>true
  </Saa:IsNotificationRequested>
  <Saa:Service>swift.fin</Saa:Service>
  <Saa:Network>FIN</Saa:Network>
  <Saa:SessionNr>0023</Saa:SessionNr>
  <Saa:SeqNr>000049</Saa:SeqNr>
  <Saa:FINNetworkInfo>
    <Saa:MessageSyntaxVersion>0605</Saa:MessageSyntaxVersion>
  </Saa:FINNetworkInfo>
</Saa:NetworkInfo>
<Saa:SecurityInfo>
  <Saa:RMAResult>Success</Saa:RMAResult>
  <Saa:FINSecurityInfo>
    <Saa:ChecksumResult>Success</Saa:ChecksumResult>
    <Saa:ChecksumValue>6E2B36369332</Saa:ChecksumValue>
    <Saa:MACSignatureValue>
      <SwSec:Signature>
        <SwSec:SignedInfo>
          <Sw:Reference>
            <Sw:DigestValue>beDU9fHr0DzMj20uMsHHT+sDfdphSFbE0KwqCNMlIUo=</
      Sw:DigestValue>
        </Sw:Reference>
      </SwSec:SignedInfo>
      <SwSec:SignatureValue>PEMF@Proc-Type: 4,MIC-ONLY
Content-Domain: RFC822
EntrustFile-Version: 2.0
Originator-DN: cn=rma1,o=saarbebb,o=swift
Orig-SN: 1147824225
MIC-Info: SHA256, RSA,
CpjLYQA60uWErTFK6aBCleo0dHqJxFeM1GeJE2dyQET+79NvyjeWf6V8CfaEXn89
GSMyou51SyzTNc3k1PBPPKaEyyFQsYZuXm64dVvzwdoWc/xev86CkSzyIyiGML0q
ELoeVna3i61v3cSNIXRPErgVuOJ52XO90d1UQ9G5czI1rboPqC8a3dy4RXeinxJm
QjWRwdNZ82YD7IqFDpG9cdUOzbs/Ppmk1a0cR+9RQDTRlftTD3LMo7VKwthqxbXfi
2m0p1ffs6/qKpUvuFQGrt5gsRI18v03t6RPBFJ01Cefzp1Q6e5mU8T6FUPy5zNWL
ufG/XZx1D+gDD8085ZqYqw==</
</SwSec:SignatureValue>
  <SwSec:KeyInfo>
    <SwSec:SignDN>cn=rma1,o=saarbebb,o=swift
    </SwSec:SignDN>
    <SwSec:CertPolicyId>1.3.21.6.2
    </SwSec:CertPolicyId>
  </SwSec:KeyInfo>
  <SwSec:Manifest>
    <Sw:Reference>
      <Sw:DigestRef>M</Sw:DigestRef>
      <Sw:DigestValue>K3GPdVCheunY0XW46FAILtOHM44A3wLrrFxsCbCEgOA=</
      Sw:DigestValue>
    </Sw:Reference>
  <Sw:Reference>
    <Sw:DigestRef>Sw.E2S</Sw:DigestRef>
    <Sw:DigestValue>fG11fE9CYvXZWm5n0TywkTvd4RKLveQ9/F0w8H+VPMs=</
  Sw:DigestValue>
    </Sw:Reference>
  </SwSec:Manifest>
  </SwSec:Signature>
  <Saa:MACSignatureValue>
  </Saa:FINSecurityInfo>
  </Saa:SecurityInfo>
</Saa:Message>
</Saa:TransmissionReport>

```

```

</Saa:Header>
<Saa:Body>DQo6MjA6VFJOIE1TRzEwMDANCjo3OTpNRVNTQUdFIFRFWFQ=</Saa:Body>
</Saa:DataPDU>

```

DeliveryNotification Sent by Alliance Access to the Application

The following example shows the DeliveryNotification DataPDU sent by Alliance Access to the application upon reception of a Delivery Notification corresponding to the original message. It can be reconciled with the TransmissionReport DataPDU through the ReconciliationInfo element, then with the Message DataPDU through the SenderReference element of the TransmissionReport DataPDU. The important information in this DataPDU is identified in bold:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:Header>
    <Saa:DeliveryNotification>
      <Saa:ReconciliationInfo>061102SAARBEBBAXXX0023000049
      </Saa:ReconciliationInfo>
      <Saa:ReceiverDeliveryStatus>RcvDelivered
      </Saa:ReceiverDeliveryStatus>
      <Saa:MessageIdentifier>fin.011</Saa:MessageIdentifier>
      <Saa:Receiver>
        <Saa:BIC12>SAARBEBBAXXX</Saa:BIC12>
        <Saa:FullName>
          <Saa:X1>SAARBEBBAXXX</Saa:X1>
        </Saa:FullName>
      </Saa:Receiver>
      <Saa:InterfaceInfo>
        <Saa:MessageCreator>FINInterface</Saa:MessageCreator>
        <Saa:MessageContext>Original</Saa:MessageContext>
        <Saa:MessageNature>Network</Saa:MessageNature>
      </Saa:InterfaceInfo>
      <Saa:NetworkInfo>
        <Saa:Priority>System</Saa:Priority>
        <Saa:IsPossibleDuplicate>false</Saa:IsPossibleDuplicate>
        <Saa:Service>swift.fin</Saa:Service>
        <Saa:Network>FIN</Saa:Network>
        <Saa:SessionNr>0023</Saa:SessionNr>
        <Saa:SeqNr>000299</Saa:SeqNr>
        <Saa:FINNetworkInfo>
          <Saa:MessageSyntaxVersion>0605</Saa:MessageSyntaxVersion>
          <Saa:CorrespondentInputReference>061102DYLQXXXHXXX0000413146
          </Saa:CorrespondentInputReference>
          <Saa:CorrespondentInputTime>20061102083900
          </Saa:CorrespondentInputTime>
          <Saa:LocalOutputTime>20061102093900</Saa:LocalOutputTime>
          <Saa:SystemOriginated>{SYS:}</Saa:SystemOriginated>
        </Saa:FINNetworkInfo>
      </Saa:NetworkInfo>
      <Saa:SecurityInfo>
        <Saa:FINSecurityInfo>
          <Saa:ChecksumResult>Success</Saa:ChecksumResult>
          <Saa:ChecksumValue>8BB8247F0C2E</Saa:ChecksumValue>
        </Saa:FINSecurityInfo>
      </Saa:SecurityInfo>
    </Saa:DeliveryNotification>
  </Saa:Header>
  <Saa:Body>ezE3NTowOTM4fxsxMDY6MDYxMTAyU0FBUKJFQkJBWFhYMDAyMzAwMDA0OX17MTA4O1JF
RjEwNjEwMzExNjM3fxsxNzU6MDkzOH17MTA3Oja2MTEwM1NBQVJCRUJCQVhYWDAwMjMwMDAyOTh9</
Saa:Body>
</Saa:DataPDU>

```

DeliveryReport Sent by Alliance Access to the Application

The following example shows the DeliveryReport DataPDU sent by Alliance Access to the application upon reception of a message that is the Delivery Notification corresponding to the initial message when the Traffic Reconciliation component of Alliance Access is used. It can be reconciled with the TransmissionReport DataPDU and the Message DataPDU through the SenderReference element. The important information in this DataPDU is identified in bold:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:Header>
    <Saa:DeliveryReport>
      <Saa:SenderReference>REF10610311637</Saa:SenderReference>
      <Saa:ReceiverDeliveryStatus>RcvDelivered</Saa:ReceiverDeliveryStatus>
      <Saa:OriginalInstanceAddressee>
        <Saa:X1>SAARBEBBXXX</Saa:X1>
      <Saa:OriginalInstanceAddressee>
      <Saa:ReportingApplication>TrafficReconciliation
      <Saa:ReportingApplication>
      <Saa:NetworkInfo>
        <Saa:Priority>Normal</Saa:Priority>
        <Saa:IsPossibleDuplicate>true</Saa:IsPossibleDuplicate>
        <Saa:IsNotificationRequested>true</Saa:IsNotificationRequested>
        <Saa:Service>swift.fin</Saa:Service>
        <Saa:Network>FIN</Saa:Network>
        <Saa:SessionNr>0023</Saa:SessionNr>
        <Saa:SeqNr>000049</Saa:SeqNr>
        <Saa:FINNetworkInfo>
          <Saa:MessageSyntaxVersion>0605</Saa:MessageSyntaxVersion>
        </Saa:FINNetworkInfo>
      </Saa:NetworkInfo>
      <Saa:Interventions>
        <Saa:Intervention>
          <Saa:IntvCategory>DeliveryReport</Saa:IntvCategory>
          <Saa:CreationTime>20061102094143</Saa:CreationTime>
          <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
          <Saa:Contents>{175:0938}{106:061102SAARBEBBAXXX002300049}
          {108:REF10610311637}{175:0938}{107:061102SAARBEBBAXXX0023000298}
        </Saa:Contents>
      </Saa:Intervention>
    </Saa:Interventions>
    <Saa:IsRelatedInstanceOriginal>true</Saa:IsRelatedInstanceOriginal>
    <Saa:MessageCreator>ApplicationInterface</Saa:MessageCreator>
    <Saa:IsMessageModified>false</Saa:IsMessageModified>
    <Saa:MessageFields>NoOriginal</Saa:MessageFields>
  </Saa:DeliveryReport>
  </Saa:Header>
</Saa:DataPDU>

```

A.2.7.5.1.2 Reception Flow DataPDUs

Message Sent by Alliance Access to the Application

The following shows an example of Message DataPDU sent by an application to Alliance Access upon reception of a message from the network:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:Header>
    <Saa:Message>
      <Saa:SenderReference>OSAARBEBBXXX199TRN MSG1000
    </Saa:SenderReference>
  </Saa:Header>
</Saa:DataPDU>

```

```

<Saa:MessageIdentifier>fin.199</Saa:MessageIdentifier>
<Saa:Format>MT</Saa:Format>
<Saa:SubFormat>Output</Saa:SubFormat>
<Saa:Sender>
  <Saa:BIC12>SAARBEBBAXXX</Saa:BIC12>
  <Saa:FullName>
    <Saa:X1>SAARBEBBAXXX</Saa:X1>
  </Saa:FullName>
</Saa:Sender>
<Saa:Receiver>
  <Saa:BIC12>SAARBEBBAXXX</Saa:BIC12>
  <Saa:FullName>
    <Saa:X1>SAARBEBBAXXX</Saa:X1>
  </Saa:FullName>
</Saa:Receiver>
<Saa:InterfaceInfo>
  <Saa:UserReference>REF10610311637</Saa:UserReference>
  <Saa:MessageCreator>FINInterface</Saa:MessageCreator>
  <Saa:MessageContext>Original</Saa:MessageContext>
  <Saa:MessageNature>Financial</Saa:MessageNature>
</Saa:InterfaceInfo>
<Saa:NetworkInfo>
  <Saa:Priority>Normal</Saa:Priority>
  <Saa:IsPossibleDuplicate>true</Saa:IsPossibleDuplicate>
<Saa:DuplicateHistory>
  <Saa:PDE>{PDE:}</Saa:PDE>
</Saa:DuplicateHistory>
<Saa:Service>swift.fin</Saa:Service>
<Saa:Network>FIN</Saa:Network>
<Saa:SessionNr>0023</Saa:SessionNr>
<Saa:SeqNr>000298</Saa:SeqNr>
<Saa:FINNetworkInfo>
  <Saa:MessageSyntaxVersion>0605</Saa:MessageSyntaxVersion>
  <Saa:CorrespondentInputReference>061102SAARBEBBAXXX0023000049
  </Saa:CorrespondentInputReference>
  <Saa:CorrespondentInputTime>20061102093800
  </Saa:CorrespondentInputTime>
  <Saa:LocalOutputTime>20061102093800</Saa:LocalOutputTime>
</Saa:FINNetworkInfo>
</Saa:NetworkInfo>
<Saa:SecurityInfo>
  <Saa:RMAResult>Success</Saa:RMAResult>
  <Saa:FINSecurityInfo>
    <Saa:ChecksumResult>Success</Saa:ChecksumResult>
    <Saa:ChecksumValue>6E2B36369332</Saa:ChecksumValue>
    <Saa:MACSignatureValue>
      <SwSec:Signature>
        <SwSec:SignedInfo>
          <Sw:Reference>
            <Sw:DigestValue>beDU9fHr0DzMj20uMsHHT+sDfdphSFbE0KwqCNM1IUo=</
Sw:DigestValue>
          </Sw:Reference>
        </SwSec:SignedInfo>
        <SwSec:SignatureValue>PEMF@Proc-Type: 4,MIC-ONLY
Content-Domain: RFC822
EntrustFile-Version: 2.0
Originator-DN: cn=rmal,o=saarbebb,o=swift
Orig-SN: 1147824225
MIC-Info: SHA256, RSA,
CpjLYQA60uWErTFK6aBCleoOdHqJxFeM1GeJE2dyQET+79NvyjeWf6V8CfaEXn89
GSMyou51SyzTNC3k1PBPPKaEyyFQsYZuXm64dVvzwdoWc/xev86CkSzyIyiGML0q
ELoeVna3i61v3cSNIXRPErgVuOJ52XO90d1UQ9G5czI1rboPqC8a3dy4RXeinxJm
QjWRwdNZ82YD71qFDpG9cd0zbs/Ppmkla0cR+9RQDTR1fTD3LMo7VKwthqxbXfi
2m0p1ffs6/qKpUvuFQGrt5gsRI18v03t6RPBFJ01CefzplQ6e5mU8T6FUPy5zNWL
ufG/XZx1D+gDD8085ZqYqw==
</SwSec:SignatureValue>
<SwSec:KeyInfo>

```

```
<SwSec:SignDN>cn=rma1,o=saarbebb,o=swift
</SwSec:SignDN>
<SwSec:CertPolicyId>1.3.21.6.2</SwSec:CertPolicyId>
</SwSec:KeyInfo>
<SwSec:Manifest>
<Sw:Reference>
<Sw:DigestRef>M</Sw:DigestRef>
<Sw:DigestValue>K3GPdVCheunY0XW46FAILtOHM44A3wLrrFxsCbCEgOA=</
Sw:DigestValue>
</Sw:Reference>
<Sw:Reference>
<Sw:DigestRef>Sw.E2S</Sw:DigestRef>
<Sw:DigestValue>fGllfE9CYvXZWm5n0TywkTvd4RKLveQ9/F0w8H+VPMs=</
Sw:DigestValue>
</Sw:Reference>
</SwSec:Manifest>
</SwSec:Signature>
</Saa:MACSignatureValue>
</Saa:FINSecurityInfo>
</Saa:SecurityInfo>
</Saa:Message>
</Saa:Header>
<Saa:Body>DQo6MjA6VFJOIE1TRzEwMDANCjo3OTpNRVNTQUdFIFRFWFQ=</Saa:Body>
</Saa:DataPDU>
```

A.2.7.5.2 Exchange of MX Messages

A.2.7.5.2.1 Emission Flow DataPDUs

Overview

The following sections contain examples of DataPDUs exchanged between an application and Alliance Access during the emission flow of an MX message.

Message Sent by an Application to Alliance Access

The following shows an example of Message DataPDU sent by an application to Alliance Access:

```
<?xml version="1.0" encoding="utf-8" ?>
<DataPDU xmlns="urn:swift:saa:xsd:saa.2.0">
<Header>
<Message>
<SenderReference>REF10610311505</SenderReference>
<MessageIdentifier>camt.029.001.02</MessageIdentifier>
<Format>MX</Format>
<Sender>
<DN>o=saaabebbb,o=swift</DN>
<FullName>
<X1>SAAABEBBXXX</X1>
</FullName>
</Sender>
<Receiver>
<DN>o=saaabebbb,o=swift</DN>
<FullName>
<X1>SAAABEBBXXX</X1>
</FullName>
</Receiver>
<InterfaceInfo>
<UserReference>REF10610311505</UserReference>
</InterfaceInfo>
<NetworkInfo>
<Service>swift.eni</Service>
</NetworkInfo>
<SecurityInfo>
<SWIFTNetSecurityInfo />
```

```

        </SecurityInfo>
        </Message>
    </Header>
    <Body>
        <AppHdr xmlns="urn:swift:xsd:$ahV10">
            <MsgRef>REF10610311505</MsgRef>
            <CrDate>2006-10-31T03:05:41.502</CrDate>
        </AppHdr>
        <Document xmlns="urn:swift:xsd:swift.eni$camt.029.001.02">
            <camt.029.001.02>
                <Assgnmnt>
                    <Id>RCUSTA20050001</Id>
                    <Assgnr>AAAAGB2L</Assgnr>
                    <Assgne>CUSAGB2L</Assgne>
                    <CreDtTm>2005-01-27T11:04:27</CreDtTm>
                </Assgnmnt>
                <RslvdCase>
                    <Id>CCCC-MOD-20050127-0003</Id>
                    <Cretr>CUSAGB2L</Cretr>
                </RslvdCase>
                <Sts>
                    <Conf>MODI</Conf>
                </Sts>
            </camt.029.001.02>
        </Document>
    </Body>
</DataPDU>

```

MessageStatus Sent by Alliance Access to the Application

The following example shows the MessageStatus DataPDU sent by Alliance Access to the application and the important information in this DataPDU is identified in bold:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
    xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
    xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
    <Saa:Header>
        <Saa:MessageStatus>
            <Saa:SenderReference>REF10610311505</Saa:SenderReference>
            <Saa:SeqNr>000001</Saa:SeqNr>
            <Saa:.IsSuccess>true</Saa:.IsSuccess>
        </Saa:MessageStatus>
    </Saa:Header>
</Saa:DataPDU>

```

TransmissionReport Sent by Alliance Access to the Application

The following example shows the TransmissionReport DataPDU sent by Alliance Access to the application upon reception of the ACK. The important information in this DataPDU is identified in bold:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
    xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
    xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
    <Saa:Header>
        <Saa:TransmissionReport>
            <Saa:SenderReference>REF10610311505</Saa:SenderReference>
            <Saa:ReconciliationInfo>SWITCH21-2006-11-02T08:41:47.11481.1454972Z</Saa:ReconciliationInfo>
            <Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
            <Saa:OriginalInstanceAddressee>
                <Saa:X1>SAAABEBBXXX</Saa:X1>
            </Saa:OriginalInstanceAddressee>
            <Saa:ReportingApplication>SWIFTNetInterface
        </Saa:ReportingApplication>

```

```

<Saa:NetworkInfo>
  <Saa:Priority>Normal</Saa:Priority>
  <Saa:IsPossibleDuplicate>true</Saa:IsPossibleDuplicate>
  <Saa:Service>swift.eni</Saa:Service>
  <Saa:Network>SWIFTNet</Saa:Network>
  <Saa:SessionNr>000008</Saa:SessionNr>
  <Saa:SeqNr>00000001</Saa:SeqNr>
  <Saa:SWIFTNetNetworkInfo>
    <Saa:SWIFTRef>SWITCH21-2006-11-02T08:41:47.11481.1454972Z
    </Saa:SWIFTRef>
    <Saa:SNLRef>SNL10391-2006-11-02T08:35:20.6268.030308Z
    </Saa:SNLRef>
    <Saa:Reference>c98e3458-1dd1-11b2-91dd-5bdc6d3f0133
    </Saa:Reference>
    <Saa:SnFInputTime>0102:2006-11-02T08:26:47</Saa:SnFInputTime>
  </Saa:SWIFTNetNetworkInfo>
</Saa:NetworkInfo>
<Saa:Interventions>
  <Saa:Intervention>
    <Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
    <Saa:CreationTime>20061102093520</Saa:CreationTime>
    <Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
    <Saa:Contents>
      <AckNack>
        <PseudoAckNack>{1:F21SAAABEBBAXXX00008000000001}{4:{177:0611020935}
{451:0}{311:ACK}{108:REF10610311505}}</PseudoAckNack>
      </AckNack>
    </Saa:Contents>
  </Saa:Intervention>
</Saa:Interventions>
<Saa:IsRelatedInstanceOriginal>true</Saa:IsRelatedInstanceOriginal>
<Saa:MessageCreator>ApplicationInterface</Saa:MessageCreator>
<Saa:IsMessageModified>false</Saa:IsMessageModified>
<Saa:MessageFields>NoOriginal</Saa:MessageFields>
</Saa:TransmissionReport>
</Saa:Header>
</Saa:DataPDU>

```

DeliveryNotification Sent by Alliance Access to the Application

The following example shows the Message DataPDU sent by Alliance Access to the application upon reception of a message that is the Delivery Notification corresponding to the initial MX message. It can be reconciled with the TransmissionReport DataPDU through the ReconciliationInfo element, then with the Message DataPDU through the SenderReference element of the TransmissionReport DataPDU. The important information in this DataPDU is identified in bold:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:Header>
    <Saa:DeliveryNotification>
      <Saa:ReconciliationInfo>SWITCH21-2006-11-02T08:41:47.11481.1454972Z
      </Saa:ReconciliationInfo>
      <Saa:ReceiverDeliveryStatus>RcvDelivered
      </Saa:ReceiverDeliveryStatus>
      <Saa:MessageIdentifier>Delivery Notification</Saa:MessageIdentifier>
      <Saa:InterfaceInfo>
        <Saa:MessageCreator>SWIFTNetInterface</Saa:MessageCreator>
        <Saa:MessageContext>Original</Saa:MessageContext>
        <Saa:MessageNature>Network</Saa:MessageNature>
      </Saa:InterfaceInfo>
      <Saa:NetworkInfo>
        <Saa:Priority>Normal</Saa:Priority>
        <Saa:IsPossibleDuplicate>false</Saa:IsPossibleDuplicate>
      </Saa:NetworkInfo>
    </Saa:DeliveryNotification>
  </Saa:Header>
</Saa:DataPDU>

```

```

<Saa:SessionNr>188959</Saa:SessionNr>
<Saa:SeqNr>000000155</Saa:SeqNr>
</Saa:NetworkInfo>
</Saa:DeliveryNotification>
</Saa:Header>
<Saa:Body>
  <Sw:NotifySnFRequestHandle>
    <Sw:SnFRef>SWITCH21-2006-11-02T08:41:47.11481.1454972Z</Sw:SnFRef>
    <Sw:SnFRefType>InterAct</Sw:SnFRefType>
    <Sw:AcceptStatus>Accepted</Sw:AcceptStatus>
    <Sw:AckSwiftTime>2006-11-02T08:39:29Z</Sw:AckSwiftTime>
    <Sw:AckInfo>Acked</Sw:AckInfo>
  </Sw:NotifySnFRequestHandle>
</Saa:Body>
</Saa:DataPDU>

```

A.2.7.5.2.2 Reception Flow DataPDUs

Message Sent by Alliance Access to the Application

The following example shows an example of Message DataPDU sent by an application to Alliance Access upon reception of a message from the network:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
  xmlns:Sw="urn:swift:snl:ns.Sw" xmlns:SwInt="urn:swift:snl:ns.SwInt"
  xmlns:SwGbl="urn:swift:snl:ns.SwGbl" xmlns:SwSec="urn:swift:snl:ns.SwSec">
  <Saa:Header>
    <Saa:Message>
      <Saa:SenderReference>OSAAABEBBXXX029REF10610311505
      </Saa:SenderReference>
      <Saa:MessageIdentifier>camt.029.001.02</Saa:MessageIdentifier>
      <Saa:Format>MX</Saa:Format>
      <Saa:SubFormat>Output</Saa:SubFormat>
      <Saa:Sender>
        <Saa:DN>o=saaabebbb,o=swift</Saa:DN>
        <Saa:FullName>
          <Saa:X1>SAAABEBBXXX</Saa:X1>
        </Saa:FullName>
      </Saa:Sender>
      <Saa:Receiver>
        <Saa:DN>o=saaabebbb,o=swift</Saa:DN>
        <Saa:FullName>
          <Saa:X1>SAAABEBBXXX</Saa:X1>
        </Saa:FullName>
      </Saa:Receiver>
      <Saa:InterfaceInfo>
        <Saa:UserReference>REF10610311505</Saa:UserReference>
        <Saa:MessageCreator>SWIFTNetInterface</Saa:MessageCreator>
        <Saa:MessageContext>Original</Saa:MessageContext>
        <Saa:MessageNature>Financial</Saa:MessageNature>
      </Saa:InterfaceInfo>
      <Saa:NetworkInfo>
        <Saa:Priority>Normal</Saa:Priority>
        <Saa:IsPossibleDuplicate>true</Saa:IsPossibleDuplicate>
        <Saa:Service>swift.eni</Saa:Service>
        <Saa:Network>SWIFTNet</Saa:Network>
        <Saa:SessionNr>188959</Saa:SessionNr>
        <Saa:SeqNr>000000154</Saa:SeqNr>
        <Saa:SWIFTNetNetworkInfo>
          <Saa:SWIFTRef>SWITCH21-2006-11-02T08:41:47.11481.1454972Z
        </Saa:SWIFTRef>
        <Saa:SNLRef>SNL10391-2006-11-02T08:35:20.6268.030308Z
      </Saa:SNLRef>
      <Saa:Reference>14be9dc8-1dd2-11b2-91dd-5bdc6d3f0133
      </Saa:Reference>
      <Saa:SnFQueueName>saaabebbb_enimsg</Saa:SnFQueueName>
    </Saa:Message>
  </Saa:Header>
</Saa:DataPDU>

```

```

<Saa:ValidationDescriptor>
  <SwInt:ValResult>Warning</SwInt:ValResult>
  <SwInt:ValStatus>
    <SwGbl:StatusAttributes>
      <SwGbl:Severity>Warning</SwGbl:Severity>
      <SwGbl:Code>Sw.MVAL.ValidationWarning</SwGbl:Code>
      <SwGbl:Text>This message could not be validated
      due to an internal SWIFT error</SwGbl:Text>
      <SwGbl:Action>Contact customer support
      </SwGbl:Action>
    </SwGbl:StatusAttributes>
  </SwInt:ValStatus>
</Saa:ValidationDescriptor>
</Saa:SWIFTNetNetworkInfo>
</Saa:NetworkInfo>
<Saa:SecurityInfo>
  <Saa:SWIFTNetSecurityInfo>
    <Saa:SignerDN>cn=rma2,o=saaabebbe,o=swift</Saa:SignerDN>
    <Saa:NRTtype>SvcMand</Saa:NRTtype>
    <Saa:NRWarning>WARNING</Saa:NRWarning>
    <Saa:SignatureResult>Success</Saa:SignatureResult>
    <Saa:SignatureValue>
      <SwSec: CryptoInternal>

      <SwSec: CipherKey>UEVNRkBQcm9jLVR5cGU6IDQsTU1DLU9OTFkNCkNvbnRlbnQtRG9tYWluOibSR
      kM4MjINCKvudHJ1c3RGaWx1LVZ1cnNpb246IDIuMA0KT3JpZ2luYXRvc1ETjogY249cm1hMixvPXN
      hYWFiZWJiLG89c3dpZnQNCk9yaWctU046IDEExNDc4MjUyNjcNCk1JQy1JbmZvOiBTSEExLCBSU0EsD
      QogV1Bwb1QyU1R0OFYydzZ3NnhaV3d2c2R5bk9jTupaQUtodHJpZk1MNDN1NS9rdThmSHc4bWppUlp
      seFNBYnRkUA0KIE16Z2JrcDdKTZ3WDI5WmVjWHVpTFpzzWJzbVFQRjBBr3RBU1hsaXZNK3NPk29BV
      EV0emRnMi9naE8rR1c0NDkNCiBONk1IYmU3RD1RN3dDa2FOQnRCTS9ucTJOVkhvM050dXY5dFBOcWN
      Iamg0b2Ntamt1V0g2TjZWVzRkUWU4SW1aDQogVFZxRnhpME9ZTkRtcmQ1aW1INUQzUXkzdldIYVo4K
      zFDbH1tMFNkckViS2YxWUcvOXA1Z05YaXBMN1MxcWxPbg0KIG0vMjBUskdTd2hKSVdaajY4aw9GcjN
      5WHBhZDRTWUpGSjVseEhFRFBULLhRVjNkbFNYazl3eHNoRTVVYWd0aDcNCiBrME5EdmNzRER1R1YvM
      jZZcmY3d3NnPT0NCg==</SwSec: CipherKey>
      <SwSec: CryptoProtocol>4.0:3.0</SwSec: CryptoProtocol>
    </SwSec: CryptoInternal>
    <SwSec: CryptoDescriptor>
      <SwSec: MemberRef>RequestPayload</SwSec: MemberRef>
      <SwSec: MemberRef>RequestHeader</SwSec: MemberRef>
      <SwSec: MemberRef>RequestDescriptor.SwiftRequestRef
      </SwSec: MemberRef>
      <SwSec: SignDN>cn=rma2,o=saaabebbe,o=swift</SwSec: SignDN>
      <SwSec: CertPolicyId>1.3.21.6.2</SwSec: CertPolicyId>
    </SwSec: CryptoDescriptor>
    </Saa: SignatureValue>
  </Saa: SWIFTNetSecurityInfo>
</Saa: SecurityInfo>
</Saa: Message>
</Saa: Header>
<Saa: Body>
  <AppHdr xmlns="urn:swift:xsd:$ahV10">
    <MsgRef>REF10610311505</MsgRef>
    <CrDate>2006-10-31T03:05:41.502</CrDate>
  </AppHdr>
  <Document xmlns="urn:swift:xsd:swift.eni$camt.029.001.02">
    <camt.029.001.02>
      <Assgnmt>
        <Id>RCUSTA20050001</Id>
        <Assgnr>AAAAGB2L</Assgnr>
        <Assgne>CUSAGB2L</Assgne>
        <CreDtTm>2005-01-27T11:04:27</CreDtTm>
      </Assgnmt>
      <RslvdCase>
        <Id>CCCC-MOD-20050127-0003</Id>
        <Cretr>CUSAGB2L</Cretr>
      </RslvdCase>
      <Sts>

```

```

<Conf>MODI</Conf>
</Sts>
</camt.029.001.02>
</Document>
</Saa:Body>
</Saa:DataPDU>

```

A.2.7.5.3 SessionStatus DataPDU Sent by Alliance Access to the Application

Case of a successful session

```

<?xml version="1.0" encoding="utf-8"?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
    xmlns:Sw="urn:swift:snl:ns.Sw"
    xmlns:SwInt="urn:swift:snl:ns.SwInt"
    xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
    xmlns:SwSec="urn:swift:snl:ns.SwSec">
    <Saa:Header>
        <Saa:SessionStatus>
            <Saa:MessagePartner>CVEFileInput</Saa:MessagePartner>
            <Saa:CreationTime>20060223112705</Saa:CreationTime>
            <Saa:InputFile>D:\Batch\Input\success.mx</Saa:InputFile>
            <Saa:SessionNr>0041</Saa:SessionNr>
            <Saa:.IsSuccess>true</Saa:.IsSuccess>
            <Saa:Accepted>10</Saa:Accepted>
            <Saa:Rejected>0</Saa:Rejected>
        </Saa:SessionStatus>
    </Saa:Header>
</Saa:DataPDU>

```

Case of an aborted session

```

<?xml version="1.0" encoding="utf-8"?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0"
    xmlns:Sw="urn:swift:snl:ns.Sw"
    xmlns:SwInt="urn:swift:snl:ns.SwInt"
    xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
    xmlns:SwSec="urn:swift:snl:ns.SwSec">
    <Saa:Header>
        <Saa:SessionStatus>
            <Saa:MessagePartner>CVEForcedInput</Saa:MessagePartner>
            <Saa:CreationTime>20060224143554</Saa:CreationTime>
            <Saa:InputFile>D:\Batch\Input\formatconflict.rje</Saa:InputFile>
            <Saa:SessionNr>0001</Saa:SessionNr>
            <Saa:.IsSuccess>false</Saa:.IsSuccess>
            <Saa:ErrorCode>EFILEINVFORMAT</Saa:ErrorCode>
            <Saa:ErrorText>
                DataPDU format does not match value configured in SAA
            </Saa:ErrorText>
        </Saa:SessionStatus>
    </Saa:Header>
</Saa:DataPDU>

```

A.2.7.6 Computing the Signature of a DataPDU

Algorithm

The signature, also referred to as local message authentication code (LMAC), is computed using the algorithm HMAC based on SHA-256 as described in ISO/IEC 9797 (see RFC 2104 - HMAC: Keyed-Hashing for Message Authentication - February 1997). This way of producing a message authentication code has the following features:

- Fast to compute
- One way (irreversible).

Algorithm specification

The HMAC algorithm produces a 128 bit LMAC.

To compute the LMAC, the algorithm needs:

- A bit stream M representing the message content to sign (see "Content to sign" on page 742).
- A truncation mask keeping only the first 128 bits (out of 256 bits).

The LMAC must be converted in Base64 using standard Base-64 content transfer encoding as specified in RFC 1521. The encoded value is the Signature as specified in the Alliance Access exchange PDU (see "Protocol Data Units" on page 692).

Content to sign

The complete DataPDU field is taken as the bit stream for the authentication algorithm, including the string <?xml version="1.0" encoding="utf-8"?>.

DataPDU encoding and format

The bit stream of the DataPDU is to be preserved from the signature time until the verification time.

The steps to compute a signature from a DataPDU are:

1. The original DataPDU, whatever it is, is considered as a bit stream.
2. This bit stream is used to compute the signature.
3. The signature accompanies the DataPDU.

The steps to verify a signature of a DataPDU are:

1. The received DataPDU, whatever it is, is considered as a bit stream.
2. This bit stream is used to compute the signature.
3. This computed signature is compared with the one that accompanies the DataPDU.

Warning about character sets

It is recommended to avoid any character set translation between the signature time and the verification time. It is anyway the typical case and the simplest design.

However, the convention above does not force to preserve the character set of a DataPDU all the time. If necessary, various translations can occur during the transport of a DataPDU as far as the original bit stream can be restored at verification time.

Warning about XML representations

It is recommended to avoid any XML transformation between the signature time and the verification time. It is anyway the typical case and the simplest design.

However, the convention above does not force to preserve the XML representation of a DataPDU. If necessary, various XML transformations can occur during the transport of a DataPDU as far as the original bit stream can be restored at verification time.

For example, the business content of a DataPDU (10£ > 5£) can have this XML representation using the character set ISO-8859-1 and a CDATA section:

```
<A><![CDATA[10£ > 5£]]> <!-- A comment --></A>
```

This can be transformed to this XML representation using US-ASCII and escaped characters:

<A>10Á > 5Á

The business content is not changed, but the bit stream of the DataPDU is totally different.

A.2.7.7 Error Codes

Overview

This section lists the possible error codes and associated error text that can be returned in the MessageStatus and the SessionStatus.

A.2.7.7.1 MessageStatus

MessageStatus error codes

Error code	Error text
EFORMAT	Message text format error
EINVSENDERLT ⁽¹⁾	FIN sender logical terminal does not exist
EINVSENDER ⁽¹⁾	The sender DN does not contain an Alliance Access licensed destination
ESIGNATURE	DataPDU Local Authentication error
EPROFILE ⁽²⁾	Operator profile does not allow creating this message
EINVDATAPDU	DataPDU syntax error
EDISPOSITION	Message cannot be routed or disposed
EBROADCAST ⁽³⁾	Nickname has no mapping in Alliance Access
EFAILURE ⁽⁴⁾	An error occurred during the message processing

(1) Not applicable to MQSA: mapped to EFAILURE.

(2) Not applicable to MQSA: no mapping.

(3) Currently not applicable to MQSA.

(4) MQSA only.

A.2.7.7.2 SessionStatus

SessionStatus error codes

Error code	Error text
ESESSABORTED	Session aborted
EFILEDUPDIGEST	File with same digest already received
EFILEDUPFILENAME	File with same name already received
EFILEINVALID	File format error
EFILEINVFORMAT	DataPDU format does not match value configured in Alliance Access
EFILEINVMESSAGE	File contains a DataPDU with the wrong format
EFILEINVFILENAME	File name not valid
EFILENOTADIRECTORY	File path name not valid

Error code	Error text
EFILEDOESNOTEXIST	No such file or directory
EFILENOACCESS	File access denied
EINTERNAL	Internal error

A.2.8 Migration Path from Version 1 to Version 2

Overview

To ease the migration from XML v1 to XML v2, the following table lists the mapping between XML v1 and XML v2 data elements.

The first column contains the original XML v1 structures and elements. The second column contains the mapping to be used when migrating to XML v2. A dot between two elements indicates that the second element is a sub-element. For instance, Message.SubFormat means the SubFormat element within the Message structure.

Wherever the element name {PDUType} is mentioned, it must be replaced with:

- Message, if the PDU carries a message
- TransmissionReport, if the PDU carries a transmission report
- DeliveryReport, if the PDU carries a delivery report.

Version 1 Type/Element	Version 2 Mapping
DataPDU	SenderReference
	Message
	Report
	LogicalReply
Report	Addressee
	OrigMessageFields
	OrigMessage
	ReportLPI
	TransmissionReport
	DeliveryReport

Version 1 Type/Element		Version 2 Mapping
Message	MessageFormat	Message.Format
	MessageSubFormat	Message.SubFormat
	Sender	Message.Sender.FullName
	Receiver	<p>One of the following, depending on the receiver type (Nickname or FullName):</p> <ul style="list-style-type: none"> • Message.Receiver.Nickname • Message.Receiver.FullName
	LiveMessage	<p>Not present.</p> <p>For MX, it can be derived from the service name (presence of !p).</p> <p>For MT, it can be derived from the BIC.</p>
	MessageNature	<p>Message.InterfaceInfo.MessageNature</p> <p>In Version 2 this tag is optional: Alliance Access determines the nature automatically (always Financial for MX, derived from syntax for MT) if it is not present. This is different compared to Version 1.</p>
	MessageLPI	<p>The subfields of this composite element are mapped to Message.InterfaceInfo, Message.SecurityInfo and Message.NetworkInfo. Check the details of MessageLPI below.</p>
	MessageSRI	<p>The subfields of this composite element are mapped to both Message.InterfaceInfo and Message.NetworkInfo. Check the details of MessageSRI below.</p>
	MessageTPI	Message.NetworkInfo
MessageSRI	UserReference	Message.InterfaceInfo.UserReference
	UserPDE	Message.NetworkInfo.IsPossibleDuplicate
MessageTPI	NetworkDelivNotify	Message.NetworkInfo.IsNotificationRequested
	Network	<p>Message.NetworkInfo.Network</p> <p>See note 2.</p>
	NetworkPriority	Message.NetworkInfo.Priority
	NetworkSessionNr	Message.NetworkInfo.SessionNr
	NetworkSeqNr	Message.NetworkInfo.SeqNr
	DuplCreation	<p>This element has been split into 2 distinct elements: Message.NetworkInfo.IsPossibleDuplicate and Message.NetworkInfo.DuplicateHistory.</p>

Version 1 Type/Element		Version 2 Mapping
MessageLPI	OriginalMessage	Message.InterfaceInfo.MessageContext
	ModifyAllowed	Message.InterfaceInfo.IsModificationAllowed
	DeleteInhibited	Was not used. Not present in Version 2.
	MinValidation	Message.InterfaceInfo.ValidationLevel
	CBTPriority	Was not used. Not present in Version 2.
	DispositionState	Message.InterfaceInfo.RoutingInstruction.RoutingStep See note 3.
	NetworkAttribute	NetworkInfo
	SecurityAttribute	Message.SecurityInfo
	FormatAttribute	Was reserved for future use in Version 1. Not present in Version 2.
	TargetApplication	Message.InterfaceInfo.RoutingInstruction
	MessageOrigin	Message.InterfaceInfo.MessageCreator
	CBTRoutingInfo	Non-relevant information. Not present in Version 2.
ReportLPI	MANRoutingCode	Message.InterfaceInfo.RoutingCode
	DuplEmission	Message.NetworkInfo.IsPossibleDuplicate
	OrigSenderReference	Not used by Alliance Access. Not present in Version 2.
	MessageOrigin	{PDUType}.MessageCreator
	Modified	{PDUType}.IsMessageModified
	OriginalRelatedMessage	{PDUType}.IsRelatedInstanceOrigin
	ReportingApplication	{PDUType}.ReportingApplication
DeliveryReport	BackToNonOriginator	Not used by Alliance Access. Not present in Version 2.
	DuplEmission	{PDUType}.NetworkInfo.IsPossibleDuplicate
	Network	DeliveryReport.NetworkInfo.Network
	NetworkAttribute	The subfields of this composite element are mapped to both DeliveryReport.NetworkInfo, and DeliveryReport.Message.SecurityInfo. Check the details of NetworkAttribute below.
	NetworkSessionNr	DeliveryReport.NetworkInfo.SessionNr
	NetworkSeqNr	DeliveryReport.NetworkInfo.SeqNr
Interventions	ReceiverDeliveryStatus	DeliveryReport.ReceiverDeliveryStatus
	Interventions	DeliveryReport.Interventions

Version 1 Type/Element		Version 2 Mapping
TransmissionReport	Network	TransmissionReport.NetworkInfo.Network
	NetworkAttribute	The subfields of this composite element are mapped to both TransmissionReport.NetworkInfo, and TransmissionReport.Message.SecurityInfo. Check the details of NetworkAttribute below.
	NetworkSessionNr	TransmissionReport.NetworkInfo.SessionNr
	NetworkSeqNr	TransmissionReport.NetworkInfo.SeqNr
	NetworkDeliveryStatus	TransmissionReport.NetworkDeliveryStatus
	Interventions	TransmissionReport.Interventions
Intervention	IntvCategory	Intervention.InterventionCategory
	CreationTime	Intervention.CreationTime
	ApplicationOrigin	Redundant information, also present in Text. Not present in Version 2.
	OperatorOrigin	Intervention.OperatorOrigin
	Text	Intervention.Contents
SWIFTNetSecurityAttribute	SigningRequired	Message.SecurityInfo.IsSigningRequested
	SignerDN	Message.SecurityInfo.SWIFTNetSecurityInfo.SignerDN
SecurityAttribute	SWIFTNetSecurityAttribute	Message.SecurityInfo
SWIFTNetResponseAttribute	ResponderDN	NetworkInfo.SWIFTNetNetworkInfo.Response.ResponderDN
	NonRepType	Message.SecurityInfo.SWIFTNetSecurityInfo.Response.NRType Although the enum type name is different in the schema (NonRepType in Version 1, NRType in Version 2), the enum values stay the same.
	NonRepWarning	Message.SecurityInfo.SWIFTNetSecurityInfo.Response.NRWarning
	ResponseRef	NetworkInfo.SWIFTNetNetworkInfo.ResponseSWIFTRef
	SwiftResponseRef	NetworkInfo.SWIFTNetNetworkInfo.ResponseSNLRef
	CBTReference	NetworkInfo.SWIFTNetNetworkInfo.ResponseReference
	DuplCreation	NetworkInfo.SWIFTNetNetworkInfo.Responsels.PossibleDuplicateResponse
	ValidationDescriptor	NetworkInfo.SWIFTNetNetworkInfo.ResponseValidationDescriptor
	AuthResult	Message.SecurityInfo.SWIFTNetSecurityInfo.ResponseSignatureResult
	AuthValue	Message.SecurityInfo.SWIFTNetSecurityInfo.ReponseSignatureValue

Version 1 Type/Element		Version 2 Mapping
SWIFTNetRequestAttribute	RequestorDN	Message.Sender.DN
	ResponderDN	Message.Receiver.DN
	Service	NetworkInfo.Service
	RequestType	Message.MessageIdentifier
	NRIndicator	Message.SecurityInfo.SWIFTNetSecurityInfo.IsNRRequested
	NonRepType	Message.SecurityInfo.SWIFTNetSecurityInfo.NRType
	NonRepWarning	Message.SecurityInfo.SWIFTNetSecurityInfo.NRWarning
	SwiftRef	NetworkInfo.SWIFTNetNetworkInfo.SWIFTRef
	SwiftRequestRef	NetworkInfo.SWIFTNetNetworkInfo.SNLRef
	CBTReference	NetworkInfo.SWIFTNetNetworkInfo.Reference
	SNLEndPoint	NetworkInfo.SWIFTNetNetworkInfo.SNLEndPoint
	SnFQueueName	NetworkInfo.SWIFTNetNetworkInfo.SnFQueueName
	SnFInputTime	NetworkInfo.SWIFTNetNetworkInfo.SnFInputTime
	SnFPDMHistory	NetworkInfo.DuplicateHistory
FormatAttribute	ValidationDescriptor	NetworkInfo.SWIFTNetNetworkInfo.ValidationDescriptor
	AuthResult	Message.SecurityInfo.SWIFTNetSecurityInfo.SignatureResult
NetworkAttribute	AuthValue	Message.SecurityInfo.SWIFTNetSecurityInfo.SignatureValue
	FormatAttributeMX	Was reserved for future use in Version 1. Not present in Version 2.
MessageOrigin	SWIFTNetRequestAttribute	The subfields of this composite element are mapped to both NetworkInfo and Message.SecurityInfo. Check the details of SWIFTNetRequestAttribute below.
	SWIFTNetResponseAttribute	The subfields of this composite element are mapped to both NetworkInfo and Message.SecurityInfo. Check the details of SWIFTNetResponseAttribute below.
TargetApplication	CBTApplication	{PDUType}.InterfaceInfo.MessageCreator See note 4.
	MessagePartner	Non-relevant information. Not present in Version 2.
	SessionNr	Non-relevant information. Not present in Version 2.
	SeqNr	Non-relevant information. Not present in Version 2.
TargetApplicationRule	TargetApplicationRule	RoutingInstruction.RoutingFunction See note 5.
	TargetRoutingPoint	RoutingInstruction.RoutingPoint

Version 1 Type/Element		Version 2 Mapping
LogicalReply	SenderReference	MessageStatus.SenderReference
	SuccessIndication	MessageStatus.IsSuccess
	ErrorText	MessageStatus.ErrorText
Address	Nickname	AddressInfo.Nickname
	FullName	AddressInfo.AddressFullName In Version 2, when using FullName, you must also specify either the BIC12, the DN, or the Nickname.
AddressFullName	X1	AddressFullName.X1
	X2	AddressFullName.X2
	X3	AddressFullName.X3
	X4	AddressFullName.X4
	FinancialInstitution	AddressFullName.FinancialInstitution
	BranchInformation	AddressFullName.BranchInformation
	CityName	AddressFullName.CityName
	Location	AddressFullName.Location
	CountryCode	AddressFullName.CountryCode

Notes

1. The enumerated type 'OrigMessageFields' has been renamed to 'MessageFields' with the following mapping:

Version 1 Value	Version 2 Value
NoOriginal	NoOriginal
Minimum	MinimumInfo
Condensed	HeaderOnly
Full	HeaderAndBody
Expanded	NA

2. The enumerated type 'TransmissionNetwork' has been renamed to "Network" with the following mapping:

Version 1 Value	Version 2 Value
ApplicationNetwork	Application
SwiftNetNetwork	SWIFTNet
OtherNetwork	Other

3. The enumerated type 'DispositionState' has been renamed to 'RoutingStep' with the following mapping:

Version 1 Value	Version 2 Value
Verify	Verify

Version 1 Value	Version 2 Value
Authorise	Authorise
Modify	Modify
Ready	ReadyToSend

4. The enumerated type 'CBTApplication' has been renamed to 'MessageCreator' with the following mapping:

Version 1 Value	Version 2 Value
ApplicationInterface	ApplicationInterface
SwiftnetInterface	SWIFTNetInterface
MessageEntry	Workstation
MessengerAdapter	Messenger
Other	Other

5. The enumerated type 'TargetApplicationRule' has been renamed to 'RoutingFunction' with the following mapping:

Version 1 Value	Version 2 Value
InternalRouting	Route
CBTApplication	DisposeToRoutingStep
RoutingPoint	DisposeToRoutingPoint

A.2.9 Codes in the Trailer (Block S)

Overview

If trailers are present, then they are included in block S. This section describes the various kinds of trailers that exist and lists possible tags.

A.2.9.1 Authentication Result Trailer

Overview

When the received message requires an Authentication trailer, Alliance Access generates the Authentication Result trailer.

The following tags indicate the result of the authentication:

Tag	Meaning
SAC	Successfully authenticated and authorised. Present if both the following conditions are met: <ul style="list-style-type: none"> • signature verification was successful • RMA authorisation verification was successful
SAB	Authentication and/or authorisation bypassed.

Tag	Meaning
	<p>Present if any of the following conditions are met:</p> <ul style="list-style-type: none"> • signature verification failed but authentication was bypassed • RMA authorisation verification failed but was bypassed
SAI	<p>Authentication and/or authorisation incorrect.</p> <p>Present if any of the following conditions are met:</p> <ul style="list-style-type: none"> • signature verification failed • RMA authorisation verification failed

Note If the message to be transferred to the back-office application is PAC2-equivalent PKI-signed, then the verification result is passed with the message in block *s*. This does not apply to connection methods that use the MERVA/2 data format).

A.2.9.2 Proprietary Authentication Result Trailer

Overview

The Proprietary Authentication Result trailer is generated by Alliance Access. It is always present when the received message requires a Proprietary Authentication trailer. The following tags indicate the result of the Alliance Access authentication compared to the Proprietary Authentication trailer value (PAC).

Tag	Meaning
FAC	<p>Successfully authenticated.</p> <p>Present if both the following conditions are met:</p> <ul style="list-style-type: none"> • signature verification was successful • PAC authentication (if present) was successful using the current key
FAB	<p>Proprietary Authentication bypassed.</p> <p>Present if either the following conditions are met:</p> <ul style="list-style-type: none"> • signature verification failed but authentication was bypassed • PAC authentication (if present) failed but was bypassed
FAI	<p>Proprietary Authentication incorrect.</p> <p>Present if either the following conditions are met:</p> <ul style="list-style-type: none"> • signature verification failed • PAC authentication (if present) failed

A.2.9.3 Local Authentication Trailer

Overview

A Local Authentication trailer may be appended to messages exchanged between Alliance Access and a message partner (both sent messages and received messages). The message partner profile must be set up to activate the Local Authentication feature.

The Authentication result is based on blocks 1 through 5, and is stored in hexadecimal format.

The following connection methods and formats can use this optional tag:

- File Transfer: RJE or DOS-PCC formats
- MQHA: MQ-MT format

Two tags are available, dependent on the authentication calculation used:

LAU	Successfully authenticated using the SA/2 authentication method.
MDG	Successfully authenticated using the HMAC-SHA-256 authentication method.

Composition of a LAU value

The following sections describe the algorithm that can be used to compute a Local Authentication value to secure a message exchange with Alliance Access message partners.

The following table describes the composition of LAU keys. The LAU key parts are expressed as ASCII character strings (the allowed character set is 0-9, A-F, and a-f), which form a 32-character string interpreted as binary values. The LAU key length is then 32 x 8 bits = 256 bits. Note that uppercase characters are distinct from lowercase characters, because the characters do not represent hexadecimal values.

Key Part	Description
Send Key First Part / Send Key Second Part	The two parts together form a 32-character hexadecimal string. The string is present only when Allowed Direction is To Message Partner or To & From Message Partner , and Key Type is set to Unidirectional .
Receive Key First Part / Receive Key Second Part	These are the first / second 16 characters of the key that are used to authenticate the input sessions. The two parts together form a 32-character hexadecimal string. The string is present only when Allowed Direction is From Message Partner or To & From Message Partner and Key Type is set to Unidirectional .
Key First Part / Key Second Part	These are the first / second 16 characters of the key that are used to authenticate the output and input sessions. The two parts form a 32-character hexadecimal string. The string is present only when Allowed Direction is To & From Message Partner and Key Type is set to Bidirectional .

Note The use of the LAU tag is not recommended, because the proprietary SWIFT SA/2 algorithm is no longer tested for security and is subject to a specific Non-Disclosure Agreement.

The MDG trailer is found in the S: block of a FIN message that is exchanged with Alliance Access over File or WebSphere MQ. The MDG computation is based on the HMAC SHA-256 algorithm (see [RFC 2104](#)). A PDF is available at http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf.

Computing an MDG value

To compute an MDG value, perform the following steps. Note that only blocks 1: through 5: are retained for the calculation. Any S: block must be dropped off; the S: block will contain the MDG value.

1. Strip any S: block from the FIN message input. Keep only blocks 1: through 5:.
2. Use the FIN message input as a binary value (unsigned char in C language, byte in Java). The FIN message input must be coded in the ASCII character set.
3. Combine the left LAU key and the right LAU key as one string. The merged LAU key must be used as a binary value (unsigned char in C language, byte in Java). The merged LAU key must be coded in the ASCII character set.
4. Call a HMAC256 routine to compute the hash value. The hash value must also be treated as a binary value (unsigned char in C language, byte in Java). The *hmac* size is 32 bytes.
5. Convert the *hmac* binary values to uppercase hexadecimal printable characters (for example, byte 0x0041 is translated to the characters 0A).

Sample computation

In this sample, the FIN input message and LAU left and right key values are as follows:

FIN message	{1:F01SWCIBEABAXXX0907000001}{2:I205SWCIBEABXXXXN}{3:{103:ZCP}{119:COV}{4:20:989COV}{21:090525/123COV}{32A:090527EUR10500,00}{52A:SWCIBEAB}{58A:SWCIBEAC}{50F:/123564982101}{1:MR. BIG}{2:HIGH STREET 3}{3:BE/BRUSSELS}{59:987654321}{MR. SMALL}{LOW STREET 15}{LONDON GB}{70:INV/1234}{33B:EUR10500,00}{:}}
LAU left key	0123456789ABCDEF
LAU right key	0123456789ABCDEF

To compute the MDG value for this sample, perform the following steps:

1. The input FIN message sample, does not contain block S:, so it does not need to be stripped out. The FIN input is exactly as shown in the table.
2. The message is already in the ASCII character set. Following are the character codes:

```

00000000h: 7B 31 3A 46 30 31 53 57 43 49 42 45 41 42 41 58 ; {1:F01SWCIBEABAX
00000010h: 58 58 30 39 30 37 30 30 30 30 31 7D 7B 32 3A ; XX0907000001}{2:
00000020h: 49 32 30 35 53 57 43 49 42 45 41 42 58 58 58 58 ; I205SWCIBEABXXXX
00000030h: 4E 7D 7B 33 3A 7B 31 30 33 3A 5A 43 50 7D 7B 31 ; N}{3:{103:ZCP}{1
00000040h: 31 39 3A 43 4F 56 7D 7D 7B 34 3A 0D 0A 3A 32 30 ; 19:COV}{4:::20
00000050h: 3A 39 38 39 43 4F 56 0D 0A 3A 32 31 3A 30 39 30 ; :989COV..:21:090
00000060h: 35 32 35 2F 31 32 33 43 4F 56 0D 0A 3A 33 32 41 ; 525/123COV..:32A
00000070h: 3A 30 39 30 35 32 37 45 55 52 31 30 35 30 30 2C ; :090527EUR10500,
00000080h: 30 30 0D 0A 3A 35 32 41 3A 53 57 43 49 42 45 41 ; 00..:52A:SWCIBEAC
00000090h: 42 0D 0A 3A 35 38 41 3A 53 57 43 49 42 45 41 43 ; B..:58A:SWCIBEAC
000000a0h: 0D 0A 3A 35 30 46 3A 2F 31 32 33 35 36 34 39 38 ; ..:50F:/12356498
000000b0h: 32 31 30 31 0D 0A 31 2F 4D 52 2E 20 42 49 47 0D ; 2101..1/MR. BIG.
000000c0h: 0A 32 2F 48 49 47 48 20 53 54 52 45 45 54 20 33 ; .2/HIGH STREET 3
000000d0h: 0D 0A 33 2F 42 45 2F 42 52 55 53 53 45 4C 53 0D ; ..3/BE/BRUSSELS.
000000e0h: 0A 3A 35 39 3A 2F 39 38 37 36 35 34 33 32 31 0D ; ..:59:/987654321.
000000f0h: 0A 4D 52 2E 20 53 4D 41 4C 4C 0D 0A 4C 4F 57 20 ; .MR. SMALL..LOW
00000100h: 53 54 52 45 45 54 20 31 35 0D 0A 4C 4F 4E 44 4F ; STREET 15..LONDO
00000110h: 4E 20 47 42 0D 0A 3A 37 30 3A 2F 49 4E 56 2F 31 ; N GB..:70:/INV/1
00000120h: 32 33 34 0D 0A 3A 33 33 42 3A 45 55 52 31 30 35 ; 234..:33B:EUR105
00000130h: 30 30 2C 30 30 0D 0A 2D 7D ; 00,00..-}

```

The FIN field delimiters <Cr><Lf> are part of the data. They have a hexadecimal value of 0x0D 0x0A. As shown in the graphic above, unsigned char is used in the C language, and byte is used in Java.

3. Combine the LAU keys. The merged result is: 0123456789ABCDEF0123456789ABCDEF. In the ASCII character set, the merged LAU key is:

```

00000000h: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 ; 0123456789ABCDEF
00000010h: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 ; 0123456789ABCDEF

```

As shown in the above graphic, the LAU key character string is not hexadecimal, but rather a binary ASCII value. In the C language, unsigned char is used. In Java, byte is used. It is an array of 32 bytes.

4. Call an HMAC256 routine to compute a hash value. You can find implementations of HMAC-SHA-256 on the Internet. The Java packages javax.crypto.Mac and javax.crypto.spec.SecretKeySpec provide HMAC-SHA-256 support.

Such routines normally perform the following:

- pad the merged LAU key with null bytes up to a length of 64 bytes
- create an Inner pad mask of 64 bytes with code 0x36
- perform an XOR between the Inner pad and the merged LAU key (Inner pad result)
- create an Outer pad of 64 bytes with code 0x5C
- perform an XOR between the Outer pad and the merged LAU key (Outer pad result)
- perform a first HMAC calculation on the Inner pad result concatenated with the message
- perform a second HMAC calculation on the Outer pad concatenated with the first computed HMAC

The calculated HMAC value must be defined as a binary value. Use unsigned char in the C language. Use byte in Java. The HMAC is a 32-byte array.

5. Convert the HMAC value to ASCII uppercase. For example, byte 0x0041 is translated to the characters 0A. This produces a string value of 64 ASCII characters:

5E87F8F390E5FB886E8311E4D7C994371FA9AF3119B2C314DAE458738AFF08AC.

This value must be inserted in the S: block for Alliance Access as: {S: {MDG:

5E87F8F390E5FB886E8311E4D7C994371FA9AF3119B2C314DAE458738AFF08AC} }.

A.2.9.4 Alliance Access Instance Information Trailer

Overview

The Alliance Access Instance Information Trailer may be appended to messages that Alliance Access exchanges with a message partner when the WebSphere MQ connection method is used.

The instance information is included if the following options are configured in the message partner profile as follows:

- The **Transfer SAA Information** option is selected.
- The data format **MQ-MT** is selected.
- The **Use MQ Descriptor** option is not selected.

Parameters in block S for instance information

The following tags include the information about the Alliance Access instance:

Tag	Size	Meaning
INS	8 bytes	The name of the Alliance Access instance which sends the message and the name of the Alliance Access queue where the message was stored.
UNT	25 bytes	The Alliance Access Unit to which the message belongs
USR	20 bytes	The OS user that runs the Alliance Access server

A.2.9.5 Alliance Possible Duplicate

Overview

The Alliance Possible Duplicate trailer is an optional trailer appended by Alliance Access. It indicates to the external interface receiver of the message that the message may have been delivered several times. The only tag for this trailer is SPD.

Example

{SPD: }

A.2.9.6 Transaction Reference Number Trailer

Overview

The Transaction Reference Number trailer can be present when the File Transfer connection method is used, if the message partner is configured with direction "From and To".

The Transaction Reference Number trailer is appended when a notification is returned to the originator without block 4 information (text of the original message). In this case, 'originator' means the same message partner that received and processed the original message.

The only tag for this trailer is TRN. The associated value comes from field 20 in the message text.

Example

{TRN:<trn-value> }

Note	The generation of a {TRN:<trn-value>} trailer always implies the presence of a {CON:} trailer.
-------------	--

A.2.9.7 Condensed Trailer

Overview

The Condensed trailer is used for batch output format RJE, and DOS-PCC. This trailer is appended when a notification without block 4 information (text of the original message) is sent to an external entity.

The only tag for this trailer is CON.

Example

{CON:}

A.2.9.8 Copy Trailer

Overview

The Copy trailer is used for batch output formats RJE, DOS-PCC, and MERVA/2. This trailer may be appended to messages by Alliance Access. If present, it indicates that the message is either a primary copy (original message) or a secondary copy (copy of a message).

There are two tags for this trailer:

Tag	Meaning
COP:P	Message is a primary copy
COP:S	Message is a secondary copy

A.2.9.9 Routing Code Trailer

Overview

The Routing Code trailer is used to transmit routing information to message partners.

The content of the **routing_code** field and the **disposition_address_code** field is controlled by the value of the configuration parameter **RTV Routing**. For more information, see "Message" on page 118.

The **Routing code transmitted** check box in a message partner profile controls the transmission of the Routing Code trailer to a message partner.

If the **Routing code transmitted** check box is not selected, then only the following information is transmitted:

- For CAS 2 message partners, the routing code is transmitted in the **ManRoutingCode** field. If the message has been retrieved, then the **NetworkRetrieved** field is set.
- For RJE message partners, the {RTV:} trailer is transmitted.

If the **Routing code transmitted** check box is selected, the above information is transmitted, along with the following:

- The routing code is transmitted in the {MAN:<RoutingCode>} trailer.
- The disposition address code is transmitted in the {DAC:RTV} trailer.

A.2.10 Support for Market Infrastructure Resiliency Service (MIRS)

With the introduction of MIRS (Market Infrastructure Resiliency Service) three new fields (423, 106, 424) are introduced in Block 3 of FIN messages, and the order of two other fields (115, 119) is now tightly controlled. The order of the fields in Block 3 is now strictly defined as follows:

Field 103:<service-code>
 Field 113:<banking-priority>
 Field 108:<mur>
 Field 119:<validation-flag>
 Field 423:<balance-checkpoint-date-and-time>
 Field 106:<mir>
 Field 424:<reference>
 Field 115:<payment-release-information-receiver>
 Field 433:<sanctions-screening-receiver-information>

For more information on these changes see "Block Structure and Format" in the *FIN Operations Guide*.

You will only be confronted with these new fields at the moment your RTGS provider implements the MIRS service.

Historically Alliance Access provided always field 115 before field 119, and your back office application might rely on this. Only the XMLv2 revision 3 and later and MQHA-MT formats provided the fields in the exact order as they came from the network. In order to limit the impact of this change to your back office, Alliance Access will behave as follows.

From Alliance Access to the back office:

1. Transfers using XMLv2 revision 3 and higher (File, SOAP or MQ transfers with MQMT) will contain the full Block 3 with the fields ordered as they come from the network. The order will be as mentioned above.
2. Transfers using XMLv2 revision 2 and older ones do not support the full Fin user header exchange with back office, meaning that there is no specific fieldtag for this information, unlike XMLv2 revision 3 or higher <Saa:FINUserHeader>. In the case of XMLv2 revision 2 and older, the information in field 115 and 119 are part of separate field tags that belong to different sections and a such there is no exact order for fields 119 and 115.
3. Transfers using RJE files or DOS-PCC will continue to receive field 115 before field 119, unless you set an environment variable to indicate that you want to receive field 119 first (per UHB). The new MIRS fields will not be provided to the back office system.

From back office to Alliance Access:

1. If the message contains the new MIRS fields then the correct order as mentioned above will be expected.
2. If the message does not contain the new MIRS fields, Alliance Access will accept field 115, and 119 independently of how they are ordered and order them correctly so that the SWIFT network can accept the message.

The net result of this is that applications that are not MIRS aware will see no change, while applications that are being enhanced to become MIRS aware have the opportunity to profit from all the data.

For more information on these changes see in the *Market Infrastructure Resiliency Service Release Letter and Service Description*.

A.3 Message Validation and Disposition

Overview

This section describes how Alliance Access validates and disposes messages in the Application Interface.

This section describes the message validation and disposition process first for messages that do not use the CAS format, and then, for messages in the CAS format.

A.3.1 Message Validation and Disposition Overview

Description

Message disposition provides the means to either "hold and check" messages arriving from a particular message partner, or to forward the messages using the routing rules set at the Application Interface Inbound queue.

The default disposition for all message formats is specified in the following places:

- For automatic input sessions: the **Reception** area of the message partner profile.
- For manual input sessions: the **Start Session** or **Run Session** window.

If you require no restriction on message disposition, then select **Route** in the **Route** field of the **Reception** area

To dispose messages into a particular message preparation queue, then select:

1. Dispose from the **Route** option in the **Reception** area.

Note

All message preparation queues are available to the message partner by default. However, the permission to bypass certain stages in the message preparation sequence depends on the permissions defined by the profile used.

For instance, if the **R7.1_MsgPartner** profile permits the message partner to bypass Verification but not Authorisation, then the message may skip Verification and be disposed to the Authorisation queue.

-
2. The field **Message In** appears. Click the field to display a list of available message preparation queues.
 3. Select one of the following queues, as appropriate:
 - Modification (**_MP_mod_text**)
 - Verification
 - Authorisation
 - Ready-to-send

Validation and message disposition

The following formats of messages influence the message validation and disposition process:

- **Messages in the CAS format**

In addition to settings in the message partner and permission profile, CAS messages may contain information governing the disposition of the message.

- **Messages in non-CAS format**

For non-CAS messages, the Application Interface uses the result of validation checks combined with the settings in the message partner profile and permission profile to dispose the message.

Operator profile for a message partner

Each message partner profile has an associated operator profile, specified in the **Profile Name** field of the **File Transfer** area.

The profile that is associated with the message partner controls the activities that the message partner is permitted to perform. Specifically, the profile is a collection of rules that Alliance Access uses to govern how to dispose a message that received from a back-office application. This profile entitles the message partner to create messages in Alliance Access. A default operator profile, **R7.1_MsgPartner**, is available for use with message partners.

Note	To use the Dispose function for received messages, the operator profile that is associated with the message partner must include the action Dispose Message for the Application Interface application. By default, this action is already selected in the default profile, R7.1_MsgPartner .
-------------	---

R7.1_MsgPartner

When Alliance Access is installed, each message partner receives the default operator profile **R7.1_MsgPartner**. The default permissions in the **R7.1_MsgPartner** profile can be changed to suit the business activities of your site.

It specifies no constraints on the setting of the following attributes:

- Destinations allowed to create messages
- Message Types (MTs) that are accepted by the message partner
- Currencies used
- Permission to bypass message verification
- Permission to bypass message authorisation
- Permission to "dispose" a message directly to a routing point

A.3.2 Levels of Validation

Purpose

After the Application Interface passes the message to the routing software, a check is made to see whether message text validation must be applied.

Alliance Access applies a generic message validation and extraction process to messages that it receives from a message partner in Network Dependent Format (NDF), to ensure that the message is syntactically and semantically correct.

This validation involves a structural checking and extraction of all message blocks (1, 2, 3, 4 and 5), as well as a block content validation (excluding the message text block, that is, block 4). This is the absolute minimum requirement for a message to be added to the Alliance Access database. If Alliance Access finds that the structure and the content of these blocks are syntactically incorrect, then the message fails validation. In this case, an event is logged in the Event Log and then message is discarded from the system. Alliance Access closes the session that was responsible for delivering the message.

Note The generic check does not validate the contents or structure of the text block.

You must choose carefully the validation level to use. For instance, you can select **Minimum** validation for the batch input of messages that are prepared on your back-office application because the source of them is known. However, you can select **Medium** validation for the batch input of messages from an obscure or infrequent source, as the risk is greater.

Validation levels and uses

The **Validation level** field offers the following options for validation of the text block of a message (the default is **Medium**):

Validation level	Description
No Validation	Alliance Access does not parse or validate the message, and as a result, keywords are not extracted. If you want to route messages based on routing keywords, such as the transaction reference number (TRN), then do not select No Validation . For more details about the impact of using this value, see "Impact of using No Validation " on page 760.
Minimum	Alliance Access performs the validation and extraction of some keywords, like currency , value , amount , value date , the field MF20 , and so on. To route FIN messages based on the Transaction Reference Number (TRN) keyword, you must specify at least Minimum as the validation level.
Medium	Alliance Access performs a syntactical validation at the field level. It checks for the presence of mandatory fields, keyword validation, limits, ranges of values, and so on. If a message fails Medium validation during an Interactive session, then a negative reply is generated and sent to the message partner.
Maximum	This level is provided to allow for a possible future level of message validation. Today this level performs the same checks as Medium validation.

Impact of using **No Validation**

Keywords are not extracted when the **No Validation** level is used.

Therefore, an operator who has permissions restricted by the values of certain keywords can still open messages in the Verification and Approval queues even though those messages have values outside the permitted range of values. For example, if an operator is limited to an amount of N, messages with amounts greater than N may appear in the list of messages.

Even though keywords are not extracted when **No validation** is used, if you have configured Alliance Access to generate the message UUMID for FIN messages from the Transaction Reference Number (TRN), then Alliance Access performs a simple syntactic search on Block 4 and extracts the content of the first field 20, or any variation of field 20 (for example, 20C). If the field is 20C, then Alliance Access also extracts the first subfield, and the TRN may appear in the UUMID but you cannot route on the TRN. If the field content has more than 16 characters, then the TRN is not added to the UUMID. When you install a Message Syntax Table, you can

configure Alliance Access to generate the message UUMID from the Transaction reference number.

Validation of messages in CAS format

If the format of the received message is CAS Network Independent Format (NIF), then no generic check is applied.

The messages that are received using the CAS protocol have a field in the APDU **minValidation** that specifies the validation level that is requested for the message. If a value for this field is present, then it overrides the setting of the **Validation level** field. If no value is present in this field, then the value of the field is used.

Calculation of common reference

If the configuration parameter **Common Ref Calculation** is set to **No**, then Alliance Access does not calculate the Common Reference in field 22. In this case, the **Validation level** is ignored and a NAK may be received if field 22 of the message contains incorrect information.

A.3.3 Message Validation for RJE, DOS-PCC, and MERVA/2 Messages

Overview

Validation of these messages starts with the syntactical check that Alliance Access performs on the basic block structure of the message. Alliance Access uses the **Validation level** is specified in the **Reception** area of the message partner profile.

If the block structure of the message is found to be syntactically incorrect, then Alliance Access completes the message and store it in the database with format **internal**.

If the block structure is syntactically correct, then the level of validation requested on the text block (block 4) is checked, as follows:

- If the check reveals that minimum validation was requested, then the message is proved acceptable.
- If the check reveals that intermediate validation of the text block was requested but has failed at this level, then the message is proved unacceptable and is rejected.

However, if **Message modification** in the message partner profile is set to **Allowed**, then Alliance Access moves the message to the text modification queue (**_MP_mod_text**). This allows an operator with the appropriate permissions to modify the message.

- The maximum validation level is not implemented in this version. If selected, intermediate validation is imposed.

Checks after message is acceptable

If the validation checks prove that the message is acceptable, then Alliance Access checks the following in the operator profile that is associated with the message partner profile:

- Does the message partner have the permission to create a message?
- Is the specified destination permitted (own destinations)?
- Is the specified message type permitted?
- Is the specified currency allowed?

The operator profile is specified in the **Profile Name** field of the **File Transfer** area.

If any of these validation checks fail, then the message is rejected and completed.

If the result of each check is positive, then Alliance Access checks the value of the **Routing** files in the **Reception** area, and performs one of the following actions:

- **Dispose**: routes the message according to the bypass permissions that are preset in the message partner profile. See the section, "Routing based on bypass parameters" on page 762.
- **Route**: routes the message to the preferred network interface of the correspondent.

Note To use the **Dispose** function for received messages, the operator profile that is associated with the message partner must include the action **Dispose Message** for the Application Interface application. By default, this action is already selected in the default profile, **R7.1_MsgPartner**.

Routing based on bypass parameters

Bypass Verification	Bypass Authorisation	Route Message To
No	No	Verification Queue
No	Yes	Verification Queue
Yes	No	Authorisation Queue
Yes	Yes	Preferred network interface of correspondent

A.3.4 Message Validation for XML Messages

Overview

For XML messages (file format XML), the payload must be compliant with the Standards XML structure, and contain the `<Document>` element.

Any XML message for which no corresponding MX standard is installed in Support is rejected. This does not apply to messages in the AnyXML format, which are only validated as being a well-formed XML document.

There is no validation of the content of the payload in either format.

Checks after message is acceptable

If the validation checks prove that the message is acceptable, then Alliance Access checks the following in the operator profile that is associated with the message partner profile:

- Does the message partner have the permission to create a message?
- Is the specified destination permitted (own destinations)?
- Is the specified SWIFTNet Service permitted?

The operator profile is specified in the **Profile Name** field of the **File Transfer** area.

If any of the checks fail, then the message is rejected and completed.

If the result of each check is positive, then Alliance Access routes the message to the `_SI_To_SWIFTNet` queue. In this case, Alliance Access does not check the the bypass permissions that are preset in the message partner profile.

A.3.5 Message Validation for CAS Messages

Overview

This section describes how Alliance Access validates messages that are in CAS format.

A.3.5.1 Overview of Message Validation for Messages in CAS Format

Overview

CAS messages do not undergo the block and syntactical checks that are applied to non-CAS messages for SWIFT format (NDF). Only the validation requested on the text block (block 4) is checked.

Validation on text block

The validation requested on the text block (block 4) is checked, as follows:

1. If the validation of the text block failed, then the message is rejected.

However, if the message partner profile or relevant APDU field states that the message is modifiable, then the message is moved to the text modification queue (`_MP_mod_text`).

Validation level	Validation checks and results
Minimum	If the check reveals that minimum validation was requested, then the message is proved acceptable.
Intermediate	If the text block was requested but has failed at this level, then the message is rejected. However, if the message partner profile or relevant APDU field states that the message is modifiable, then the message is moved to the text modification queue (<code>_MP_mod_text</code>).
Maximum	The maximum validation level is not implemented in this release. If it is selected, then the Alliance Access applies intermediate validation.

3. Messages the Alliance Access receives using the CAS protocol have an optional field in the APDU *minValidation* that specifies the validation level for the message. When a value for this field is present, it overrides the setting of the **Validation Level** button in the message partner profile. If no value is present in the APDU field, then the value of the button is taken.

Warning If the APDU *minValidation* is set, then minimum validation on the message is carried out, that is, the message is accepted.

Checks after message is acceptable

If the validation checks prove that the message is acceptable, then Alliance Access considers the settings in both the message APDU fields. Alliance Access also checks the operator profile that is associated with the message partner profile, to manage the disposition of the message.

In addition, a message in CAS NDF or CAS NIF format is disposed according to a combination of the following APDU fields:

- **targetApplication**
`targetApplicationRule`

- targetRoutingPoint
- **networkAttribute**
 - networkApplicationName
 - networkPart1
 - networkPart2
 - networkPart3
- **dispositionState**

The subfield `networkApplicationName` specifies the communication interface responsible for handling the message, that is, Application Interface or SWIFT Interface.

Depending on the interface specified, the fields `networkPart1`, `networkPart2` and `networkPart3` identify the message partner, the sending or receiving logical terminal for SWIFT Interface, as follows:

networkApplicationName	networkPart1	networkPart2	networkPart3
applicationInterface	MAPID	-	-
swiftInterface	Sending logical terminal	Receiving logical terminal	-

For a more details explanation of how the combination of these fields are used to route messages in CAS format see:

- "Disposition based on APDU fields" on page 764
- "Disposition Actions for Messages in CAS Format" on page 765

Disposition based on APDU fields

Basically, Alliance Access performs four sequential checks on the APDU fields, to determine how to dispose the message that is in CAS format:

1. Is `internalRouting` specified in the field labelled `targetApplicationRule`?

If yes, Alliance Access checks the permissions of the operator profile that is associated with the message partner profile, and if acceptable, the message is created and routed according to the routing rules at the inbound queue of the Application Interface.

Note Alliance Access does not changed whether the message partner has the permission to bypass verification and authorisation.

2. Is the term `routingPoint` specified in the field `targetApplicationRule`, and does the field labelled `targetRoutingPoint` request a particular routing point in Alliance Access?

If yes, then it is important that the requested routing point exists.

Alliance Access checks the permissions of the operator profile that is associated with the message partner profile to determine whether the message partner has the "Dispose" function assigned to it.

If yes, then the message is moved to the requested routing point. This must be an "allowed target routing point" or an exit point as specified in System Management Application (SMA). No other checks are carried out.

3. Is the term `cBTApplication` specified in the field `targetApplicationRule`, and is the disposition state of the message specified in the field labelled `dispositionState`?

The available values for *dispositionState* include:

- *Fix*. This value indicates the message must be sent to the text modification queue. No checking of the permission profile is performed except the permission to modify a message. Permission to modify a message may be specified in either the message partner profile or the message APDU field *modifyAllowed*. A specification in the APDU takes precedence.
 - *Verify*. This value indicates that the message must be sent to the Verification queue. No checking of the permission profile is performed except the permission to create a message.
 - *Authorise*. This value indicates that the message must be sent to the Authorisation queue. The permission for bypass verification is checked. If the permission is set, then the message is routed to the Authorisation queue. If the permission is not set, then the message is routed to the Verification queue.
 - *Ready*. This value specifies routing according to the application specified in the field *networkApplicationName*. If *cBTApplication* is specified in the field labelled *targetApplicationRule*, then *networkApplicationName* will specify the Alliance application as either *swiftInterface* or *applicationInterface*. The permissions for bypass authorisation and bypass verification are checked.
 - *Cancel*. The message is completed.
 - For the SWIFT Interface Application (SIA), the message is routed to the **_SI_to_SWIFT** queue.
 - For the Application Interface, the message is routed to the first exit point assigned to the message partner specified as MAPID in *networkPart1*.
4. If none of the previous three checks apply, **and** the message is in input format then AI attempts to route the message as far as it can, based upon the default disposition or routing settings in the message partner profile and the permissions set in the permission profile, thus:
- If the permission for bypassing verification is not set, then the message is directed to the Verification queue.
 - If the permission for bypassing authorisation is not set, then the message is directed to the Authorisation queue.
 - If the message is in the SWIFT format and both of the above permissions are set, then the message is routed to the **_SI_to_SWIFT** queue. In all other cases, the message is completed.

A.3.5.2 Disposition Actions for Messages in CAS Format

Overview

Alliance Access moves the received messages in the CAS network-independent format (NIF) according to the combination of values for:

- *dispositionState*
- *targetApplicationRule*
- *networkApplicationName*

dispositionState	targetApplicationRule	networkApplicationName	Permissions or message partner profile settings	Action
omitted or any valid value	omitted	omitted or applicationInterface or swiftInterface	not applicable	according to default disposition set in message partner profile or Run Session or Start Session window
cancel	cBTApplication	omitted or applicationInterface or swiftInterface	not applicable	complete the message
fix	cBTApplication	omitted or applicationInterface or swiftInterface	not applicable	send to _MP_mod_text queue
verify	cBTApplication	omitted or applicationInterface or swiftInterface	not applicable	send to _MP_verification queue
authorise	cBTApplication	omitted or applicationInterface or swiftInterface	No permission to bypass Verification on Msg Type or Currency code given	send to _MP_verification queue
authorise	cBTApplication	omitted or applicationInterface or swiftInterface	Permission to bypass Verification on Msg Type and Currency code is given	send to _MP_authorisation queue
ready	cBTApplication	omitted or applicationInterface or swiftInterface	No permission to bypass Verification on Msg Type or Currency code is given; and No permission to bypass authorisation on Msg Type or Currency code given.	send to _MP_verification queue send to _MP_authorisation queue
		applicationInterface	Permission to bypass Verification on Msg Type and Currency code is given. and Permission to bypass Authorisation of Msg Type and Currency code is given.	send to first exit point assigned in the MP profile
		swiftInterface	Permission to bypass Verification on Msg Type and	send to _SI_to_SWIFT queue

dispositionState	targetApplicationRule	networkApplicationName	Permissions or message partner profile settings	Action
			Currency code is given. and Permission to bypass Authorisation of Msg Type and Currency code is given.	
omitted or any valid value ignored	internalRouting	omitted or applicationInterface or swiftInterface		route according to defined routing
omitted or any valid value ignored	cIFPreferred	omitted or applicationInterface or swiftInterface		route according to settings made in the Correspondent Information File
omitted or any valid value ignored	routingPoint	omitted or applicationInterface or swiftInterface	Permission to move messages is given	move to the routing point specified in targetRoutingPoint

Appendix B

Cold Start

B.1 General Information

What is a cold start ?

Cold start is an exceptional scenario where the SWIFT/SWIFTNet service is restarted from an empty or a zeroed state some time after a fatal failure.

The status of the FIN and store-and-forward services must be checked on www.swift.com to identify a cold start.

In most cases, the unavailability of a service is due to local problems or connectivity issues.

These problems can be diagnosed within Alliance Access using the Monitoring and Configuration GUI packages.

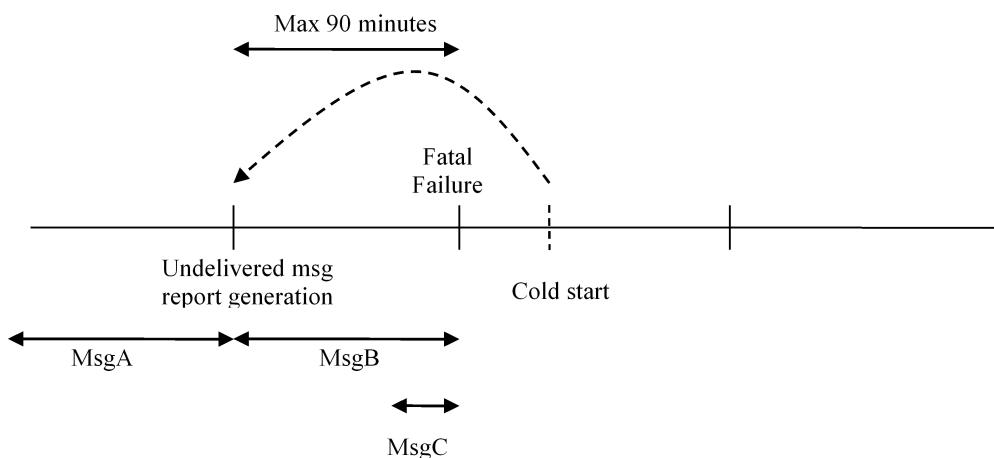
If the situation cannot be resolved, then contact Support.

What is affected by a cold start ?

In a cold start situation:

- FIN (and/or store-and-forward) does not attempt to deliver messages that were not delivered at cold start time.
- Historical data about message delivery status prior to the cold start is not available after cold start, with the exception of the last Undelivered Message Report (MT 082 for FIN) and Unsolicited Undelivered Traffic Report (xsys.005.002.01 for store-and-forward) that were generated before the event that led to a cold start. After a cold start, these are the first messages sent to Alliance Access . They are generated at most 90 minutes before the event that led to the cold start.
- All session and sequence related counters (ISNs and OSNs) are reset after the FIN cold start for all the LTs associated to a zone affected by the FIN cold start.

The following figure shows the different categories of FIN or store-and-forward messages affected by a cold start:



The following messages should be resent to SWIFT/SWIFTNet following a cold start:

- **MsgA**

messages present in the undelivered message report which have not yet been delivered to the correspondent. Alliance Access will check if these messages have been delivered since the report was generated. Messages not delivered will be resent with the Possible Duplication Emission indication.

- **MsgB**

messages sent after the undelivered message report generation which have been acknowledged by SWIFT/SWIFTNet but which have not yet been delivered to the correspondent. Alliance Access will resend these messages with the Possible Duplication Emission indication.

- **MsgC**

messages sent to SWIFT/SWIFTNet but for which a network acknowledgement is still to be received.

These messages will automatically be resent by Alliance Access using the existing SWIFT/SWIFTNet Interface recovery mechanism

Cold Start Configuration

The cold start activation is controlled by global system configuration parameters (**Activate cold start** and **FIN CS time margin** (see "Cold Start Configuration Parameters" on page 772)).

Additionally, there is the option to include/exclude a FIN Copy service in the cold start. Cold start activation/deactivation is common to FIN and store-and-forward.

In a fresh installation, cold start is active by default and no FIN Copy service is included.

In a patch upgrade, cold start is active by default and the selection of included FIN Copy services is preserved.

You can change these defaults as a post installation step.

(FIN and Store-and-forward) undelivered message/traffic report processing

Upon reception of each and every undelivered message/traffic report, Alliance Access:

1. **First** reactivates for re-transmission the messages referred to in the report
2. **Then**, reactivates the messages not present in the report and that were sent after the report generation date and time (minus a time margin for FIN messages). This second step does not require any manual action by an operator and is executed for an LT (or a BIC8 for store-and-forward) once all messages referred to in all reports covering that LT (BIC8) have been processed. This differs from what was done in FIN cold start before 7.1.10: indeed the processing of messages sent after the report generation date/time was only performed after manual confirmation by an operator that all MT 082 reports for all LTs were received.

Only original instances of messages are involved in cold start processing.

Cold start event logging is adapted to this new 'Automatic post-report' processing. In particular, the results of reactivation are logged for each message treated.

Recreation of input/output channels (store-and-forward only)

Alliance Access recreates the non-generic Input Channels and Output Channels that are defined in SWIFTNet Emission or Reception Profiles for a BIC8, upon reception of the first Unsolicited Undelivered Traffic Report (xsys.005.002.01) for that BIC.

Cold start report (FIN and Store-and-forward)

There is no dedicated cold start reports any more as the details of each message reactivation (whether successful, skipped or failed) are logged in the event journal together with the LT (for FIN messages) or Session Holder (for store-and-forward messages) involved.

Miscellaneous

- Operators can perform mass manual operations on messages in the _MP_recovery queue, namely they can authorise, complete, ... all messages meeting the filtering criteria without having to select them all. New filtering criteria are implemented in the _MP_Recovery queue in support of mass operations ('From BIC' and 'Service').
- New fields (PDE fields, MUR) are added to message lists in the Message Search application (Message Management GUI package)
- Users can identify original instances automatically reactivated to _MP_Recovery by Alliance Access as a result of a cold start and are able to prevent the related network ACKs to go to the back office applications.
- Customers can simulate a test cold start by triggering cold start MT 082 and xsys. 005.002.01. See "Cold Start Simulation" on page 780 for details.

Management of time zone differences and of clock misalignment (FIN only)

The FIN cold start processing of MT 082 is enhanced to better take into consideration the possible time difference between the Alliance Access system local date/time and the SWIFT date/time.

This is done by:

- storing the date and time at which Alliance Access receives the SWIFT Ack
- enabling more flexibility in defining a time margin (via global system configuration parameter)

Note For InterAct store-and-forward and FileAct store-and-forward , clock misalignment is not an issue as the SWIFTNet time stamp is associated with each message.

For real-time this is not required, as the messages are exchanged directly with the correspondent and the delivery status of the message is always known.

B.2 Cold Start Events

Overview

- Events related to cold start message processing or to cold start Input Channel/Output Channel recreation have their application service name set to 'Cold start'.
- Events are logged upon reception of the first MT082 for a specific LT or the first xsys. 005.002.01 for a specific BIC8
 - Event 2160 is logged when the first MT082 is received for an LT.
 - Event 2215 is logged upon reception of the first xsys.005.002 for a specific BIC8.
- Events are logged when MT082/xsys.005.002.01 post processing starts for an LT or for a BIC8 (when all MT082 messages or all xsys.005.002.01 messages have been received and processed for an specific LT/BIC8).

- Event 2164 is logged when Alliance Access starts looking for acked undelivered FIN messages sent after the date/time of the MT082 minus the FIN CS time margin, and to reactivate them to _MP_recovery.
- Event 2216 is logged prior to each BIC8 post processing. It indicates Alliance Access starts looking for acked undelivered store-and-forward messages sent after the date/time of the xsys.005.002 reports related to that BIC8.
- During MT082/xsys.005.002.01 processing or postprocessing, events are logged for each message not found in the database, each message whose reactivation failed, each message whose reactivation succeeds and each message whose reactivation is skipped (because the message was delivered)
 - Event 2162 is logged when a message referred to in the MT082 or xsys.005.002.01 can not be found in the Alliance Access database.
 - Event 2163 is logged when message reactivation fails.
 - Event 2213 is logged when a message is skipped for reactivation as it is already delivered to correspondent or the FIN Copy service is not included in cold start.
 - Event 2214 is logged for each FIN or Store-and-FF message successfully reactivated.
- Events are logged when post-processing is finished for an LT (or for a BIC8). Such events contains counters of messages successfully reactivated, messages not found in the database, messages whose reactivation was skipped and messages whose reactivation failed, globally during MT082 (or xsys.005.002.01) reports processing **and** post-processing for that LT (or BIC8).
 - Event 2165 is logged when Alliance Access has finished treating acked undelivered FIN messages sent after the date/time of the MT082.
 - Event 2217 is logged when xsys.005.002 post-processing is finished for a BIC and provides counters of messages processed.
- Event 12023 is logged when a FIN Copy service is installed, to advise synchronising with the Central Institution on the inclusion/exclusion of the service in cold start processing.
- Event 12024 is logged when a FIN Copy Service is updated (changes to the value of the 'Include in cold start' field).
- Event 28153 is logged when an Input Channel is successfully recreated following a cold start
- Event 28154 is logged when Input Channel recreation fails
- Event 28155 is logged when an Output Channel is successfully recreated following a cold start
- Event 28156 is logged when Output Channel recreation fails

Note Reactivate a message to _MP_Recovery means:

- the message status is changed from 'Completed' to 'Live'
- the original instance of the message is moved to _MP_recovery

Only non-archived 'Completed' messages can be reactivated to _MP_Recovery

Searching the Event Journal

The **Cold_start** value is available in the **Other** tab of the **Event Journal - Search criteria** GUI screen (Application/service list box when using Alliance Workstation).

The **Cold_start** value is available in the **Specific** tab of the **Event log - Search criteria** GUI screen (Application list box when using Alliance Access Configuration package on the Alliance Web Platform).

Routing keywords

As part of the support of cold start by Alliance Access, a new routing keyword (**Mesg_inst_CS_reactivated**) is implemented in Alliance Access and can be used for FIN, InterAct and FileAct messages. It exposes the '**Inst_is_CS_reactivated**' message instance field.

In particular, this routing keyword can be used, to avoid sending the SWIFT ACKs of message (original) instances reactivated and resent to SWIFT as a result of cold start, to the Back Office applications which can not manage receiving two ACKs for the same message.

B.3 Cold Start Configuration Parameters

To configure Alliance Access to enable cold start processing, the system configuration parameter **Activate cold start** must be set to **Activated**.

The time margin (in minutes) applied by AccessAlliance Access when performing cold start MT082 post-processing can be set with the **FIN CS time margin** message parameter.

The only permission required to modify these parameters is the System Management permission.

FINCopy profiles can also be included (or excluded) from the cold start processing. For details, see "FINCopy Services Setup" on page 778.

B.4 Input and Output Channel Management

Upon reception of the last xsys.005.002.01 related to a BIC8, Alliance Access automatically recreates the following channels:

- The non generic Input Channels that are defined in Alliance Access Emission Profiles for that BIC8. They are identified by their name that is different from **<BIC8>_generic** and different from **<BIC8>_generic!p**. Log event 28153 in case of success or event 28154 in case of failure.
- The Output Channels that are defined in Alliance Access Reception Profiles for that BIC8 and whose name does not match the name of the queue associated to that Reception Profile. Log event 28155 in case of success or event 28156 in case of failure.

The Output Channels recreated by Alliance Access are put in Exclusive mode. If you had set these Output Channels to Shared mode before the cold start, you need to change the mode from Exclusive to Shared manually.

Note	Channel recreation is done by the SNSS process.
	The channel recreation process uses the Primary SAG connection of the EP(s)/RP(s) to which the channel being recreated belongs (1). If that SAG connection is not available, there is no automatic switchover to the Secondary SAG connection of the Emission/Reception profiles, Input/Output Channel recreation fails and event 28154 or event 28156 is logged. Note that if the channel does not belong to any Emission/Reception profiles, then it is not recreated (as it is not used). Note that if a channel is shared and therefore belongs to more than one Emission/Reception profile, these profiles share the same connection settings.

B.5 FIN Message Processing

This processing occurs each time an unsolicited undelivered message MT082 report (with 'CS' in tag 301) is received AND the 'Activate cold start' system configuration parameter is 'Activated'.

Each MT082 reports on one LT. The same LT can be covered by several MT082s

Sequence of events

1. If the MT082 is the first one for that LT, event 2160 is logged.
2. **Processing (original) instances referred to in the MT082 for retransmission**

For each (original) instance referred to by its MIR (tag 335) in the MT082, if one of the following criteria is met, Alliance Access skips the (original) instance and logs event 2213 :

- The (original) instance's last Emission Appendix.ReceiverDeliveryStatus is 'Delivered' or 'Delayed Receiver NAK'.
- The FINCopy service code is present but is not included in the cold start processing.

For each (original) instance referred to by its MIR (tag 335) in the MT082, and that meets ALL the following criteria:

- The (original) instance's last Emission Appendix.ReceiverDeliveryStatus is 'Unknown' or 'Receiver Overdue', 'Released by Central Institution' or 'Receiver Aborted'.
- The FINCopy service code, if present, is included in the cold start processing.
- The (original) instance's last Emission Appendix.NetworkDeliveryStatus is 'Network Ack'.

If the (original) instance is not archived and is 'Completed', the following processing takes place:

- reactivate it to _MP_Recovery (meaning that its status changes to 'Live' and it is moved to _MP_Recovery) with ReactivationComment set to "Cold Start re-transmission".
- log event 2214
- set its 'Inst_is_CS_reactivated' field to yes.
- add an intervention to the (original) instance with the following attributes:
 - Message LastModifier: SYSTEM
 - Intervention.Category: Routing

Intervention.Name: Instance Reactivated
Intervention.Text: "Reactivated in rp _MP_Recovery by operator SYSTEM.
Operator comment: Cold Start re-transmission.

Note If the MT082 is empty, no (original) instance is identified for retransmission in this step.

3. Processing (original) instances sent after MT082 generation date/time, for retransmission

This step is only executed if the MT082 is the last MT082 for the LT.

1. Alliance Access logs event 2164
2. For each message instance in the database that meets ALL the following criteria, the same processing as in step 2 takes place:
 - The instance is an original instance.
 - The instance was sent after the date and time (that is expressed in GMT) of the MT082 (based on the instance's last Emission Appendix "ACK Reception Date Time" field, which is also expressed in GMT) minus the time margin defined in the 'FIN CS time margin' global system configuration parameter.
 - The instance meets the criteria listed in step 2.
3. When all (original) message instances are processed for the LT, event 2165 is logged.

4. Error Handling

If during steps 2 and 3 no message instance corresponding to a MIR can be found, event 2162 is logged

If the message (original) instance is archived OR if it is not archived and is still Live and is not in _MP_Recovery:

- it cannot be reactivated.
- event 2163 is logged.

If the message (original instance) is still Live and is already in _MP_Recovery, it is not reactivated (as it is already in the _MP_Recovery queue) and no event is logged.

5. PDE Handling

As the message (original) instances selected for retransmission already have at least one emission appendix, Alliance Access will add a PDE to it when re-sending it to SWIFTNet.

The following table shows the conditions used to identify whether a message (original) instance must be re-sent in the context of FIN cold start

The following table shows the conditions used to identify whether a message (original) instance must be re-sent in the context of FIN cold start:

Message (original) instance in MT082?	Receiver Delivery Status	Network Delivery Status	FINCopy service present and excluded from cold start?	Time > (MT082 report -Time Margin)	Cold Start?
Yes	Unknown	Network Ack			Yes
Yes	Receiver overdue	Network Ack			Yes
Yes	Delivered to receiver	Network Ack			No
Yes	Receiver aborted	Network Ack	No		Yes
Yes	Delayed receiver NAK	Network Ack			No
Yes	Released by Central Institution	Network Ack	Yes		No
Yes	Released by Central Institution	Network Ack	No		Yes
No	Unknown	Network Ack	No	Yes	Yes
No	Receiver overdue	Network Ack	No	Yes	Yes
No	Delivered to Receiver	Network Ack			No
No	Receiver aborted	Network Ack	No	Yes	Yes
No	Delayed receiver NAK	Network Ack			No
No	Released by Central Institution		Yes		No
No	Released by Central Institution	Network Ack	No	Yes	Yes
No	Unknown	Not Network Ack			No
No	Receiver overdue	Not Network Ack			No
No	Released by Central Institution	Not Network Ack			No
No	Unknown	Network Ack		No	No
No	Receiver overdue	Network Ack		No	No
No	Released by Central Institution	Network Ack		No	No

What to do next

Go to Message Recovery/Authorisation to authorize or complete the messages which were re-activated in that queue.

B.6 Store-and-forward Message Processing

This processing occurs each time an unsolicited store-and-forward Unsolicited Undelivered Traffic Report (xsys.005.002) is received AND the 'Activate cold start' system configuration parameter is set to 'Activated'.

Each store-and-forward undelivered message reports on one BIC8. Each BIC8 may be covered by several xsys.005.002 messages.

Sequence of events

1. Logging event

When the first xsys.005.002 message is received, event 2215 is logged.

2. Processing (original) instances for retransmission

For each (original) instance referred to by its SwiftRef (IA)/TransferRef (FA) in the xsys.005.002 that meets the following criteria:

- The last Emission Appendix.ReceiverDeliveryStatus is 'Delivered' or 'Delayed Receiver NAK'

The instance is skipped and event 2213 logged.

For each (original) instance referred to by its SwiftRef (IA)/TransferRef (FA) in the xsys.005.002 that meets BOTH the following criteria:

- The (original) instance's last Emission Appendix.ReceiverDeliveryStatus is 'Unknown' or 'Receiver Overdue', 'Released by Central Institution' or 'Receiver Aborted' AND
- The (original) instance's last EmissionAppendix.NetworkDeliveryStatus is 'Network Ack'

If the (original) instance is not archived and is 'Completed':

- reactivate it to _MP_Recovery (meaning that its status changes to 'Live' and it is moved to _MP_Recovery)
- set its 'Inst_is_CS_reactivated' field to yes
- event 2214 is logged
- an intervention is added to the message, with the following attributes

```
Message LastModifier: SYSTEM
Intervention.Category: Routing
Intervention.Name: Instance Reactivated
Intervention.Text: "Reactivated in rp _MP_Recovery by operator SYSTEM.
Operator comment: Cold Start re-transmission.
```

Note If the xsys.005.002 is empty, no (original) instance is identified for retransmission in this step.

The StoreAndForwardReference in the xsys.005.02.01 is the SnFRef of the message or the file that was not delivered. In the case of FileAct, the local suffix C is not present, because only the signed part is provided.

3. Processing (original) instances sent after xsys.005.002 generation date/time, for retransmission

This step is only executed if the xsys.005.002 is the last xsys.005.002 for the BIC8.

Event 2216 is logged.

For each original store-and-forward message instance in the database that meets the criteria listed in step 2 and the instance was sent after the xsys.005.002 generation date/time (based on the messages store-and-forward Input Time), processing is the same as in step 2.

4. Error handling

If during step 2 and step 3 no instance corresponding to the SwiftRef (IA) or TransferRef (FA) can be found, event 2162 is logged.

If the message (original) instance is archived or if it is not archived and is still Live, it can not be reactivated and event 2163 is logged.

5. PDE handling

As the message (original) instances selected for retransmission already has at least one emission appendix, a PDE is added when re-sending it to SWIFTNet.

What to do next

Go to Message Recovery/Authorisation to authorize or complete the messages which were re-activated in that queue.

B.7 Searching for Cold Start Messages

In support of cold start, the changes have been made to the Message Search in the Message Management application on Alliance Web Platform.

Filtering criteria

You can now specify filtering criteria to search for messages whose original instance has automatically been reactivated to _MP_Recovery by Alliance Access following a cold start:

- **Label:** 'Re-activated due to cold start'
- **Values:** Yes, No, Any
- Default value: Any

Note The filtering criteria is a drop-down field in the **Instances Location** tab.

Procedure

1. On Alliance Web Platform, select Message Search in the Message Management application.
2. From the drop-down field in the **Instances Location** tab, select **Re-activated due to cold start**.
3. In the **Values** field, select one of the following:
 - **Yes** to display messages whose original instance has been automatically reactivated to the _MP_recovery queue.
 - **No** to display messages whose original instance has **never** been automatically reactivated to the _MP_recovery queue.

Any to display messages based on the other selection criteria and irrespective of whether or not they were ever automatically reactivated to _MP_recovery following a cold start

4. Click

B.8 Message Details and Reports

When the original instance of a message has been reactivated to _MP_recovery automatically by Alliance Access as a result of a cold start, the **Status** field of the **Header** tab of the message details screen shows Re-activated due to cold start. It also appears in the **Header** section of the detailed report.

Note The information is not shown in Message lists or summary reports.

FIN messages

The **Ack reception date/time** field is displayed with label **ACK Reception date/time (GMT)**. It also appears in the detailed reports.

Note The information is not shown in Message lists or summary reports.

B.9 FINCopy Services Setup

Alliance Web Platform

In the Configuration package, SWIFTNet Interface, FIN Copy Profiles screen, a new check box field **Included in cold start** is available. It is used to indicate whether a specific FIN Copy service must be included or excluded in/from cold start processing. By default, FIN Copy services are not included in Cold Start.

This field can be updated in housekeeping mode or in operational mode.

Note When installing a new FIN Copy service, it is initially set to 'No'.

B.10 What To Do Before the First Login/Select

Procedure

1. Disable automatic login/select.

As the automatic login/select to FIN prevents controlling the messages that Alliance Access re-sends when the ISN/OSN is reset, it is better to set the operation mode of the logical terminals to Manual.

For more information, see the [System Management Guide](#).

2. Manage the impact of the ISN/OSN reset.

If the ISN and OSN present in Alliance Access before the FIN cold start were close to zero, then the reset to zero of these ISN and OSN has the following impact:

- When performing a message search, you can have repeating session and sequence numbers, but the transmission times are different (before and after the cold start)
 - Retrievals will only return the messages that have been processed by FIN after the cold start
 - The message partners defined in the Application Interface send duplicate session and sequence numbers in the transmission reports. The back-office applications must be dealing with this.
3. Deactivate any automatic message archiving to allow the re-sending of messages that have not been delivered yet. This is only required if the retention period for your message archiving is set to one day.

For more information, see the [System Management Guide](#).

4. Deactivate any FINCopy service where the Service Administrator has instructed that messages must not be re-sent in the event of a FIN cold start. In case of doubt, contact your Service Administrator.

For more information, see the [System Management Guide](#).

5. Identify on www.swift.com when the special undelivered message (UNDELV) report was generated.

This report is in the form of the MT 082 Undelivered Message Report at a Fixed Hour, and reflects the situation no more than 30 minutes before the event that led to the FIN cold start. The content of this special UNDELV report, which contains the value CS in tag 301, must be compared with the information contained in the most recent UNDELV report that you receive during normal FIN processing. If you have selected to receive undelivered message reports at the cut-off time of the receiver's country (MT 083), then review the undelivered message reports for all countries, to determine the appropriate report(s), to use.

If there is any doubt about which UNDELV report to use, then it is always safe to use the special UNDELV report. This report is the first UNDELV report that you receive after the cold start.

B.11 Performing the First Login/Select

Procedure

1. Log in all the logical terminals that were used for sending the messages.
2. Ensure that the logical terminals for which the Select is performed are selected for output, and that the logical terminal directed queue (LTDIR) is selected. This is required as the first messages that will be delivered after restoring the FIN service will be the MT 082 messages that have been generated after the cold start. The MT 082 is a logical terminal directed message.

When performing the **Select** command on a logical terminal in the SWIFT Interface application, ensure that:

- the **Mode** field has the value "Receive Only"
- the **LT Directed Queue** field has the value "Select" (to receive the MT 082 message).

For more information, see the [Daily Operations Guide](#).

B.12 Re-approving Messages to be Re-sent

Re-approve

You can easily locate the messages that require re-approval in the Message Approval application (on Alliance Workstation) or the Message Management GUI package (on Alliance Web Platform).

Select **Recovery** from the **View** menu on the **Verification - Message Approval** window.

The **Recovery - Message Approval** window appears.

B.13 Resuming Normal Operations

Description

When the messages identified for re-sending have been re-sent, you may have to perform some final tasks before resuming normal operations. These tasks are:

1. Enable automatic login/select.
If, originally, some logical terminals were operating in automatic mode, then they can now be reverted to that mode.
2. Activate any FINCopy service which was deactivated before the first login/select following the FIN cold start.

For more information, see the [System Management Guide](#).

B.14 Cold Start Simulation

Procedure for store-and-forward

1. **Activate Cold Start**

Make sure that Cold Start is activated. By default, Cold start is in activated mode. See "Cold Start Configuration Parameters" on page 772.

2. Send messages before xsys.005.002.01 execution time

Prepare a few store-and-forward, InterAct, and FileAct messages for pilot services. Some of them should have the notification requested set to true. Activate the emission profile, but do not open the reception profiles yet.

3. send xsys.004.001

Using MMA , send a xsys.004.001 using swift.snf.system!p to retrieve all messages not yet delivered with as delivery queue, the <bic8>_generic!p queue.

4. Open the <bic8>_generic!p reception queue.

Open the reception queue <bic8>_generic!p queue to receive the xsys.005.001.

You will receive an undelivery report. The execution time of the received xsys.005.001 will be used as execution time in the xsys.005.002.

5. Exchange of messages after execution of xsys.005.001

Send some more store-and-forward InterAct and FileAct messages. This will simulate the traffic received after the execution of a xsys.005.002.

6. Open the other involved reception queue

Open the reception queue to receive the above Interact and FileAct messages sent to yourself.

7. Wait until delivery reports are processed

Wait a few minutes to allow the delivery notification (xsys.011.) to be reconciled with the input message (could take up to the time specified in the Msg reconciliation cycle parameter).

Verify that instance notification deliveries are created for the messages for which a delivery notification has been received (could take up to the time specified in the Msg reconciliation cycle parameter).

8. Build the xsys.005.002

An example of the xsys.005.002 report is provided in the <installation directory> \MXS\batch_example\cold_start directory.

Modify the example xsys.005.002.01 xml message:

- Modify the Receiver DN (SAA:DN) and full name X1 (SAA:X1) tags with your own BIC (respect lowercase and uppercase) and replace Saa:SnFQueueName tag value and the Doc:ExctnTm tag with the ones present in the received xsys.005.001.01.
- Replace the content of the <Doc:UdlvrdMsgList> content of the xsys.005.001.01 one received in step 4 on page 781.

Uncheck "display expanded text" before copying the text.
- Update the length of the updated attached xsys.005.002.01 with the length of the signature + datapdu. Update the signature (LAU) or make sure you still get it padded with null characters if no LAU is required.

9. Create a routing rule

If you have not done so yet, define _TR_REC as a valid target for _AI_from_APPLI.

Duplicate the active schema and add for _AI_from_APPLI queue a new rule and select the new schema for this rule. The rule is used to send a copy of the MT 082 or xsys.005.002.01 to _TR_REC and complete the source instance.

Activate the new schema.

10. Create a Message Partner to process the xsys.005.002.01

Define and enable the Message Partner with Connection Method: File Transfer, Data Format : XML Version 2 Revision 3, Validation Level: No validation, and Routing Option: Route.

11. Process xsys.005.002

Run session for the above Message Partner to process the file containing the updated xsys.005.002.01 , wait _TR_REC to process it (could take at least the time specified in the Msg reconciliation cycle parameter).

Check the result in the event journal Event will be logged for each message which was successfully re-activated, or skipped or for which instance is not present in the database or for which the reactivation of the message instance has failed. Original instances of messages required to be resent will be moved to _MP_Recovery.

12. Message Recovery

From the Recovery queue, route the messages.

Depending on the selected option, the message will put in the _SI_to_SWIFTNet queue or completed.

Procedure for FIN

1. Activate Cold Start

Make sure that FIN Cold Start is activated. By default, Cold Start is in activated mode (see "Cold Start Configuration Parameters" on page 772).

2. Include FIN Copy service

If you are using FIN Copy services, then don't forget to flag or not the "Included in cold start" option of those FINCopy services; this is an option in the **FIN Copy Profile Details** window.

3. Send messages before Cold Start time (do not receive them yet)

Perform a Select FIN Input/Output for your Test & Training LT with only subset system and LT direct queue selected. Send some Test & Training messages (requesting delivery notification) to simulate a realistic traffic scenario.

4. Send an MT046

For your sending BIC, send an MT046 with Report type RT and your LT ID.

Wait until you have received the MT 066.

5. Select I/O

Select FIN I/O all subsets

You shall receive messages sent to yourself, plus the 011 system message for successful delivery of message to receiver.

6. Wait Fin Cold Start margin

Wait 15 min (default value for FIN CS time margin System Management parameter)

This will leave as well the time for _TR_REC to reconcile the delivery system messages with the related input messages

7. Exchange of messages after 082 generation

Send some additional T&T messages.

This will simulate traffic exchanges after the 082 report generation time.

8. Build the fin.082

In the <installation directory>\MXS\batch_example\cold_start, you will find an example of 082 report : Update the information present -the BIC12 sender in block 1 - the date in field 171 and the time in field 175 and replace all blocks {335...}, {108..} {431..} and {103:} with the ones present in the 066 received in step 4. Use RJE format.

9. Create a routing rule

If you have not done so yet, define _TR_REC as a valid target for _AI_from_APPLI;

Duplicate the active schema and add for _AI_from_APPLI queue a new rule and select the new schema for this rule. The rule is used to send a copy of the 082 or xsys.005.002.01 to _TR_REC.

Activate the new schema.

10. Create a Message Partner to process the MT082 (Allowed direction: FROM)

Use Message Partner with Connection Method : File Transfer , Data Format : RJE , with validation level : No validation and Routing option : Route.

11. Process 082

Run session for above Message Partner to process the file containing the 082 message.

Wait (could be long) that _TR_REC has finished to process it. Check the result in the event journal. Event will be logged for each message which was successfully re-activated , or skipped or for which instance is not present in the database or for which the reactivation of the message instance has failed. Original instance of messages required to be resent will be moved to _MP_Recovery.

12. Message Recovery

From the Recovery queue, route the messages.

Depending on the selected option, the message will put in the _SI_to_SWIFT queue or completed

Appendix C

Handling Double-Authenticated Messages with FINCopy

Overview

This appendix is intended for the Service Administrators at Central Institutions.

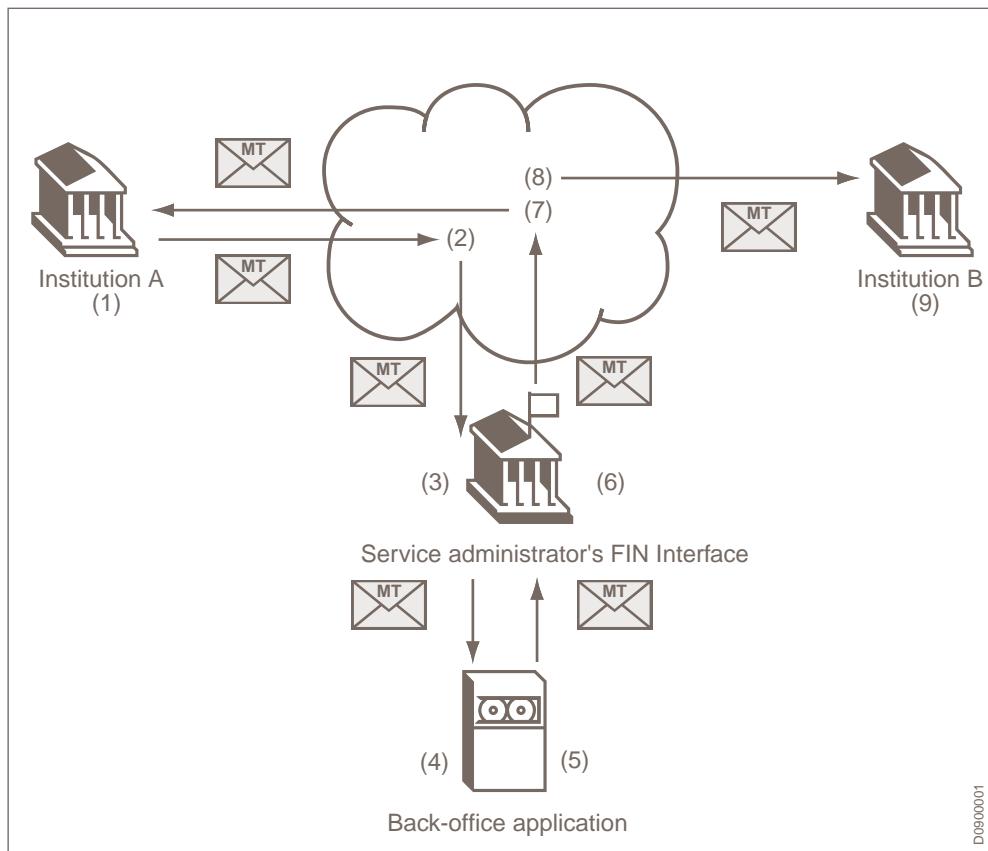
The appendix describes the impact on the back-office applications of the Service Administrators of FINCopy services, which exchange messages through Alliance Access. In particular, the appendix covers the methods of authentication and the signing algorithms that were introduced as part of SWIFTNet Phase 2. These new signing algorithms require the exchange of additional information containing special characters between the interface and the back-office application of the Service Administrators of FINCopy services.

Alliance Access does not support the formats RJE, MERVA/2, and CAS-1, in the scope of FINCopy services. All MQSA/MQHA formats are supported.

C.1 Message Flow

Introduction

This section describes the message flow and implementation of double-authenticated messages (in the scope of the Y-Copy mode), authenticated by means of SWIFTNet PKI signatures.

Figure 3

"Figure 3" on page 785 represents the message flow of a double-authenticated message from the moment that the emitting interface constructs and sends it until the moment that it is delivered at the receivers interface.

Explanation of the message flow

1. The emitting institution A issues a message, for example an MT 103, to its correspondent institution B.

The emitting institution prepares a USER signature containing:

- the SignDN
- a Manifest element containing the reference(s) to and the digest value(s) of those parts of the payload that require authentication
- an Object element containing a random number

For a double-authenticated message there are two parts of the payload that require authentication:

- the FIN message requires a MAC-equivalent authentication. The USER signature element is extended with a digest value calculated on the complete FIN message. The reference to this digest value is "M". The random number, provided in the Object

element of the USER signature, is part of the input used for the digest value calculation of the MAC-equivalent authentication

- based on the FINCopy service Profile, the complete message, or only a part of it requires a PAC1-equivalent authentication. A digest value is calculated and added to the USER signature. The reference to this digest value is 1.

Upon emitting, SWIFTNet Link signs the message and converts the USER signature into a SYS signature.

2. The MT 103 arrives at the SWIFT Central System.

Based on the service profile (as defined by the SA), the SWIFT Central System extracts a number or all of the fields contained in block 4 of the MT 103.

It creates an MT 096 message, with a block 4 that contains block 1, 2, 3 (if present), 4 (limited to the extracted fields) and 5 of the MT 103. The MAC-equivalent and PAC1-equivalent authentication is provided through the SYS signature and passed with the MT 096 message.

Note	The Object element, containing the random number, is removed from the SYS signature.
-------------	--

3. The SWIFTNet Link of Alliance Access receives the message.

The SWIFTNet Link verifies the SYS signature and passes the message to Alliance Access together with the verification result. If the verification of the SYS signature was successful, then Alliance Access will verify that the PAC1-equivalent digest.

Alliance Access can define routing rules to send a message that failed authentication directly to the back office or to require operator intervention. If operator intervention is needed, then the operator can take one of the following actions:

- Bypass the authentication
 - Route the message (to the back-office application)
 - Re-authenticate the message, in case the reason for failure may have been fixed
- You cannot re-authenticate system messages or MT 096 messages. You can only progress system messages by using the Bypass Security command.
- Complete the message (without further treatment)

The message (including the authentication status) is forwarded to the back office (except in the last case).

4. The back office receives the message and evaluates the business request. It decides to accept or reject the request and if optional field 115 (<payment-release-information-receiver>) is used.
5. The back office prepares an MT 097 message which, amongst other fields, contains the accept or reject status - indicating to SWIFT if the message can be released - and transfers it to Alliance Access.
6. Alliance Access receives the message and prepares a (new) USER signature for PAC2-equivalent authentication. It calculates the digest value: this digest value is referenced to as "2".

The MT 097 is sent to the SWIFT Central System. SWIFTNet Link converts the USER signature into a SYS signature.

7. The SWIFT Central System creates:
 - an MT 012 if the MT 097 contains an accept indication and if it is requested by the FINCopy service, or
 - an MT 019 if the MT 097 contains a reject indicationand sends it to institution A.
8. If the MT 097 contains an accept indication, then the SWIFT Central System releases the original message and delivers it to institution B, together with the SYS signatures calculated in stage 1 and in stage 6.
9. Institution B receives the message.

Its SWIFTNet Link verifies both SYS signatures and passes the message together with the verification results to the SWIFT interface application of institution B.

If the SYS signature verification was successful then the SWIFT interface application verifies the MAC-equivalent and PAC2-equivalent digests. Routing rules can be defined to send a message that failed authentication directly to the back office or to require operator intervention. If operator intervention is needed, then the operator can take one of the following actions:

 - Bypass the authentication
 - Route the message (to the back-office application)
 - Re-authenticate the message, in case the reason for failure may have been fixed

You cannot re-authenticate system messages or MT 096 messages. You can only progress system messages by using the Bypass Security command.
 - Complete the message

The message (including the authentication status) is forwarded to the back office (except in the last case).

C.2 Implementation

C.2.1 Generic Implementation

Overview

To prepare the PAC2-equivalent USER signature in Step 6 of "Figure 3" on page 785, Alliance Access must calculate its `<DigestValue>`; for this calculation, it must have access to the following data elements:

- BIC8 of the central institution destination
- BIC8 of the receiver
- block 4 of the original message (or a part of it in case of partial copy)
- the signature value on the M digest, if an M digest is present, as calculated by the emitting institution (that is, the signature value of the Signature element containing the MAC-equivalent digest)
- field 115 (`<payment-release-information-receiver>`), if used

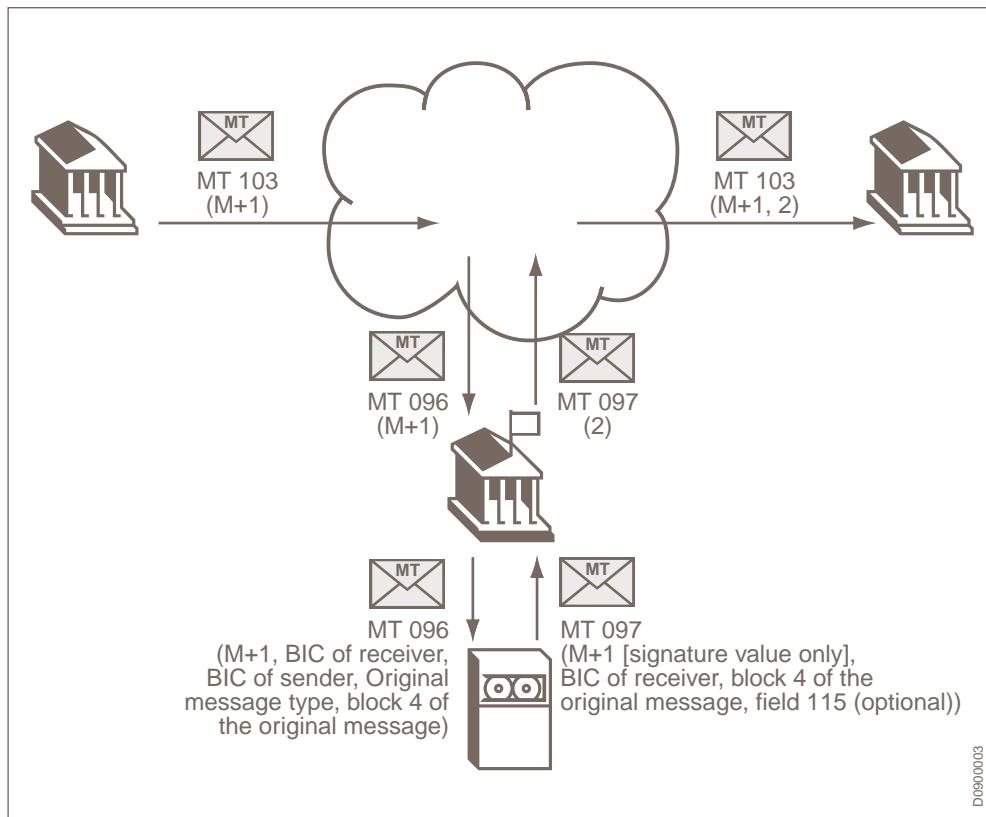
These data elements are added by the back office when preparing the MT 097 during stage 5 on page 786.

- the back office decides whether to use the optional field 115
- the back office adds the following data elements by means of extra fields (in addition to the fields defined by the MT 097 message standard):
 - BIC of the receiver of the original message
 - the original message type
 - block 4 of the original message as it has been copied in the MT 096
 - signature value on the M digest, if an M digest is present

The back office must have received this information from Alliance Access in Step 4 of "Figure 3" on page 785, together with the PAC1-equivalent authentication status. The PAC1 authentication status passed by Alliance Access to the back office in Step 4 of "Figure 3" on page 785 has one of the following values:

- FAC: authenticated with the PAC1-equivalent signature
- FAB: authentication bypassed
- FAI: authentication incorrect

Figure 4



Therefore, the following requirements apply to the back office:

- The back office must have access to the signature value. This is achieved by providing the whole SYS signature to the back office
- If the SYS signature contains an M digest, then the back office must provide the signature value of the received SYS signature back to Alliance Access.

C.2.2 Implementation in Alliance Access

Overview

In Step 3 of "Figure 3" on page 785 (when Alliance Access forwards the MT 096 to the back-office application), the required information is provided to the back office as described in the following table:

	MQSA format	RJE, DOS, MERVA/2 and CAS-1 formats ⁽¹⁾	CAS-2 NIF / NDF Text encoding	CAS-2 NIF / NDF ASN.1 encoding	ADK
BIC of emitter of original message	Contained in block 1 of the message embedded in MT 096	Not supported	Contained in block 1 of the message embedded in MT 096	Contained in block 1 of the message embedded in MT 096	Contained in block 1 of the message embedded in MT 096
BIC of receiver of original message	Contained in block 2 of the message embedded in MT 096	Not supported	Contained in block 2 of the message embedded in MT 096	Contained in block 2 of the message embedded in MT 096	Contained in block 2 of the message embedded in MT 096
Original message type	Contained in block 2 of the message embedded in MT 096	Not supported	Contained in block 2 of the message embedded in MT 096	Contained in block 2 of the message embedded in MT 096	Contained in block 2 of the message embedded in MT 096
Signature value on the M digest	SIG trailer in S-block, containing complete SYS signature	Not supported	field SIGV	field sigValue	field appe_pk1_pac2_value in the reception appendix
PAC1-equivalent authentication status	Trailer in block S of MT 096	Not supported	field PACR	field pacResult	field appe_pk1_pac2_result in the reception appendix

(1) These formats are no longer supported in the scope of FINCopy services.

In Step 6 of "Figure 3" on page 785, the required information is received from the back office through the following fields in the MT 097 (as described in "Generic Implementation" on page 787): 102, 124, 199, and 999. Field 999 is a field tag (SignatureValue) and is listed as *Reserved for internal use in the [FIN System Messages](#)*. If the SYS signature does not contain an M digest, then the field 999 is passed without content.

Alliance Access removes these fields when sending the message to the SWIFT Central System.

Note The back office must be able to extract the signature value on the M digest from the SYS signature.

C.3 Examples of MT 096 and MT 097 with PKI Signatures

MT 096 received by Alliance Access from SWIFT Central System

The following MT 096 is received by Alliance Access.

MT 096

Example

```

{1:F01DCRIFRTAAXXX0165005109}

{2:00960933041018DYLXXXXXXX00000176830410180533S}

{3:{103:COP}

{108:SMAIBE22A1033570}

{4:
{1:F01SMAIBE22AXXX0246001570}

{2:I103SMAIBE23XDLVN}

{3:{103:COP} }

{4:
:20:COP/103/test01
:32A:041025EUR1,
-}

{5:{MRF:041018093334041018SMAIBE22AXXX0246001570} }

}

{5:{CHK:73AC90A7A3F1}

{SYS:0933041018SMAIBE22AXXX0246001570} }

```

The MAC-equivalent and PAC1-equivalent authentication is provided by means of the following SYS signature:

SYS signature	Comments
<SwSec:Signature>	
<SwSec:SignedInfo>...</SwSec:SignedInfo>	
<SwSec:SignatureValue>PEMF@Proc-Type...</SwSec:SignatureValue>	Elements specific to SYS signature
<SwSec:KeyInfo>...</SwSec:KeyInfo>	Contains the SignDN
<Sw:Manifest>	
<Sw:Reference>	
<Sw:DigestRef>M</Sw:DigestRef>	
<Sw:DigestValue>...</Sw:DigestValue>	MAC-equivalent
</Sw:Reference>	
<Sw:Reference>	
<Sw:DigestRef>1</Sw:DigestRef>	PAC1-equivalent

SYS signature	Comments
<Sw:DigestValue>...</Sw:DigestValue>	
</Sw:Reference>	
</SwSec:Manifest>	
</SwSec:Signature>	

This example contains two `<Sw:Reference>` instances:

- one for the MAC-equivalent, with `<Sw:DigestRef>` equal to M
- one for the PAC1-equivalent, with `<Sw:DigestRef>` equal to 1

Other `<Sw:Reference>` elements can be present (for example, for end-to-SWIFT signature): these are left out for readability.

MT 096 Transferred from Alliance Access to back office

Alliance Access transfers the MT 096 to the back office as follows:

- MQSA format

A new S-block trailer is added containing the complete `<SwSec:Signature>` element:

```
{S:{FAC:}
{SIG:<SwSec:Signature>...</SwSec:Signature>}}
```

- CAS-2 NIF or NDF Text Encoding format

The PKI signature is delivered to the back office by means of a new field named SIGV:

```
:SIGV:nnnnn:<SwSec:Signature>...</SwSec:Signature>
```

whereby nnnnn stands for the length of the signature element starting with `<SwSec:Signature>` and ending with `</SwSec:Signature>` (both tags included).

- ADK

The information is transferred to the back office by means of designated fields:

Signature value:	appe_pk1_pac2_value in the reception appendix
PAC1 equivalent authentication status:	appe_pk1_pac2_result in the reception appendix

MT 097 Transferred from back office to Alliance Access

The back office provides Alliance Access with the following MT 097:

Message	Comments
{1:F01MASGSGSMAXXX0122000199}	
{2:I097SWFTXXXXXXXXS}	
{4:}	
{103:COP}	
{109:090514091701090514SENDRBICAXXX0685697419}	
{451:0}	

Message	Comments
{114:PAYMRELINFO2SENDER}	
{115:PAYMRELINFO2RECEIVER}	
{102:SMAIBE23XDLV}	Receiver BIC of the original MT message that was sent
{124:103}	Original Message Type
{199:	Start of block 4 of original msg
:20:COP/103/test01	Original msg field
:32A:041025EUR1,	Original msg field
-}	End of block 4 of original msg
{999:PEMF@Proc-Type...}}	New field tag - <code>SignatureValue</code>
}	

For the MT 097, note that:

- field 117 is absent (MAC of the original message)
- in case of TARGET, field 102 does not occur twice
- field 999 is added, which contains the `SwSec:SignatureValue` of the signature element of the original message.

Note

If the MT 097 contains a reject indication, then a PAC2-equivalent USER signature must be provided in Step 6 of "Figure 3" on page 785. As of SWIFTNet Phase 2, the back office must therefore always provide Alliance Access with fields 102, 124 and 199.

MT 097 Sent by Alliance Access to SWIFT Central System

Alliance Access performs the following actions on the received MT 097:

- removes from block 4 all fields starting with field 102 until the end of block 4

{1:F01MASGSGSXXXX0122000199}

{2:I097SWFTXXXXXXXXX}

{4:

{103:COP}

{109:090514091701090514SENDRBICAXXX0685697419}

{451:0}

{114:PAYMRELINFO2SENDER}

{115:PAYMRELINFO2RECEIVER}

}

{5:{CHK:73AD80A7A3F1}}

}

- prepares the PAC2-equivalent USER signature (it finds all the required input in the MT 097 it just received):

USER Signature	Comments
<SwSec:Signature>	
<SwSec:KeyInfo>...</SwSec:KeyInfo>	
<SwSec:Manifest>	
<Sw:Reference>	
<Sw:DigestRef>2</Sw:DigestRef>	PAC2-equivalent
<Sw:DigestValue>...</Sw:DigestValue>	
</Sw:Reference>	
</SwSec:Manifest>	
</SwSec:Signature>	

Legal Notices

Copyright

SWIFT © 2015. All rights reserved.

Restricted Distribution

Do not distribute this publication outside your organisation unless your subscription or order expressly grants you that right, in which case ensure you comply with any other applicable conditions.

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

Translations

The English version of SWIFT documentation is the only official and binding version.

Trademarks

SWIFT is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: the SWIFT logo, SWIFT, SWIFTNet, Accord, Sibos, 3SKey, Innotribe, the Standards Forum logo, MyStandards, and SWIFT Institute. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.