Connectivity

Alliance Access/Entry 7.0

Functional Overview

This document provides a high level description of the main functional enhancements provided by Alliance Access/Entry 7.0, available beginning of 2011.

The purpose of this document is to provide an advanced description of these enhancements, so that customers can assess how to take advantage of these new features and accordingly plan for it.

This document also briefly covers the functional enhancements specific to Alliance Entry 7.0.

The target audience are users familiar with current Alliance Access/Entry functionality.

December 2010

Table of Contents

1 Summary Overview

This section provides a summary of the functional enhancements provided by Access 7.0 and Entry 7.0. These enhancements are further detailed in following sections of this document.

Operational Monitoring & Control

Access 7.0 supports the integration with existing supervision and monitoring systems (such as IBM Tivoli, BMC Patrol, HP Openview, and CA Unicenter) through a command-line based tool, available on the Access server only. This tool provides commands to extract selected monitoring information from Access into an external text file, in an open format that can be processed by these monitoring systems or by customer applications.

Alliance Access provides a second command-line tool, also available on the Access server only, supporting commands to operationally manage Alliance Access (e.g. enabling/disabling a message partner, logging in/out a logical terminal). These commands can be launched either manually or from a scheduler application running outside Access. These commands can be invoked locally from customer developed scripts, or remotely by means of agents running locally on the Access server and controlled remotely by these supervision systems.

For monitoring purpose, the SNMP feature remains available, as a way to feed operational information to monitoring systems. The new command-line tool provides an alternate way to extract monitoring information from Access.

Remote Disaster Site Recovery

With Access 7.0, the Database Recovery option introduced in Access 6.3 is enhanced to support remote disaster site recovery. It allows bringing the database back to a consistent state, recovering from the last available transaction found in an incomplete set of recovery data.

The typical challenge when working with a remote disaster site is how to replicate data from the primary site. A synchronous replication is often not feasible and consequently. An asynchronous replication is the only option, meaning that the last database updates contained in the recovery data on the primary site will not be available on the disaster site.

With this enhancement, the database can be recovered on the disaster site in a consistent state, but representing its situation a few minutes before the incident on the primary site. This situation can lead to the duplicate emission of transactions. The Database Recovery option in Release 7.0 provides a new Database Repair service which addresses this operational risk (see below).

Oracle Hosted Model

The current embedded Oracle database model is complemented with a new installation option, the 'hosted' model, supporting the configuration of the Access database on an external, customer provided Oracle instance.

This is mainly beneficial for customers who manage their own Oracle infrastructure, and want to re-use investments made in this infrastructure or in resiliency tools such as Oracle Clusters and disaster replication features such as Oracle Data Guard.

For a new installation, the customer has now the choice in Access 7.0 between 2 installation options:

- Select the installation of the local embedded Oracle database (as currently available) or
- Select an external Oracle instance where to install the Access database schema.

An upgrade from the embedded to the hosted model is not possible. For such scenario, the customer must install a separate Access instance, using the hosted model and then use the new 7.0 export and import tools to move the configuration from the embedded to the hosted installation.

The use of additional resiliency Oracle options on the external instance must be transparent to Access software[1].

Note that the Web Platform, which also embeds an Oracle database, also supports the hosted database option.

Database Repair Service

The data loss resulting from a partial recovery of the Access database (i.e. messages being restored as live on the disaster site although they were just completed on the primary site before the incident) creates an operational risk of generating duplicate transactions: for outgoing messages, their reprocessing will result in duplicate transactions sent to correspondents; for incoming messages, their reprocessing (in exit points) will result in duplicate transactions sent to the back-office systems.

Access 7.0 introduces a new Database Repair Service to address this operational risk. This repair service takes the necessary actions to ensure that no duplicate transactions are generated during a recovery situation. The repair service is integrated with the embedded Database Recovery option, and will be automatically invoked during a recovery process.

The Repair Service is also available for the Oracle hosted model, as the asynchronous replication tools that can be used (like Oracle Data Guard) can create the same operational risk of duplicate transactions. In hosted model, the repair service will need to be invoked explicitly during the recovery procedure on the disaster site.

Enhanced Duplicate Detection

In order to further enhance resiliency in recovery situations, Access/Entry duplicate detection mechanism is enhanced to detect outgoing and incoming transactions that are full duplicates of other transactions already processed by Access/Entry (meaning that they are sent to the same correspondent with an identical payload). The detection history is extended to cover all active days (i.e. non archived days) and all message formats (FIN, InterAct and FileAct). The detection continues to rely on the *'possible_duplicate'* keyword, available in Access routing to flag messages as duplicate.

This duplicate detection enhancement further complements the disaster recovery support. It can protect against the risk of back-office applications or middleware systems generating duplicates during their own recovery procedures. In contrast, the Repair Service makes sure that possible duplicate transactions present inside Access are marked with a PDE trailer. The Repair Service is not able to detect the duplicates resulting from external retransmissions.

This duplicate detection logic is part of the Access/Entry core services. It is not linked to the database recovery option. It is always active and can therefore be used in a normal situation (i.e. outside the context of a recovery scenario).

Configuration Management

Access 7.0 provides a new set of command-line tools supporting the export of selected configuration data into an external, user modifiable text file, and the import of configuration data from an external file.

These tools address various configuration management needs:

- They facilitate the exchange of configuration data between a test and a production system, where the possibility to alter the configuration data is required to cope with the inherent differences between the two systems (like T&T BICs versus production BICs).
- The availability of command-line based options also facilitates the automatic transfer of configuration changes between cloned production instances.
- The possibility to manually create and alter the configuration file also helps to automate repetitive configuration tasks, typical of a service bureau activity.

[1] For example, Access will be Oracle RAC-compatible, but not Oracle RAC-aware. Meaning that upon a node failure, Access will not try to reconnect to another node and replay the in-flight messages.

In comparison with the database backup tool, the export process allows the operator to precisely specify the configuration data to export.

The import process validates the data to import and aborts the operation in case of error. In case some entities were already updated when the import process is aborted, these updates are kept.

The import process shares the same pre-update constraints and post-update approval rules that are applicable to the equivalent manual operations available from Access graphical interfaces (Workstation or Web Platform).

Operational Data Query

Alliance Access 7.0 provides a set of Web Services that can be used by external applications to query operational data available in the Alliance Access database. These Web Services allow:

- the search and query of RMA authorisations and query/answer
- the search and query operations of messages and events

The search service returns the entities matching a search criteria. The query service returns the details of a specific entity. For a message, not all database fields are returned. The most often used fields of all message records (header, text, instances and associated interventions) are returned. Archived messages and events, still present in the database, are also accessible.

This Search/Query based Web Service provides an alternative to Alliance Developer Kit (ADK) to address simple query needs like accessing the full history of a message for audit purpose, collecting daily traffic statistics, or exporting the message content and history into an external archive system.

ADK remains the only option available to integrate components into Access main message flow, providing the performance, security and configuration requirements specific of such applications. The Web Services are positioned as more straightforward and more standard way to externalise the data available in Access.

Note The message and event query service is not delivered with Access 7.0, but as a functional patch to be installed on top of Access 7.0. This patch is planned to be delivered during Q2 of 2011.

Browser based GUI using the Web Platform

Alliance Workstation 7.0 and Web Platform 7.0 are both available for Access/Entry 7.0. The Web Platform 7.0 provides all the functionality necessary to operate Access/Entry 7.0 (i.e. configuration, monitoring, message management and RMA).

Customers currently using the Workstation can continue to use it with release 7.0. The Workstation does not include new functionality. It only provides the existing 6.x functions upgraded to 7.0.

Customers are however encouraged to use Web Platform 7.0, as new GUI functionality is only implemented on the Web Platform (e.g. 'Direct FileAct' message partner configuration, RMA over InterAct and FileAct, etc).

Web Platform 7.0 also significantly improves Access/Entry 7.0 monitoring. Although the monitoring application is still available on Workstation 7.0, the Web Platform 7.0 includes a completely redesigned monitoring interface (the Monitoring Dashboard), providing a more efficient monitoring summary of all Access entities, allowing operators to quickly spot anomalies and take appropriate actions.

This Monitoring Dashboard also supports the monitoring of multiple Access instances.

ADK based GUIs

The availability of additional Web Services, which will enable the development of browser based graphical applications integrated with Access, is planned for a future release of Access. These Web Services must allow an application to influence the routing of messages in Access.

Workstation 7.0 is still mandatory to use these ADK based GUI. This includes ADK applications developed by vendors and the use of MQSA configuration GUI.

RMA Enhancements

Access/Entry 7.0 provides a set of RMA enhancements, aiming at:

- Supporting RMA beyond FIN
  - The enhancement extends the management of RMA authorisations currently limited to FIN to also support RMA authorisations for InterAct and FileAct services.
  - The enhancement also supports filtering of InterAct and FileAct traffic based on RMA authorisations.
- Providing an audit trail per RMA authorisation.

  This trail lists all actions performed on an RMA authorisation, providing an easy way to audit the actions done on an RMA authorisation.
- Supporting the transmission status.

  Each authorisation to receive has a new status, the "transmission status", indicating the processing the status of the underlying RMA InterAct message. The message reconciliation process is also capable of properly reporting this status when the RMA InterAct message referenced by the non-delivery notification, is already archived (a common situation as the notification can be generated 14 days after the InterAct emission).
- Making the management of RMA authorisations easier.

  It is possible to clean up RMA authorisations for which there is no BIC defined in the Correspondent Information File.

  A configuration parameter allows the automatic export of RMA authorisations as soon as they are changed.

  Search and display enhancements are provided in the user interfaces, mainly in the Alliance Web Platform RMA package.

SOAP Host Adapter

Alliance Access provides the SOAP adapter, a new host adapter supporting the exchange of MT and MX messages between back-office applications and Alliance Access, over a SOAP connection. The SOAP adapter is an interactive adapter, offering an alternative to the MQ host adapter.

The SOAP adapter does not yet support FileAct messages, but it is planned to support it as well.

Some important characteristics of the SOAP adapter are:

- Data transferred over a SOAP connection must use the XMLv2 format. This format is already used by other Access host adapters (File Transfer, MQHA and MQSA).

  The SOAP adapter requires the XMLv2 revision 2 level at minimum.
- The SOAP communication channel supports session management and duplicate prevention, and can as such guarantee a one time delivery.
- The communication is always initiated by the back office. Therefore, only a SOAP client is required in the back office. Alliance Access acts as the SOAP server.

Licence 14:AI SOAP ADAPTER is required for using the SOAP host adapter.

FileAct Support

Access 6.3 introduced FileAct support, over the File Transfer adapter only.

Access 7.0 extends FileAct support, by supporting it over MQ based back-office connections. The MQ FileAct support is available on the MQHA adapter only (MQSA does not support FileAct transactions).

settings.

Note The SOAP Adapter on Access 7.0 does not yet support FileAct. The SOAP evolution to support FileAct is planned to be made available in a functional patch to be installed on top of Access 7.0. This patch is planned to be delivered during Q2 of 2011.

Access 7.0 also supports a new host adapter simplifying the integration of FileAct between back-office applications and Access. This new adapter, 'Direct FileAct', enables the back-office application to only provide the payload file to initiate a FileAct exchange. The back-office application does not need to generate an XMLv2 file to provide the FileAct settings. These settings are statically configured in each 'Direct FileAct' based Message Partner.

The 'Direct FileAct' adapter enables legacy applications, already producing a payload file, to integrate with SWIFTNet FileAct without requiring any additional developments.

The 'Direct FileAct' adapter also facilitates the prototyping of a new FileAct solution with Access, as a base integration can be tested without requiring the development of an XMLv2 file.

LDAP Support

Access/Entry support LDAPv3 repositories for user authentication. This allows institutions to re-use their existing user directories with Access/Entry to perform central user management.

LDAP authentication is available as an additional authentication mechanism in Access/Entry, next to the standard local user authentication and authentication via One-Time passwords.

Using this new feature implies the following:

- If an operator is defined in Access/Entry to be authenticated through LDAP, then Alliance Access/Entry forwards the login request to the LDAP server for the user authentication.
- The LDAP server(s) must be defined and configured within Access/Entry.

This function is included in Access/Entry core functionality.

Entry 7.0 Evolution

Entry 7.0 inherits some of the features introduced in Access 6.3 and Access 7.0.

An important evolution is the replacement of the existing C-ISAM database with an embedded Oracle database. This database replacement is transparently managed by the upgrade procedure when migrating from Entry 6.0 to 7.0.

Entry 7.0 supports LDAP integration, FileAct over the File Transfer adapter and FIN Cold Start.

The RMA enhancements to support authorisations for InterAct and FileAct services are also available on Entry 7.0.

Web Platform 7.0 and Workstation 7.0 are both available on Entry 7.0. Web Platform 7.0 provides all the services required to operate Entry 7.0. Entry 7.0 customers can therefore progressively start using the Web Platform as an alternative to the Workstation.

The following new Access 7.0 based features are not available on Entry 7.0:

- The Web Services interface
- The Database Recovery option
- The Direct FileAct adapter
- The operational integration and configuration replication tools

Standalone RMA Evolution

The dedicated RMA software does not exist anymore with 7.0. The Access Standalone RMA configuration remains available commercially. Customers using Access Standalone RMA 6.0/6.3 and upgrading to 7.0 will receive the Access 7.0 DVD, with a specific licence limiting the use of this Access system to RMA operations only.

Standalone Alliance Access for Message Entry/Repair

Some customers have a need to separate, in different systems, the functions of message management and the functions of message exchange with SWIFT.

The Standalone Alliance Access meets this requirement by allowing the manual creation or repair of messages, working as a fully functional Alliance Access, but with the unique difference that this system is not connected to SWIFT's network but instead must communicate over the MQ host adapter with another Access system for SWIFT connectivity.

The standalone Alliance Access requires the activation of licence 07:STANDALONE REC.

Standalone Alliance Access supports the creation and repair of FIN and InterAct messages. FileAct messages are also supported, but limited to the creation function only. The repair of FileAct messages is not supported.

The management of RMA authorisations cannot be done in Standalone Alliance Access. The RMA authorisations must still be managed in an Access system connected to SWIFTNet. It is however possible to import the RMA authorisation into Standalone Alliance Access.

The Standalone Access Information Paper available on SWIFT.com provides more information on this Access configuration option.

2 Operational Integration

Overview

The operational integration is based on two new command-line based tools, available on the Access server (one for monitoring and one for operational management). These tools provide control and monitoring commands that can be invoked from a command-line prompt or from a command script (Windows batch file or a UNIX script).

Some key characteristics of these tools are:

- Selective control of access rights, based on 2 alternatives:
  - Providing the credentials (user name and password) of an Access operator, to use the associated Access profiles for access control.

    The password is either provided from the command line, prompted or read from a file.
  - Executing, without providing credentials, from the Access owner account only ('all_adm' account).

    This privileged access method needs to be authorised by the LSO and RSO, who will then assign an operator profile to this account determining the authorised operations.
- The command-line tools are local to the Access server. If a remote execution is needed, it is the customer's responsibility to implement the necessary procedures and security checks. This configuration is in-line with most supervision architectures which rely on agents running locally on the system.
- The command-line tools make use of the exit code to indicate successful execution. These exit codes allow customers to sequence the execution of multiple commands, in particular when the execution of a command depends on the execution status of the prior command.

Integration Alternatives

These command-line tools are using control and monitoring Web Services, available internally to support these functions on the Web Platform. These Web Services remain internal (i.e. they are not documented and can be changed by SWIFT) with Access 7.0. The command-line tools are the only documented way of controlling and monitoring Access from an external application.

The use of SNMP queries, although quite powerful and sophisticated, has been considered but is not supported, as not being often used for integration.

Note SNMP queries should not to be confused with SNMP traps. Access will continue to support SNMP traps, which are the preferred method to push information to an external system (to the opposite of a command-line based tool that pulls information on request). There are no plans to further enhance SNMP trap support (V1 protocol only).

Note In a future release of Access, these Web Services might be documented to provide an alternative integration method for control and monitoring applications.

2.1 Operational Monitoring

The main purpose of operational monitoring through a command-line based tool is to enable an external application to extract specified monitoring information from Access, at regular intervals.

This section provides more details how to use this monitoring tool. More detailed information is available in the *Installation and Administration* guide, Appendix B.

2.1.1 Command-line Overview

The operational monitoring is available via the `saa_monitor` command. The syntax is as follows:

```
saa_monitor
   -monitorparameterfile <monitor_parameter_file>
```

```
 -monitoroutputfile <monitor_output_file>
[-user|-application <username>]
[-password <password>] | [-passwordfile <password_file>]
[-cycle <nnnn_sec>]
[-duration <nnnn_h>]
[-continue_on_error]
[-port <port_number>]
[-overwrite]
```

Some key characteristics of the saa_monitor tool are:

- The monitor parameter file specifies the information to be monitored. The file can specify different entities (like monitoring 'Message Partner' and 'Logical Terminal' in a single command).
- The monitored information is output into a user specified file, using a documented XML schema.
- The tool can either run once (i.e. no cycle provided) or run continuously, at a specified 'cycle' interval.

2.1.2 Monitoring Information

Existing Monitoring Information

In general, the monitoring information provided by the saa_monitor tool is similar to the information displayed on Access graphical monitoring applications (on Workstation or Web Platform).

The below table list the entities that can be monitored. Please refer to Section 'Entities Eligible for Monitoring and Monitoring Fields', in the *Installation and Administration* guide for more detailed description of these entities, along with the entity fields that can be monitored.

Eligible Entity	Monitored occurrences	Occurrence selection
Logical Terminal	All, Exceptions, Selection	LT Status
Message Partner	All, Exceptions, Selection	Name Status Session status
Queue (System queue, User queue and Exit point)	All, Exceptions, Selection	Name
SWIFTNet Profile	All, Exceptions, Selection	Name Status, Session status
System Resource	All, Exceptions	N/A
Process	All	N/A
Operator session	All Summary	N/A
File Transfer	All	N/A

2.1.3 Additional Monitoring Data

Access 7.0 also provides additional monitoring information, either available on the monitoring screens, or available via the saa_monitor tool.

User-controlled Sent/Received Counters

The Message Partner, Emission/Reception Profile and Logical Terminal entities already maintain two session counters which indicate the number of messages exchanged (sent and received) during a session. These counters are reset by Access at each new session.

To support long-running traffic statistics, two additional counters are maintained by each Message Partner, Emission/Reception SWIFTNet Profile and Logical Terminal entity, to record the number of the messages sent and received by these entities.

Compared to the previous session counters, these user-controlled counters are not reset by Access, but must be reset on request by an operator or an external application.

Some characteristics of these counters are:

- Web Platform allows an operator to view and individually reset each counter (this function is not available on the Workstation).
- The saa_manage tool provides a way to individually reset these counters. The current counter value, before reset, is returned by the tool during reset.
- These long-running counters are part of the monitoring information returned by the saa_monitor tool.
- A roll over mechanism is still foreseen, in case that the maximum value (over 2 billion) is reached.

These User-Controlled counters are further detailed in the *Daily Operations* guide.

User Session Monitoring

The total number of operator sessions currently opened is available for monitoring, with a distinction between operator and application based sessions.

Instance Age Monitoring

Access 7.0 maintains the age of an instance, i.e. how long a message instance has remained in a given queue. This instance age is reset each time the instance moves from one queue to another queue (the age is therefore not the elapsed time since a message instance has been created in Alliance Access). The instance age is therefore only relevant for live instances.

This age information allows detecting messages residing for an abnormal period in Access queues.

The instance age is visible when looking at the details of an instance, using Message consultation functions.

The age information is part of the instance fields, supported by the Message Query Service.

Queue Age Monitoring

Access 7.0 queues provide a new age monitoring field, which represents the age of the oldest message present in the queue.

The queue age field is part of the monitoring fields supported by the saa_monitor tool when monitoring queues. It allows a monitoring application to quickly detect messages that are abnormally idling in Access queues.

Queue Age Threshold Alert

Access 7.0 allows an event to be generated on a given queue, when the age of a message present in the queue exceeds a user configured value.

The queue age threshold must be configured by the administrator, per queue. This configuration operation is available on the Web Platform only. The default threshold value per queue is 0, which by default disables the age threshold alert function.

When the age threshold alert is reached, the age event is generated once per message (i.e. not repeated at regular intervals).

Queue Depth Monitoring

Access 7.0 queue monitoring function provides the queue name and status, but also returns the number of message instances present in the queue. The queue monitoring function also returns the current queue throughput.

This additional depth and throughput information allows an external application to monitor the queue 'health', i.e. the activity on the queues that are supposed to be transient (like the SWIFT emission queue).

2.2 Operational Management

The main purpose of the new Access 7.0 operational management function is to allow an external application to invoke operational commands on Access through a new command-line based tool available on the server only.

2.2.1 Command-Line Overview

The operational management is provided by the new `saa_manage` tool. The tool syntax is as follows:

```
saa_manage
       -manageparameterfile <manage_parameter_file>
       -manageoutputfile <manage_output_file>
       -action <action> <action parameter 1, action parameter 2, ...>
      [-user|-application <username>]
      [-password <password>] | [-passwordfile <password_file>
      [-overwrite]
      [-port <port_number>]
```

Some key characteristics of the `saa_manage` tool are:

- saa_manage is available as an alternative mechanism for invoking control operations already available from the Access GUI (Workstation or Web Platform).

  Some GUI commands available from the Web Platform or the Workstation are not available via `saa_manage`, either because there is no interest in exposing such commands or their invocation is too complex (i.e. numerous arguments, with inter-dependencies).
- The operational management command to execute is passed as an argument, along with all other required parameters.
- A command can only be executed against a given entity, possibly supporting multiple occurrences of this entity (e.g. login all defined Logical Terminals). When commands must be performed on different entity types, multiple executions of `saa_manage` must be done for each entity type.
- The execution status of the command is provided in XML format and can be redirected to a file.
- The command updates the system exit code to indicate its global execution status (success or failure).

More details about the `saa_manage` tool can be found in the *Installation and Administration* guide, in Appendix B section.

2.2.2 Control Commands

Supported Command-line Operations

The table below lists the entities supported for operational control along with the commands available for each entity.

Eligible Entity	Occurrence Identification	Available Action

Eligible Entity	Occurrence Identification	Available Action
Component	All or Name field values	Start Stop
Logical Terminal	All or Name field values	Login Select_FIN Logout Quit Change_mode Reset_Sent Reset_Received
Emission/Reception SWIFTNet profile	All or Name field values	Activate De_activate Enable Disable Change_mode Reset_Sent Reset_Received
Message Partner	All or Name field values	Enable Disable Run_session Abort_session Start_session Stop_session Reset_Sent Reset_Received
Queue	All or Name field values	Hold Release
Operator	All or Name field values	Enable Disable

Please refer to Section 'Entities Eligible for Managing', in the *Installation and Administration* guide for more detailed description of the Access entities that can be managed, along with a detailed description of the operational actions allowed for each entity.

Limited CREST Support

The operational control of CREST component is limited to the start and stop of the component (as available via System Management command).

Limited MQSA Support

The operational control of MQSA is limited to the generic Start and Stop action on an Access ADK based component.

The other monitoring and management features are not available to the MQSA component. This is because MQSA is built on a different architecture (ADK based) then the other Application Interface components (such as MQHA, SOAP, File Input/Output).

MQSA is in maintenance mode. There are no plans to further enhance MQSA in the area of operational monitoring and management. MQHA is the recommended alternative for MQ based connectivity. MQHA is fully supported by operational monitoring and control.

Command-line operations already available

The `saa_system` and `saa_dbrecovery` command-line based tools, already available on Access 6.3, are still available on Access 7.0. Some of the functions supported by these tools are:

`saa_system` command-line tool:

- Archive messages and events
- Backup, Remove and Restore message and event archives
- Full database backup
- Start / Stop Alliance Access

`saa_dbrecovery` command-line tool:

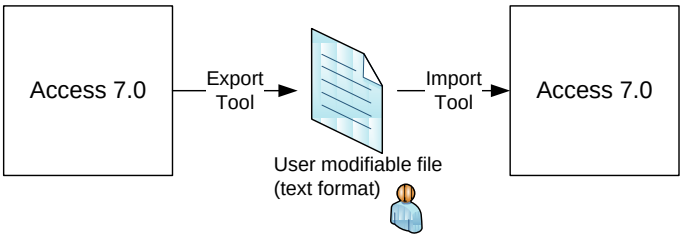
- Full database recovery backup
- Incremental database recovery backup

3 Configuration Management

3.1 Concepts

Access 7.0 allows to export its configuration into an external text file, and to import this configuration file to update its configuration.

The basic principles of the import/export functionality are highlighted below:



- A new export tool (`saa_export`) is provided to export selected configuration data into a text file.

  A search criteria available per configuration entity allows to control which configuration elements to export. Operational entities like Messages or Events are not included.

  Different entities can be exported in the same file.

  The name and location of the exported file is defined by the user.
- The configuration file, generated by the export tool, is based on a documented XML schema.

  This is a text file that can be further modified by the end user (using a regular text editor), for example to substitute all Test and Training BICs with a production BIC in the whole configuration.
- Operator passwords can be exported on request. LAU settings cannot be exported.
- A new import tool (`saa_import`) is provided to import the configuration information contained in the text file and update Access configuration.

  The import process can either add new entities or modify existing ones. It does not support deletion of existing entities, except for routing rules updates.

  The import process first validates the import file format. It also validates that the entities to be modified are in the correct state (i.e. allowed for configuration changes).

  The import process follows the same update rules as applicable to an operator when using the Workstation or the Web Platform. Entities must be in the correct state to be modified (e.g. disabled state), and security related changes still needs to be approved by another user (e.g. schema changes, operator permission changes).
- The export and import tools are executables available on the Access server only.

  They can be invoked by any account defined on the system where Access is installed (i.e. not limited to the Access owner account 'all_adm' only).

  A regular account will need to provide the credentials of an Access operator to use the tools. The entitlements associated to this Access operator will determine the allowed actions.

  The Access owner account ('all_adm') has the possibility to execute the tools without providing credentials. A specific profile, associated to the owner account, determines the allowed rights. This security bypass must be enabled by the LSO and RSO.

3.2 Export Tool

Overview

The export functionality is provided by a new command-line utility `saa_export`, available on the Access server only. This tool can be invoked from a command prompt or included in a command script.

The tool syntax is:

```
saa_export
  [-user|-application <username>]
  [-password <password>]
  [-passwordfile <password_file>]
  [-exportsensitivedata]
   -parameterfile <parameter_file>
   -exportfile <export_file>
  [-overwrite]
  [-port <port number>]
  [-reportfile <file_pathname>]
  [-summaryonly]
```

Where:

- `user/password/passwordfile`: optional parameter

  Specifies the credentials of an Access operator.

- `exportsensitivedata`: optional parameter

  Indicates that sensitive data must be exported (See Exporting Sensitive Data section)

- `parameterfile`: mandatory parameter

  Specifies the export parameter file name/location, that contains the groups or entities to export (See Export Parameter File section)

- `exportfile`: mandatory parameter

  Specifies the file name/location of the configuration file where to export the configuration data.

- `overwrite`: optional parameter

  Forces the overwrite of export file if it already exists.
  If the export file already exists and –overwrite is not specified, the export will be aborted.

- `port`: optional parameter

  Port to be used by the tool for accessing Access. If omitted, the default Access port is used.

- `reportfile`: optional parameter

  Name of the resulting report file in which details of the export execution are logged. If omitted, the default report filename is used.

- `summaryonly`: optional parameter

  If specified, the produced export log contains less information about the entity occurrences exported.

More details about the `saa_export` tool can be found in the *Installation and Administration* guide, in Appendix B section.

Export Parameter File

The Export Parameter file specifies the entities to export. Different entities can be specified. For each entity, a filtering criteria is available to specify the entity occurrences to export.

In most cases the entity field name can be specified as a search criteria. For some entities, additional search criteria are available to facilitate the export selection (like a modification date/time for routing rules).

The list of supported entities, along with the available search criteria is detailed in the *Installation and Administration* guide, mostly in 'Replication of Configuration Data' section. The sub-section 'Exported Fields' details the entities and their associated fields that can be exported.

Securing Sensitive Data

The sensitive data items are LAU settings and operator passwords. They are handled differently during the export process:

- LAU settings

  The entities currently making use of LAU settings are:

  – The Gateway Connection, where LAU is used to secure the Access / Gateway connection.

  – The Message Partner, which can optionally use LAU settings to security the back-office connection.

  When exporting an entity which has LAU settings defined, the fact that the LAU settings are defined is exported, but the actual LAU values are not exported.

- Operator password

  When the option `exportsensitivedata` option is specified when exporting operator entities, the password information is exported with other operator fields. This information is encrypted and cannot be manually modified.

  If the option is not specified when exporting operator entities, all fields except the operator password are exported.

The next section 'Import Tool' describes the system behaviour when importing such LAU settings and operator password information.

Please refer to the Section 'Handling the Export and Import of Sensitive Data' in the *Installation and Administr*ation guide for more details.

Export Log

The export generates a log providing:

- The date/time of export
- The export arguments
- The name and type of each exported entity. It also logs if LAU settings are defined but not exported, or if the operator password is not exported.
- The total number of exported entities

3.3 Import Tool

Overview

The import functionality is provided by a new command-line utility `saa_import`, available on the Access server only. This tool can be invoked from a command prompt or included in a command script.

The tool syntax is:

```
saa_import
   -exportfile <Export_file>
  [-user|-application <username>]
  [-password <password>]
  [-passwordfile <password_file>]
  [-overwrite]
  [-port <port number>]
  [-reportfile <file_pathname>]
  [-summaryonly]
```

Where:

- `user/password/passwordfile`: optional parameter

  Specifies the credentials of an Access operator.

- `exportfile`: mandatory parameter

  Specifies the file name/location of the file containing the configuration entities to be imported.

- `overwrite`: optional parameter

  Indicates that existing entities should be overwritten. If this option is not specified, the import process skips this entity modification, and logs this information in the import log.

- `port`: optional parameter

  Port to be used by the tool for accessing Access. If omitted, the default Access port is used.

- `reportfile`: optional parameter

  Name of the resulting report file in which details of the import execution are logged. If omitted, the default report filename is used.

- `summaryonly`: optional parameter

  If specified, the produced export log contains less information about the entity occurrences exported.

Import Validation Process

Once started, the import process applies the configuration updates provided from the configuration file.

The following validations are performed during the import process:

- New entities are added, modifications to existing entities are done if the overwrite mode is selected. If the overwrite mode is not selected, and modification requests are present, the associated entity update is skipped.
- The validation rules are identical to the ones applicable to an operator performing a similar operation from the Workstation or the Web Platform:
  - Licence verification

    The entities to be imported must be related to actual licence options. Failure to find a matching licence for any specified entity aborts the process.

  - Updatable state for modification

    An entity must be in a specific state to be modified (e.g. a message partner must be in 'Disabled' state; an active schema cannot be modified).

    The import process aborts if any modification attempt is made on an entity which is not in the appropriate state.

Note The import tool does not provide means to alter the state of an entity before modification. This operation is however available from the operational management (See Section 2.2.2, Control Commands). It is therefore be possible, within the script, to first alter the operational status of the entities to modify, then import the modification, then reset the operational status back to an operational state.

  - References

    The import process aborts if, when having imported all entities from the file, there is any 'unresolved' reference (i.e. an entity referring to an undefined entity).

    The import process also aborts, if after processing a configuration file, there are still entities with mandatory references that are undefined.

- Sensitive data
  - LAU Settings

    When importing entities that were configured with LAU based security, the tool does not import the LAU keys (as the information is not present in the file), but indicates in the import log that LAU settings were set for the entity but were not imported.

If the entity to import exists and has LAU settings already set, these settings remain unchanged.

- Operator Passwords

  Operator passwords, if present in the file, are imported but set as expired. At first login, the operator will have to change its password. If not present in the file, the existing operator password is left unchanged (or the system generated password is set for a new operator).

Please refer to the Section 'Handling the Export and Import of Sensitive Data' in the *Installation and Administration* guide for more details.

The import process first validates the import file and cancels in case errors are found, ensuring that the database is always consistent. The import process is however not capable of 'rolling back' the configuration updates already done, the updates already done before the import process aborted are kept. The customer must correct the import file and launch again the import process. The entities already updated can be skipped (depending on the `-overwrite` mode)

If the customer wants to implement an 'all or nothing' function for the import procedure (i.e. all entities are updated or none is updated), the customer is required to take a backup of the database before the import process, and in case of import errors, to restore this database backup.

Routing Rule Deletion

When all routing rules of a queue have been exported, and these rules are imported on an existing queue in Access, the import process first deletes all rules defined on that queue, before importing the new rules.

This is the only situation where the import tool can delete entities. This operation is necessary to ensure an update of the whole routing rule configuration of a queue. The import tool will prompt the operator before performing this delete operation.

The import tool relies on a special qualifier ('Full') that is present in the export file. The export tool adds this qualifier when it exports all the rules of a specified queue (i.e. no search criteria is specified when exporting the rules of a queue).

Import Log

The import process generates a log providing:

- The date/time of import
- The import arguments
- The name and type of each imported entity, indicating if the entity was added, modified or skipped.
- The entities with skipped LAU settings
- For the operator, whether the password was imported or reset.
- Summary counters providing:
  - The total number of skipped occurrences
  - The total number of added occurrences
  - The total number of updated occurrences

Approval rules

The import process does not bypass the standard approval rules that are applicable in Access when manually changing some sensitive entities. For example:

- Left and Right approval of operator changes
- Approval of schema modification

After the import process, all sensitive entities that were either added or modified are set in their corresponding approval state. A manual user intervention, from Access graphical interface, is required to approve these entities.

4 Web Platform Evolution

This section provides general information about the evolution of graphical interfaces in Access/Entry 7.0. For more detailed information specific to the Web Platform 7.0, please refer to the Alliance Web Platform 7.0 functional overview document.

4.1 Web Platform Finalisation

Overview

The finalisation of the Web Platform 7.0 consisted in supporting the administration and monitoring functions of Access and Entry, which were not yet available on release 6.3 of the Web Platform. The availability of these new functions, coupled with the existing Messenger and RMA functions (available on Web Platform 6.3 and migrated to 7.0), enables the Web Platform 7.0 to support all related Access services, using a browser based interface.

Starting from this release, the Web Platform 7.0 can be positioned as an alternative to the Workstation 7.0. The Workstation 7.0 remains available, although in maintenance mode. In general, when a new function is implemented on Access 7.0 and it requires graphical support, the implementation of its associated graphical services is only done on the Web Platform 7.0.

The Web Platform 7.0 is also available for Alliance Entry 7.0, supporting all graphical services required to operate Entry 7.0. The Workstation 7.0 remains available, in maintenance mode, for Entry 7.0.

Administration Rationalisation

With Web Platform 7.0, there was an opportunity to rationalise the current Workstation administration applications.

The main operational difference between the Web Platform and the Workstation is the use of on an 'object' based view, instead of an 'application' based view as used on the Workstation.

For example, on the Workstation, the 'Logical Terminal' entity is accessible both from the 'SWIFT Interface' application and from the 'SWIFT Support' application. On the Web Platform, as the notion of application disappears, there is a single 'Logical Terminal' entity, defined in the 'SWIFTNet Interface' group, on which all activities related to 'SWIFT Interface' and 'SWIFT Support' for a Logical Terminal are available.

The screen and display layout of the Access administration functions is harmonised with Gateway, supporting a similar layout as introduced on Web Platform 6.3 for the Gateway administration. The Access administrator primarily works with a list of objects to configure and monitor on the Web Platform 7.0. For each selected object, detailed information is displayed, and the relevant administration functions are available on the screen.

Note The security model of Access 7.0 remains based on the existing 3 levels organisation of Workstation: application, function, and permission.

The advantage of keeping this model is a straightforward migration of security data to 7.0. It makes it easy to manage security in a mixed environment, as the same permission settings are used between Workstation and Web Platform.

On Web Platform 7.0, the notion of application does not exist. The Workstation based security model is mapped to the Web Platform model (for new Access customers, using only the Web Platform, the mapping may not always be intuitive).

It is foreseen to reorganise this security model, to map to the Web Platform structure. This will be considered when the majority of existing Access/Entry customers will have stopped using the Workstation in favour of the Web Platform.

Monitoring Rationalisation

The monitoring functions, available on the Workstation, have also been rationalised when implemented on the Web Platform 7.0, available through a new 'Monitoring Dashboard' application:

- On one hand, on the Monitoring Dashboard, the detail monitoring functions are attached to their relevant object (such as detail monitoring of a logical terminal, emission/reception profile, message partner). So, when administrating an object, the user has the possibility to directly view the monitoring information (if authorised).
- On the other hand, the Monitoring Dashboard is designed to provide a more intuitive and efficient way of monitoring Access functions, compared to the Workstation 7.0 Monitoring application. The Monitoring Dashboard also supports the monitoring of multiple Access instances.

The Monitoring Dashboard provides a clear distinction between the summary, high level monitoring information, and the detailed monitoring information available for each relevant object. It is possible to directly navigate from a monitored entity on the Monitoring Dashboard to display its monitoring details, along with its configuration information (in read-only mode).

4.2 Graphical Packages

Web Platform is a modular system. It allows the plugging of new graphical elements, as the needs arise.

For Access/Entry 7.0, four graphical packages are provided to support the whole range of graphical services needed to interact with Access/Entry 7.0.

These graphical packages are further detailed below.

4.2.1 Alliance Messenger Package

The Messenger package on Web Platform includes the functionality delivered in Messenger 6.0 as well as additional enhancements. Some of the additional enhancements that are available only on the Messenger package are:

- Direct FileAct functionality (7.0, not available on Entry)
- Authorisation of FileAct messages (7.0)
- Message search criteria is enhanced with FileAct Copy, FIN Copy, Bank Priority, and MUR fields (as from 6.3)
- Report export in HTML, xls, PDF, and CSV formats (as from 6.3)
- Support for FpML messages (as from 6.2)
- Support for AnyXML message format (as from 6.2)
- Fast mode for message creation, modification, and consultation (as from 6.2)
- Minor GUI enhancements such as date, BIC and currency pickers, and variable page size (as from 6.2)

4.2.2 Alliance Relationship Management Package

The Relationship Management package on Web Platform includes the RMA functionality delivered in Workstation as well as additional enhancements. Some of the additional enhancements available on the Relationship Management package are:

- RMA audit trail: full history of an authorisation (7.0)
- Management of Authorisation for InterAct/FileAct messages (7.0)
- Cleanup of RMA authorisations, for example for authorisations of removed BICs (as from 6.3)
- Cloning/Reciprocating authorisations (as from 6.3)

- Export reports in HTML, xls, PDF, and CSV formats (as from 6.3)

4.2.3 Alliance Access/Entry Monitoring Package

The Monitoring package provides the workspace management functions of the Monitoring application and a more efficient monitoring of Access/Entry. It is now also possible to monitor several Access/Entry instances at the same time. Some new monitoring elements which are only available on the Access/Entry Monitoring package are:

- User controllable message counter: Each Message Partner, Logical Terminal and Emission/Reception Profile now maintains two long-running counters (for sent and received messages). These counters can be manually reset on the Web Platform.
- Message instance age: This is the amount of time that a message instance has spent in a queue. You can configure Access/Entry to alert you when a message has spent a certain amount of time in a queue (this is configurable per queue).
- Queue age: The queue age is the amount of time that the oldest message has spent in a queue.

4.2.4 Alliance Access/Entry Configuration Package

The Access/Entry Configuration package offers the administration and configuration features of the Workstation. Some of the new features that are only available on Access/Entry Configuration package are:

- Direct FileAct functionality (not available on Entry)
- Reset new counters for Message Partners, Emission/Reception Profiles and Logical Terminals
- Configure age threshold alert per queue. The age is the time a message has spent in a certain queue.

4.3 Monitoring Dashboard

Overview

The Monitoring Dashboard is based on existing Access monitoring concepts:

- Events

  Logged in the Event Journal, events are the main mechanism for Access health state monitoring.

- Alarms

  A special (configurable) type of event indicating abnormal situations and incidents.

- Exceptions

  An Access entity (LT, Message partner, etc.) is reported to be in an exception state when a defined condition is fulfilled. For example, a disabled Message Partner is considered to be in exception state.

The Monitoring Dashboard, available on the Web Platform 7.0, provides the following major functions.

Dashboard

The central point for Monitoring application is a single-window dashboard view, displaying the latest alarms and exceptions raised for a specific Access/Entry instance. The information is displayed on the screen in a chronological order and is refreshed at a configurable rate.

The main elements of the monitoring dashboard are:

- The left navigation tree, provide a high level, at a glance view of the Access/Entry instance(s) being monitored. Colour codes are used to indicate the overall status of an object.

  - The main Access/Entry node shows the overall status (which is a consolidation of all the objects being monitored).
  - Each monitored object is visible, with its monitoring status.
- The Exceptions and Alarms pane provides a summary of the last alarms raised for the Access being monitored and selected.

Multi-instance monitoring

The Monitoring Dashboard also provides a single consolidated view of all the monitored Access instances, bringing the following features:

- It is possible to monitor all Access instances of the infrastructure on the same screen.
- It is possible to investigate incidents and take operational actions on different Access instances within the same screen.

Additional Access instances can be included in the general monitoring tree, to show their global statuses.

The Exceptions and Alarms view shows the summary information related to the instance selected in the monitoring tree.

Monitoring Scope Definition

The Monitoring Scope Definition feature allows operators to monitor only a subset of all the LTs, Message Partners, Emission/Reception Profiles and Queues. Exceptions on the entities not included in the monitoring scope are not reported by the Monitoring application.

This feature allows a customer to adapt the monitoring view to the actual operational state. For example, a customer may have a set of LTs configured to take over from another Access instance. In a normal operation mode, it is normal that these LTs are disabled. These LTs should not be reported as an exception and they should not be monitored. However, in a takeover scenario, these LTs might become operational and should then be monitored.

5 Disaster Site Recovery Support

5.1 Enhanced Database Recovery

With the introduction of the 'Database Recovery' option in release 6.3, Alliance Access provided a mechanism to recover the database content in case of a major incident resulting in the unavailability or corruption of the database. Database Recovery allows resuming operations with up to date business data. Database Recovery requires the licence option 14:DATABASE RECOVERY to operate.

Access 7.0 enriches further Database Recovery to support the recovery of the database in a remote disaster site recovery scenario. Database Recovery now enables customers relying on the embedded Oracle database model to asynchronously replicate recovery data to the remote disaster site support. Database Recovery now support local and remote recovery scenario.

Access 7.0 also features a new Database Repair Service, used to analyse a recovered database and prevent live messages to be sent as duplicate transactions. This service is triggered automatically by Database Recovery, once the database has been recovered. This service is also available for manual invocation, typically for the case where the database is hosted in the customer Oracle infrastructure and must be investigated following its recovery on a disaster site.

In Access 7.0, the existing duplicate detection mechanism is also enhanced to detect full duplicate messages over all active days. This enhancement, which is part of core Access features, protects against accidental re-emission of messages by back-office and middleware applications, during their own recovery procedures.

For a more detailed description of the different resiliency solutions supported by Access, please refer to the Database Recovery Information Paper available on www.swift.com. This paper describes the different options supported by Database Recovery.

5.2 Hosted Database

Overview

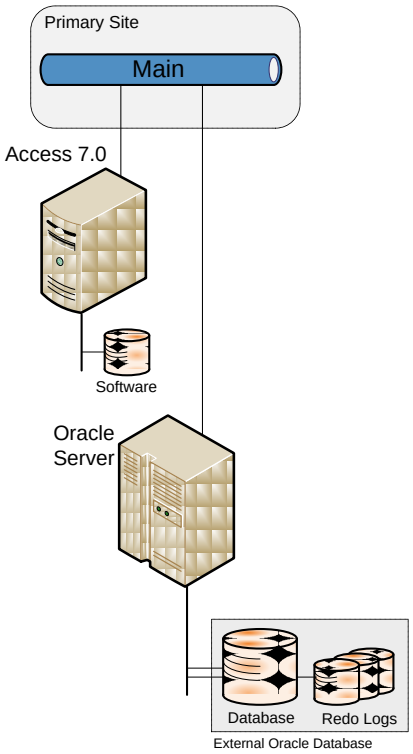
Sometimes, customers already have an Oracle infrastructure in place and have all the necessary expertise to manage and administer an operational database. Some customers prefer to manage themselves the Access Oracle database on their infrastructure, either to align with the operational procedures in place, or to benefit from the resilient infrastructure already in place (e.g. Oracle Clusters, RAC, DataGuard).

To support this configuration, Access 7.0 provides a new installation model, the 'Hosted Database' model that configures Access schema (tables and procedures) on an external Oracle instance, provided by the customer.

The Hosted Database model is available as a new installation option of Access 7.0.

This configuration assumes that the customer already has an Oracle infrastructure, with all the necessary expertise to manage it. At installation time, the customer simply needs to specify the Oracle instance where to install the Access database.

The Access software is still installed on a dedicated server system, including the Oracle client software required to handle connectivity between the Access server and the Oracle server.



Note The term Oracle instance refers to the set of Oracle processes managing a database instance, capable of hosting multiple database schemas. It will be possible to install the Access database schema on this instance, along with other schemas.

In such a configuration, the recovery of the Oracle database is managed by the customer using its own tools and procedures. This means that the Database Recovery option is not available in the hosted database configuration.

Hosted Database License

The use of the hosted database option is linked to the availability of licence ’13:HOSTED DATABASE’. This license option can be ordered free of charge.

SWIFT recommends that a customer orders this free licence option when using the hosted database model on production. It helps SWIFT identify the customers using this installation option, and ensure that incompatible options like Database Recovery are not ordered when the hosted installation model is used.

If the licence is not selected, Access will still allow the selection of the Hosted Database installation model. A warning will be provided by the installer to indicate that this licence option is required if the installation occurs in a production environment.

Architecture Resiliency

The hosted database model separates the software server (i.e. the machine running Access software) from the data server (i.e. the Oracle configuration hosting the Access database).

This architectural separation between the software and the data servers already provides a first level of additional resiliency.

In contrast with the embedded database model, where a loss of the Access server also results in the loss of its database, the loss of Access server in hosted model does not result in the lost of the Access database. The Access database, running in the hosted Oracle environment is still available, and is left 'frozen' in the situation of the failure, i.e. with a set of in-flight messages to recover.

In such a configuration, as the database is still available on the Oracle infrastructure (it is assumed that the Oracle configuration is highly resilient), the recovery of these in-flight messages can be transparently managed (i.e. without requiring the EAI to perform retrieval and re-emission logic) by reconnecting a 'dormant' Access instance that can connect to this database and process the in-flight messages.

The recovery scenario performed at that moment is identical to the one performed by the standard recovery of Alliance Access server after an unplanned shutdown (like a power supply loss or a forced immediate shutdown).

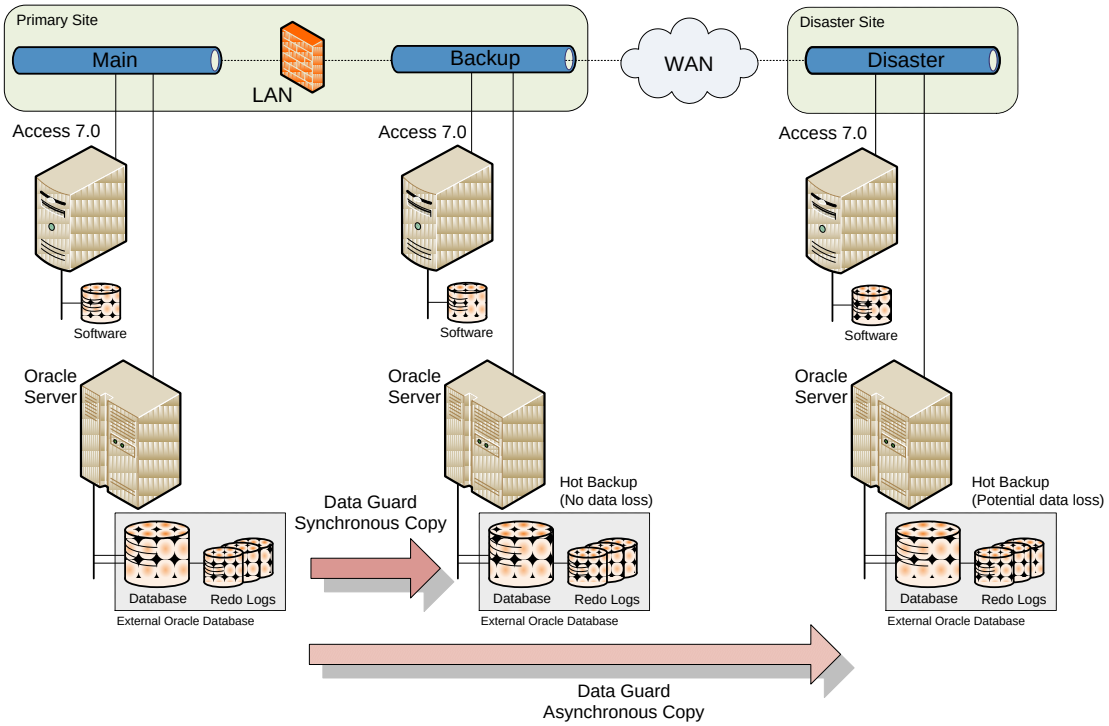
Leveraging Oracle Resilient Infrastructure

Another important reason for selecting this option is when customers have invested in setting up highly resilient Oracle infrastructure (e.g. using Oracle Clusters, Oracle RAC or Oracle Data Guard). Access will automatically benefit from these resiliency features by having its database installed in this Oracle infrastructure.

Note SWIFT does not qualify Oracle tools that can be used to setup a resilient infrastructure. The important assumption is that the use of such tools in the Oracle infrastructure remains completely transparent to Access.

Data Guard Example

The diagram below shows a recovery configuration example based on Oracle Data Guard, which can be used to maintain a replicated database, possibly simultaneously for a backup and a disaster database. The synchronous mode is used to maintain a hot standby backup, with no data loss. The asynchronous mode is used to maintain a hot standby disaster, with potential data loss.



In case of an incident on the primary site, a consistent Access database can be immediately available on the backup site. No manual intervention is required on the backup site to recover the database (hence sometimes referred to a 'hot standby').

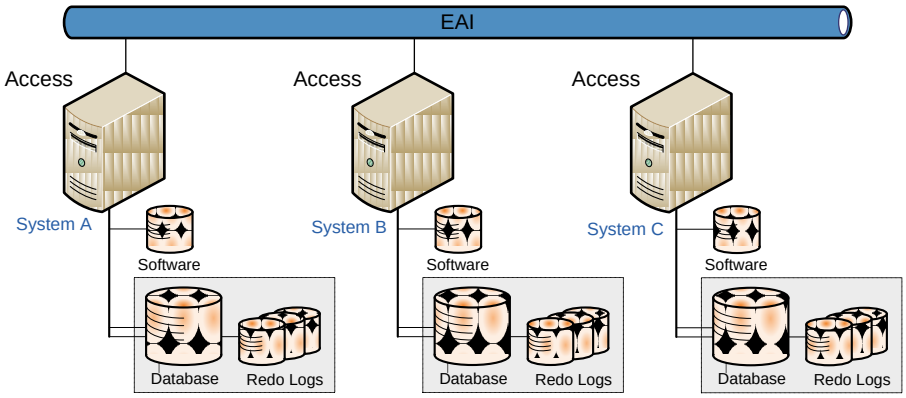
The use of Oracle Data Guard, in asynchronous mode, can also result in the same information loss as present when using Database Recovery for a disaster recovery scenario. The Database

Repair Service must be manually invoked by the administrator on the disaster site to prevent duplicate emissions.

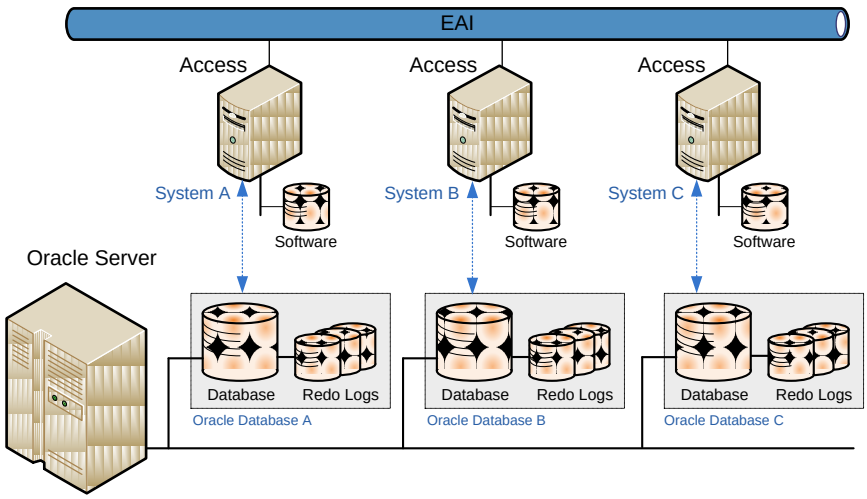
In this configuration, it is therefore the customer responsibility to execute the repair service before resuming communication with SWIFT network.

Multi Instance Configuration

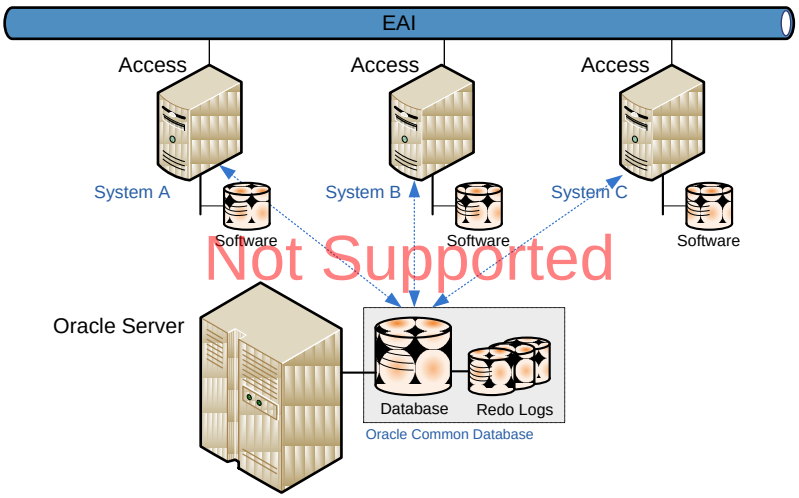
In order to implement a highly resilient and scalable architecture, customers sometimes implement a multi-instance configuration as depicted below. This is a configuration where multiple Access instances, acting as pure messaging pipes, are interfaced by a message bus middleware (or EAI).



With the hosted model, it is possible to apply the same configuration, as depicted below. Each Access instance still has its own dedicated database, hosted on the Oracle environment.



Warning The model below, where multiple Access servers are updating a **single** common Oracle database, is **not** supported. Access 7.0 will actually check this situation in hosted mode and refuse multiple concurrent connections on the database.



5.3 Database Repair Service

Overview

This service addresses the risks linked to possible duplicate emissions, either to SWIFT or to back-office application, resulting from a partial recovery of Access database (either using the 'partial' recovery function of Database Recovery option, or using Oracle Data Guard asynchronous replication).

In a disaster site take over scenario, customers' main priority is usually to resume operations as fast as possible but safely on the disaster site (to process as quickly as possible the traffic accumulated during the down-time period). The recovery of the messages affected by the incident (i.e. the messages that have been lost and must be resent) is usually done once the main message exchange flow has been re-established.

The Repair Service feature is designed to take this priority into account, i.e. to enable Access to resume traffic as quickly as possible, while providing sufficient information to later analyse the messages to recover.

PDE Trailer Addition method

The Repair Service adds a PDE trailer to all live messages present in the database. This will guarantee that any of the live recovered messages processed in the system that could result in a duplicate transaction, will never be sent without PDE trailer.

The drawback of this option is that unique messages will also be flagged with a PDE trailer.

Optional Additional Repair action

The Repair Service provides an additional action to either complete or route to an investigation queue all the live messages (already flagged with a PDE trailer).

By default, the Repair Service does not perform any additional action on the live messages. This mode provides the fastest recovery option, but with the risk of effectively sending duplicate transactions, marked with a PDE trailer.

If default action is set to route the messages to an investigation queue, no duplicate transactions are sent. A manual investigation is then required to identify the messages that must still be exchanged, and to manually re-activate or move them to the appropriate queues.

This operating mode is more suitable for customers with a limited number of live messages, and wanting to limit the risk of sending duplicate transactions, even if these transactions are flagged with a PDE trailer.

The administrator can decide whether the default action (none, complete or route) should be fixed (through the configuration of a security parameter) or should be prompted when the Repair Service tool is invoked during a recovery situation.

Live Message Repair Report

In all cases, the Repair Service generates a report, in XML format, of all live messages present in the system, at recovery time. The report includes basic message identification information, but also business information like currency/amount, value date, source entity and original queue.

This report will be used to analyse the live messages impacted by the recovery, and possibly requiring further actions. The business information is provided to enable customers to identify the high value transactions that should be investigated first.

Back-office recovery steps

Once Access is recovered, the customer is responsible to perform the remaining back-office recovery:

- For messages sent to SWIFT, the back-office systems need to re-send all messages still waiting for a SWIFT Ack.

  These are messages which have been lost between the back-office systems and Access during the recovery. It can also be the live messages completed in Access by the repair service.
- For messages received from SWIFT, the customer needs to identify the missing transactions, and either retrieve them from SWIFT (if not present in Access), or re-activate them if present in Access.

5.4 Duplicate Detection

The existing duplicate detection mechanism is enhanced in Access 7.0 to support the following features:

- Full duplicate detection

  The full message payload (FIN text block, InterAct payload, FileAct digest) is taken into account to detect a message as duplicate. The detection itself is based on the comparison of digests which include, in addition to the full message payload, the following fields for their calculation:
  - Sender: BIC11 for FIN, Requestor DN for InterAct and FileAct
  - Receiver: BIC11 for FIN, Responder DN for InterAct and FileAct
  - Direction: I or O
  - Message Type: Message Type for FIN, Request Type for InterAct and FileAct
  - Unique message reference (UUMID)
- All active days

  The detection occurs against all non-archived, live or completed messages present in the Access database.

The duplicate detection will typically be used to protect against accidental re-emission of messages by the back-office systems or by the middleware. These problems typically occur during a recovery situation.

The enhanced duplicate detection functionality is part of Access core functionality (i.e. not linked to the Database Recovery licence), meaning that it is also available for normal message flow processing (i.e. outside the scope of a recovery situation) to protect against accidental re-emission of messages.

The enhanced duplicate detection continues to use the 'possible_duplicate' routing keyword, allowing to route duplicate messages to an investigation queue. When flagged as 'possible_duplicate', this keyword now means that the message payload is a true duplicate of another message.

Warning As a consequence of this enhancement, messages with an identical UUMID (usually the same F20 field) but with a different text block will not be detected as duplicates anymore (the duplicate detection logic is extended to compare the full text).

6 Query Operational Data

6.1 Overview

Alliance Access 7.0 provides a generic Web Services layer, which allows business applications and third party applications to access specific data from Alliance Access using standard web protocols. These Web Services provide their full value only when integrated into an application developed by a partner or by the customer.

Configuration

A WSDL (Web Service Description Language) file is available that describes the services provided. In order to make use of that service, the customer or application vendor has to develop a client application. Due to the loose coupling nature of Web Services, this client application can be developed in any programming language, assuming that a toolkit is provided for that environment to interpret the WSDL file and invoke the exposed functions. The available Web Services are described in the *Alliance Access Web Services Developer Guide*.

The Web Services interface requires the application to first authenticate with credentials of an Access account (user name and password), before invoking the services. The application is able to authenticate through an interactive or an application based account. This authentication enables Alliance Access to validate the incoming request and make sure that the account used has the appropriate permissions to read the requested data.

An operator with "application password" can be defined by the security officers, the same way as for an interactive operator. These application accounts have strong password validation rules and can only be used by a non-interactive application (it is not allowed to login with an application account from Alliance Web Platform or Workstation). Furthermore these accounts are never locked in case of invalid logins and there is no login time restriction. The Access security profiles, associated to the authenticated account, determine the scope of the data that can be accessed. For more information on how to define an operator with application password, please refer to the *Alliance Access System Management Guide*, section Defining Operators.

In Alliance Access, the Web Services Service (WSS) has to be started for Alliance Access to respond to incoming requests. To start this service from the System Management application, please refer to the *Alliance Access System Management Guide*, section Stopping and Restarting Components.

The use of Web Services requires the activation of the licence option 91:WEB SERVICES, whether to be used for development or for run-time usage.

No direct SQL support

As Access is now using an embedded Oracle database, a frequent question to address reporting needs is whether a direct access to the database schema, using SQL tools (like Oracle PL-SQL interface) is allowed.

Although this approach looks quite logical from a pure technical view point, it is not supported by SWIFT for the following reasons:

- Commercially, the embedded nature of the Oracle database prohibits SWIFT from directly exposing Oracle features.
- Technically, such direct access to the Access database is operationally risky:
  - The uncontrolled nature of external SQL queries could potentially impact the Oracle engine, negatively affecting the stability and performance of Access.
  - The Access database schema has been designed to maximize performance and not to support data warehousing and reporting applications. For example, each day of activity is represented by a separate set of tables. A SQL query to build a monthly statistical report would require the union of 30+ tables.

Therefore, direct SQL queries to the Access database are not supported by SWIFT (even for the Hosted Database model). The Access database schema is not documented.

The Web Services provide the only supported method for querying Access database.

6.2 RMA Web Service

Overview

The RMA Web Service facilitates real-time retrieval and querying of RMA authorisations and of Query/Answer records by external systems. It provides the following queries:

- Get a list of RMA authorisations based on a set of search criteria;
- Get the full data of a specific RMA authorisation including references to the exchanged queries and answers;
- Get a list of query/answers based on a set of search criteria;
- Get the full data of a specific query/answer

The RMA Web Service only supports query functions. It is not possible to update or create RMA records. This service is therefore positioned for back office applications that need to query the Alliance Access RMA store to check valid relationships. This service is not suitable for synchronising RMA stores across different Alliance Access systems. For that purpose, the file export/import functionality should be used.

RMA Operations

Once the client application has successfully opened an authenticated a session with Access, it can make use of the search and get operations to read RMA authorisations and query/answer records or verify whether the exchange of messages is authorised for specified criteria. The following operations are available:

- SearchAuthorisation
- GetAuthorisation
- SearchQueryAnswer
- GetQueryAnswer
- MayExchange

When using the Search services (SearchAuthorisation and SearchQueryAnswer) the back office application provides search criteria, based on RMA fields, to retrieve corresponding authorisations or query/answers. The search criteria are similar to the search criteria available on Alliance Web Platform or Workstation. The service then returns a list of authorisations or query/answers matching the search criteria. A page based mechanism is used to handle long search results, ensuring that only a controlled limited set of information is returned to the client. The table below shows in the second column which search criteria can be used by the back office to search for authorisations. The third column shows which information is returned in the response.

The Get services (GetAuthorisation and GetQueryAnswer) allow the application to obtain the full details of a specific authorisation or query/answer. In the case of GetAuthorisation, the application must provide the RMA key (service + own BIC + correspondent BIC). The service then returns the full details of the authorisation specified. The table below shows in the fourth column the search criteria that have to be used for a GetAuthorisation. The fifth column shows which information is returned in the response.

	SearchAuth	Response	GetAuth	Response
Own BIC	x	x	x	x
Correspondent BIC	x	x	x	x
Service name	x	x	x	x
Authorisation status	x	x		x
Transmission status	x	x		x
Issued date/time	x			x
Stored date/time	x	x		x
Granularity	Y/N	Y/N		x
Time-bound: not before / not after	x	x		x
Draft / disapproved	Y/N	Y/N		Y/N
Preparation status	x	x		x
New auth: issued date/time	x			x
New auth: stored date/time	x	x		x
New auth: not before/ not after	x			x
Related Query/Answer	x			x
Audit trail				x
Reject code and Reject reason				x
Auth comment + date of comment				x
Operator name				x
Auth origin				x
Auth origin				x

MayExchange

The MayExchange service allows verifying if the exchange of messages from a specific message type or request type is authorised between institutions at a given time. This service simplifies the integration of RMA filtering logic in a back-office application. The back-office application can simply invoke the service to know whether a message exchange is allowed. Without this service, the back-office application would need to query the appropriate RMA authorisation, and implement the RMA logic to interpret its content. The table below shows in the second column

the criteria that have to be used for a MayExchange. The third column shows which information is returned in the response.

	MayExchange	Response
Own BIC	x	
Correspondent BIC	x	
Service name	x	
Type of authorisation	x	
Date date/time	x	
Message type or request type	x	
Authorisation status		x
RMA check required		x
RMA in trial period		x

6.3 Message and Event Query Service

Note The Message and Event Query Service is not included in Access 7.0 release. It will be available through a functional patch to be installed on Access 7.0.

Overview

Access 7.0 supports a new set of Web Services, the 'Message and Event Query Service', complementing the RMA Web Services already provided with Access 6.3.

This new service offers the capability to search and query messages and events present in the Access database. The service implementation is similar to the RMA search and query service already implemented on Access 6.3:

- Message/Event Search Service

  The Message/Event Search Service enables an application to search for messages and events in the database. As input, a filtering criteria is provided to the service, which provides on output the list of messages or events matching the criteria.

  The main search criteria is based on the message/event creation date. Additional fields are also available in the search criteria (such as message type).

- Message/Event Query Service

  The Message/Event Query Service returns the details of a specific message or event, in a documented XML structure:

  – For a message, the different records constituting a message (the message header, the text, the instances and their associated network and system interventions) are returned.

    For each record, the fields returned are most of the fields visible when consulting a message through the Workstation or Web Platform.

The XML support for repetitive and hierarchical representation enables to represent, in a single document, all the message elements (header, text, instances and associated interventions).

- For an event, the fields returned are most of the fields visible when consulting an event through the Workstation or Web Platform.

- Archive Access Support

  The Message/Event Web Service can access messages and events for active days but can also access messages and events in archived days, as long as these archived days are not removed from the database. It can also access message and event in archived days restored in Access database using the restore of backup of messages or events function.

  The Message/Event Web Service indicates that the message or event returned by the query service is either coming from an active or an archived day.

Note The access to archived days of messages and events primarily guarantees that the information used for reporting is complete and non-changeable and can reliably be used for audit reporting. The access to information on active days, even for completed transactions, is never 100% reliable. The information is still subject to change, as it is always possible to re-activate a message.

Benefits

The main benefit of this Message Query Service is to address the needs for analysing, from an external application, the operational data present in Access database. This operational data consists of:

- FIN, InterAct or FileAct messages, providing both the business data (text block, InterAct payload) and the message audit trail (i.e. the message history within Access).
- Events, providing the details for each event.

The needs for an external analysis of operational data are multiple. The list below gives some typical needs:

- Audit Reporting

  The ability to trace in detail the history of a financial transaction, including its business content.

- End of Day Reporting

  The ability to generate message traffic statistics, either on a specific transaction (e.g. to calculate the time taken to process the whole message flow in Access) or on a group of transactions (e.g. statistics on message traffic per day, week or month, peak traffic hours, etc).

- External Archiving

  The need to incorporate into external archiving systems, in a specific format, large volumes of messages, containing all the required audit information (typically the transaction header and business data, along with its Access audit trail).

Positioning against ADK

The ADK also provides means to query message and event information in the Access database.

The Message/Event Query Web Service provides an easier method to query this information in the database, using standard technology, based on Web Service Description Language (WSDL file).

The Message/Event Query Web Service does not allow, like for ADK, to extract specific fields of a message or an event. The service returns by default all the fields associated to a message or event record. The service is therefore easier to implement, at the cost of being less efficient than an ADK application. For this reason, the Message/Query Web Service is positioned for 'end of day' reporting, i.e. extraction of information when the transaction is completed, while ADK is better suited for real-time query of individual message/event fields.

On the other hand, the ADK remains the only solution to integrate external applications into Access main message flow (via the creation of additional ADK based queues, integrated in the whole Access routing).

7 SOAP Host Adapter

The embedded SOAP Host Adapter offers an alternative to the MQ Host Adapter, providing an interactive, real-time exchange of MT/MX messages between Access and back office applications.

The SOAP adapter does not yet support FileAct messages, but it is planned to support it as well.

Some important characteristics of the SOAP adapter are:

- Data transferred over a SOAP connection must use the XMLv2 format. This format is already used by other Access host adapters (File Transfer, MQHA and MQSA).

  The SOAP adapter requires the XMLv2 revision 2 level at minimum.
- The SOAP communication channel supports session management and duplicate prevention, and can as such guarantee a one time delivery.
- The communication is always initiated by the back office. Therefore, only a SOAP client is required in the back office. Alliance Access acts as the SOAP server.

Licence 14:AI SOAP ADAPTER is required for using the SOAP host adapter.

7.1 Configuration

The SOAP adapter is based on Web Services technology. A WSDL (Web Service Description Language) file is provided to describe the operations supported by the SOAP adapter. In order to make use this adapter, the customer or application vendor has to develop a client application making use of these services. Due to the loose coupling nature of Web Services, this client application can be developed in any programming language, assuming that a toolkit is provided for that environment to interpret the WSDL file and invoke the exposed functions.

The client application must provide the MT or MX messages using Access XMLv2 representation, using Revision 2 at a minimum. XMLv2 specifications can be found in the *System Management Guide*, Appendix E, section XML Format 2.

In Alliance Access, the Web Services Service (WSS) subsystem has to be started for Access to respond to incoming requests. To start this service from the System Management application, please refer to the *System Management Guide*, section Stopping and Restarting Components.

Note The SOAP adapter and the Web Services interface should not be confused, although they both rely on Web Service technology. SOAP is a back-office adapter, providing all the logic to reliably exchange messages between Access and a back-office application, while the Web Service interface is a new method to query the content of Access database.

7.2 Session handling

In order to exchange messages, the client application first needs to open a session with Access. Compared with the Query Web Services which requires authentication, the back office does not have to provide a user name and password. Authentication is possible by specifying an LAU key in the back office and the message partner name. Once the session is open, the back office application initiates the requests to either send messages to Access or to receive messages from Access. Although the SOAP message partner can be configured for bi-directional traffic, in most cases, the back office application will dedicate a separate channel for emission and reception.

To open a session, the back office has to send an open request to Access. Access answers with an open response containing a session token. This token uniquely identifies the session and should be put in all the exchanged SOAP requests of that session. When the message exchange is finished, the back office closes the session with a close request.

In order to guarantee recoverability of the connection, the SOAP adapter uses a window size concept. The window size is a configurable value in the message partner. It defines the number

of messages that the back office application can send or receive, and that will be recovered in case of an interruption of the link. The value should be between 1 and 10.

To guarantee one-time delivery, messages should have a unique sequence number. This sequence number is generated automatically by Access when it sends messages to the back-office. It is provided as a sequential continuous number by the back-office when the messages are emitted by the back-office to Access. This unique number is used either by the back-office or by Alliance Access to identify the message and determine if the message has already been sent or received.

The SOAP protocol and the window size concept are explained in detail in the *System Management Guide*, Appendix G, section SOAP.

7.3 Emission logic

In emission mode, the back office application uses the ‘put’ request to send an XMLv2 message to Access. This XMLv2 message contains an MT or MX message. When Access has successfully received this message and stored the MT/MX message in the database, it sends a put response confirmation to the back office.

As for all message partners, messages received via a SOAP message partner are created in the _AI_from_APPLI queue. From there, normal Access routing rules apply to process the messages from the _AI_from_APPLI queue to SWIFT.

7.4 Reception logic

When messages are received from SWIFT, Access routing is used to route these messages to a SOAP message partner. The back office application must ‘poll’ for new messages waiting in the message partner for delivery to the back office.

In order to provide an optimised throughput, the back office application can in the same request acknowledge the previous message received while asking for the next message to receive. This is accomplished via the 'Get and Ack' request. In a 'Get and Ack' request, the back office:

- Asks Access to send the next available message
- Optionally acknowledges a previously received message

A separate 'Ack' request is available to the back office application to only acknowledge a message, without requesting for another message.

To reduce the number of poll requests when no new messages are present in the message partner, a timeout can be specified in the 'Get and Ack' request. This timeout defines an interval (in seconds) to wait before Access replies to the 'Get and Ack' request that no new messages are present in the message partner. If, during this wait interval, a new message becomes available, Access will then immediately reply to the 'Get and Ack' request with a response containing this message.

8 FileAct Support

Access 6.3 initiated the support for FileAct, limited to the File Transfer adapter. With release 7.0, FileAct support has been extended to the MQHA adapter.

Access 7.0 also provides a new adapter, the 'Direct FileAct' adapter, which can also be used by back-office applications for FileAct integration. The use of this new adapter is subject to the activation of a new licence option.

This section provides a summary description how FileAct is supported in Access.

8.1 General Principles

Overview

With FileAct support, Access now provides a single integration window for back-office applications to support all SWIFT services (FIN, InterAct or FileAct).

Access fully supports FileAct store-and-forward mode. Access partially supports FileAct in real-time mode. The limitations are further documented below.

No specific licence is required to use FileAct through the File Transfer (Access/Entry) and MQHA adapter (Access only). The generation of FileAct transaction, through these adapters, requires the use of the XMLv2 format. Since release 6.3, this format is supported by all adapters, without any additional licence option (i.e. the previous licence option 19:AI FILE XML is now included in Access).

The FileAct traffic is included in the overall band calculation of Access, per destination, as described in SWIFT Price List.

File based message

Access integrates FileAct transactions in the database by supporting a new message format, i.e. a 'File' based message (on top of FIN or XML-based messages).

As for other message formats, a file based message can be generated by Access message partners. The file based message can be searched and consulted using the same applications as for FIN or MX messages (i.e. Messenger on the Web Platform or Message File on Workstation).

The FileAct header fields, including the enhanced FileAct header, can be consulted in Access. Other common message elements like message history can also be consulted. Some specific FileAct information is also available (such as Transfer Info, File Digest). The file content (i.e. the file payload) is never visible in Access. Refer to the 'File Storage' section for more details how the file payload is managed in Access.

By extending the message concept to files, FileAct transactions benefit from the rich messaging features of Alliance Access (consulting, routing, monitoring, resiliency, archiving).

XMLv2 usage

The creation of a FileAct transaction through the File Transfer or the MQHA adapter requires that the back office provides the FileAct settings necessary to generate the transaction using Access XMLv2 representation (the XMLv2 revision 2, at least, is required).

Monitoring

Access provides graphical monitoring of file transfers (the Monitoring application on Workstation or the Monitoring Dashboard on Web Platform). The monitoring application shows the file transfers in progress, indicating the percentage of total file size already sent or received.

It is also possible to abort an ongoing File Transfer from the Monitoring graphical interfaces.

Various events are also generated during a file exchange session. The event "File Emission Progress" shows in percentage (%) how much of the total file size has been transferred. These

events can be forwarded to external applications, using the SNMP protocol, to support external monitoring file transfers.

File Storage

When processing a file, Access stores the content of the file into the database. A special area of the database (a dedicated 'saa_file.dbf' tablespace) is used to store this file content.

Access stores the file content in the database to ensure that the file is always accessible when needed for an operation (like sending the file to SWIFTNet, re-activating a file transaction).

As a general rule, the file content is internally stored in Access database but is not visible to end-users, or to external applications (like the ADK interface or the Message Query interface).

The file content is physically deleted from the database when the associated file message is archived in Access. This also means that the file content is not included in the backup of message archives. The message backup does however contain the file digest.

8.2 File Transfer Support

Configuration

The File Transfer adapter requires two directories:

- The 'Input Attachment Path' directory where the actual payload file resides
- The 'Input File Path' directory where the file containing the FileAct XMLv2 settings must be stored.

The back-office application must be able to send and receive XMLv2 messages. The tag "Format" in XMLv2 revision 2 is enhanced to support the value "File" (to identify the transaction as a FileAct message). The tag "Body" must contain the physical file name. More information on the XMLv2 format can be found in the *Alliance Access System Management Guide*, appendix E, section XML Format 2.

SWIFTNet emission and reception profiles have to be configured in the SWIFTNet Interface application. For emission profiles the Messaging Service should be defined as FileAct or both (InterAct and FileAct). Store-and-Forward reception profiles should be defined to receive InterAct, FileAct or system messages, or a mix of those. When receiving different kinds of messages, priority will be given to the first one in the list. More information on how to set up emission/reception profiles can be found in the *Alliance Access System Management Guide*, section 16 Defining SWIFTNet Profiles.

The Access routing needs to be configured to route the file messages correctly from input message partners to _SI_to_SWIFTNet and from _SI_from_SWIFTNet to the correct output message partner. For the routing of file messages, new routing keywords are available such as file size and file logical name (file name as sent over SWIFTNet). Keywords already available for InterAct that are shared with FileAct can also be used (like RequestorDN or ResponderDN).

Emission logic

The emission logic is as follows:

- The back office stores the payload file in the input attachment directory and puts the XMLv2 file in the message partner input directory.

  The payload file must be provided before the XMLv2 file.
- The message partner will detect the XMLv2 file either automatically (if AFT (Automatic File Transfer) is activated) or on manual initiation of a message partner session.
- Access analyses the XMLv2 file. When it identifies a File message. Access will get the path to the payload file from the message partner configuration and the physical file name of the payload file from the XMLv2 message.
- The FileAct header information (Requestor DN, Responder DN, Service Name, Request Type) is retrieved from the XMLv2 file.

- If the payload file is correctly stored in the database, Access creates a "File" message. The payload file and XMLv2 file are moved to the backup directory.
- The routing rules should send the file message eventually to _SI_to_SWIFTNet.
- Eventually, the FileAct request is created and sent to SWIFTNet.
- If requested, a delivery notification can be received and forwarded to the back office.

Reception logic

The reception logic is as follows:

- Alliance Access receives an incoming SWIFTNet File Transfer request via an activated SWIFTNet reception profile.
- Once the File Transfer is complete (the file payload is stored in the database), Access creates a File message.
- The routing rules send the file message to the relevant exit point from which it will be processed by an output message partner.
- When the message partner session is run (automatically or manually), it stores the payload file in the output attachment directory. Access 7.0 generates the physical file name based on the logical file description (with Access 6.3, the file name was an automatically generated file name). The extension of the file is as configured in the message partner. Furthermore, an XMLv2 file is produced containing FileAct detailed information (such as the HeaderInfo) on this transaction.

8.3 MQ Support

Overview

With Access 7.0, the MQHA adapter is enhanced to support FileAct flows over IBM WebSphere MQ.

Note MQSA 7.0 does not support FileAct.

FileAct support over MQ requires the usage of the XMLv2 data format. The back-office application must provide the FileAct settings, using the XMLv2 data format.

MQHA supports two different modes (Full & Mixed mode) to transfer the payload file.

Mixed Mode

In Mixed mode, the payload file is provided to Access 7.0 and stored in a local directory, defined in the WebSphere MQ message partner.

The MQ channel is only used by the back-office to transmit the XMLv2 message. This XMLv2 message provides the actual name of the payload file. The reception of the XMLv2 message by Access 7.0 triggers the processing of the payload file in Access.

The exchange method is very similar to the File Transfer method. In both cases, the payload file is transferred 'as a whole' between the back office and Access 7.0. The difference is how the XMLv2 message is transferred (through an MQ message for MQ or as a separate file for the File Transfer).

For emitting a file, the back office must transfer the payload file to Access, into the local directory associated to the WebSphere MQ message partner, create the XMLv2 message and send it over MQ to Access.

For receiving a file, the back office will receive through the MQ channel the XMLv2 message generated by Access. Upon reception of this MQ message, the back office is responsible for locating the file present in the local directory of the MQ message partner and to transfer this file to the back-office.

Full Mode

In Full mode, all information (XMLv2 settings and payload file) is exchanged through a single MQ queue.

In full mode, multiple MQ messages must be created in order to generate a FileAct transaction. Access 7.0 makes use of MQ Message Group feature, along with segmentation support, to ensure that all the MQ messages needed for a FileAct transaction are treated as a whole.

The MQ Message Group must include at least 2 MQ messages:

- The first MQ message in the group provides the FileAct settings using the XMLv2 representation.
- The following MQ messages provide the file payload. It is necessary to segment a large file into multiple MQ messages.

This grouping of XMLv2 message and file payload into a single MQ Message Group allows the FileAct transaction to be sent over a single MQ queue.

When sending a file to SWIFTNet, it is the responsibility of the back-office application to generate the MQ message group, to create the initial XMv2 message and to convert the file data into one or multiple MQ messages.

When receiving a file, Access 7.0 will automatically generate the MQ message group. The split of file payload in multiple messages is controlled by a configuration parameter determining the maximum MQ message size. It is the responsibility of the back-office application to extract the MQ messages from the Message group and to reconstitute the payload file.

Resiliency

The MQHA adapter uses generic WebSphere MQ functionality to ensure that it does not end up with partial messages.

When reading FileAct messages from the MQ queue, MQHA will only process messages for which all the MQ segments are available. If a MQ segment of a FileAct message is missing, the FileAct message is not read by the MQHA adapter. If all the MQ segments of a FileAct message are present, MQHA starts a transaction when the first segment is read and commits it once the FileAct message is successfully added in the Alliance Access database.

When sending FileAct messages to a MQ queue, MQHA starts a transaction before sending the XMLv2 message containing the FileAct settings and commits it after the last MQ segment has been sent. This ensures that MQHA will only route the FileAct message in Alliance Access once it has been successfully sent to the MQ queue.

8.4 SOAP Support

Access 7.0 does not yet support FileAct over the SOAP connection method. This support is planned for a future update of Access 7.0.

8.5 Real-Time File Get Support

The Real-Time File Get operation allows an application or a user to request the reception of a specific file from a correspondent, using a FileAct real-time service. A typical usage example is the regular download of directories.

Access 7.0 provides a command-line tool to initiate the reception of a specific file over FileAct.

Note FileAct real-time mode also describes the Get operation, acting as a server (also referred to 'FileAct download server'). Access 7.0 does not support this mode, meaning that it cannot act as a FileAct server, responding to file get requests initiated by correspondent's.

This command can be invoked interactively from a command prompt or from a script, allowing it to be invoked from an external scheduler.

The command invocation initiates the file transfer and returns as soon as the FileAct negotiation has been successfully accepted by the correspondent. The actual reception of the file follows the normal route in Access, i.e. reception of the file through the specified SWIFTNet Reception profile, routing to a message partner for transmission to a back-office application.

No additional licence is required to use this functionality.

Note Access 7.0 currently only provides a command-line based initiation. An equivalent initiation available from a graphical interface on Web Platform is under study for a future update of Access 7.0.

8.6 Direct FileAct Adapter

Introduction

To initiate a file transfer, Access 7.0 File Transfer and MQHA adapters require the back office to provide the payload file but also the FileAct settings, using Access XMLv2 data format (either as a separate file or as an MQ message). The integration with Access to use FileAct services requires therefore the creation of an XML file.

In some situations, this additional XML development to integrate Access FileAct capabilities into back-office systems can be a significant effort. The customers with a limited number of FileAct correspondents are looking for a simpler integration solution, allowing them to only provide the payload file and to rely on Access configuration settings to generate the associated FileAct transaction. This avoids the adaptation of the back-office applications to produce the XMLv2 file.

Note Customers having the necessary skills and resources to produce an XMLv2 file sometimes require such a configuration based approach to easily prototype a new FileAct service. This easy and cost effective set-up helps them build the business case before investing the required development resources to implement an XMLv2 based integration.

Direct FileAct Connection Method

To address this integration requirement, Access 7.0 supports a new adapter type, the 'Direct FileAct' adapter, supporting FileAct flows based on providing payload files only.

The use of the 'Direct FileAct' adapter requires the activation of the licence option 22:DIRECT FILEACT.

The 'Direct FileAct' adapter allows configuring Message Partners to automatically exchange payload files over FileAct. The 'Direct FileAct' Message Partner is bidirectional; supporting the reception of incoming FileAct files from a directory, and supporting the emission of outgoing FileAct files and network delivery notifications into another directory. Each 'Direct FileAct' message partner holds the FileAct settings to be used.

The 'Direct FileAct' adapter creates an association between a directory and a FileAct correspondent, allowing back-office systems to exchange payload files only.

For more information on this new Direct FileAct adapter, please refer to the Direct FileAct paper available on swift.com

Sending Files

The 'Direct FileAct' adapter can operate in automatic or manual mode for session initiation.

In automatic mode, Access automatically picks the files dropped by the back-office systems, in the configured input directory.

In manual mode, the user activates the session, selecting the (payload) file to be sent. This method provides a mechanism in Access 7.0 to manually initiate the emission of a file over FileAct.

In both automatic and manual modes, Access uses the FileAct settings stored in the associated Message Partner handling the file to generate the FileAct message in Access and route the message internally to send it to SWIFT.

Note The FileAct functionality supported by the File Transfer Message Partner is not practical for interactive use, because to initiate a session, the operator must select the XMLv2 file and not the payload file.

Network ACK and delivery notifications

As per standard Access routing, the network (N)ACKs and delivery notifications can be routed to an Exit Point.

When the Exit Point is associated to a 'Direct FileAct' Message Partner, the routed notification generates a 'response' file:

- A single response file is produced per notification
- The file name follows a convention to map the notification status with the file name extension (e.g. <file>.OK, <file>.err, <file>.dlok, <file>.dlnok).
- The response file is empty

The naming convention for response files allows a back office to monitor the status of a FileAct emission, using a simple directory/filename parsing logic.

The response file only provides a notification status, based on its extension name. The response file does not provide additional details (as it is empty). If the back-office needs to obtain more information on a FileAct exchange, a notification report using the XMLv2 format should be generated (by the File Transfer Message Partner).

Receiving Files

Access allows routing of incoming FileAct transactions to a 'Direct FileAct' Message Partner. The Message Partner only produces the payload file (based on the logical name), without producing an additional XMLv2 based file to contain the FileAct settings.

This mode can be used by back-office applications processing payload files only and not interested in examining the FileAct settings detailed in the associated XMLv2 file (when using a File Transfer based message partner).

Support on Web Platform only

The setup of 'Direct FileAct' based message partners is only available on the Web Platform 7.0.

The manual initiation of a Direct FileAct message partner session is only available from the Web Platform as well.

The 'Direct FileAct' based message partners are visible on Workstation 7.0 Application Interface but their details cannot be visualised, and consequently acted upon, on the Workstation.

Gateway FTA similarities and differences

A similar integration technique is already supported by the File Transfer Agent (FTA) on Gateway, which allows an end user or a back-office application to drop a payload file in a pre-configured Gateway directory. Each directory is associated with a given correspondent and has specific FileAct settings. When a file is dropped in the directory, the settings are used to automatically send the file to the correspondent over FileAct.

These similarities between 'Direct FileAct' and Gateway FTA are done on purpose to facilitate the migration of an FTA based integration to Access. There are however some noticeable differences between the two implementations:

- The response file (.<OK>, .<ERR>, …) is empty. An XMLv2 based notification must be created if more transmission details must be integrated with the back office.

- The FTA parameter file on Gateway, which can optionally be used to provide FileAct settings, is not supported on Access. This means that specific SWIFTNet features cannot be set by the back-office when using the Direct FileAct connection method.
- If a back-office application has developed logic to generate the FTA parameter file, the File Transfer adapter of Access should be used. The FTA parameters must be mapped to the XMLv2 data format supported by Access.

  The dependency between the payload file and the parameter file is also different between Access and Gateway.

  – On Gateway, the parameter file must be provided before the payload file, as the payload file is the trigger for the file exchange.
  – On Access, the XMLv2 file is the trigger, so the payload file must be provided before the XMLv2 file.

8.7 Other enhancements

Enhanced file naming on reception

Access/Entry 7.0 now derives the physical file name of an output file it produces from the logical file name provided with the FileAct transaction (in prior 6.3 release, the file name was based on an internal reference, which had no meaning to a back-office application).

To generate this physical file name, Access eliminates from the logical name any characters that are invalid for a physical file name, and adds the necessary suffix information to the file name to guarantee its uniqueness (the suffix is derived from the SWIFTNet transfer reference).

This output file name is often important information to allow a back office to interpret a file. This is particularly true for the 'Direct FileAct' mode, which only produces a payload file without accompanying XMLv2 file.

File Authorisation

Access/Entry 7.0 supports the authorisation of FileAct transaction. Similarly to FIN and InterAct messages, it is possible to route FileAct messages to the authorisation queue where they need to be manually authorised by an operator.

The authorisation of FileAct transaction is only available on Web Platform. The authorisation application allows viewing the various FileAct settings, including the optional enhanced FileAct header, before authorising the message. The file content remains invisible to any Access users.

RMA Support

Access/Entry 7.0 supports the management of RMA authorisations related to FileAct traffic and the associated RMA filtering. Further information is available in section 9.1.

9 RMA Evolution

9.1 RMA beyond FIN

The Access/Entry 7.0 RMA application, already supporting the management of FIN based authorisations, is enhanced to support the management of InterAct and FileAct based authorisations.

The RMA filtering, currently handling FIN traffic only, is enhanced to filter InterAct and FileAct messages.

Note For each InterAct and FileAct service, the corresponding ASP loaded in Access/Entry defines the RMA characteristics.

Consequently, Access/Entry 7.0 can support the coexistence within the same system, of a mix of InterAct and FileAct services, some being subject to RMA filtering and others not.

9.2 Functional Enhancements

This section explains which RMA functional enhancements are implemented in Access/Entry 7.0. Except where mentioned differently, the enhancements are implemented both in Workstation and Web Platform.

9.2.1 RMA audit trail

Access/Entry already provides a detailed audit trail of all actions performed on an authorisation, via the event journal. The event distribution for RMA provides a complete list of event to trace these actions. RMA related actions are always logged (RMS events have a fixed distribution).

It is however difficult to rely on these events to analyse the audit trail of an RMA authorisation:

- Events have a short retention period

  Events are archived frequently. After a few days, they are removed from Access/Entry database. RMA authorisations have a long life in Access/Entry. The analysis of their whole history will require restoring multiple event archives.

- No summary view

  Although it is possible to limit the search to RMA events, it is not simple to generate a summary view of all the events that occurred on a specific authorisation.

In order to address above limitations, Access/Entry 7.0 provides a new RMA audit trail, associated with each RMA authorisation (sent and received). This trail, visible with each RMA authorisation (on the Web Platform only), displays in chronological order the list of all actions performed on the authorisation. The trail provides the necessary information to understand the authorisation history, without having to consult the details of associated RMA InterAct messages and events.

Query & Answer operations, when associated with an authorisation, are included in the audit trail.

The Access 7.0 RMA Web Services is adapted to return this audit trail field, in addition to the other RMA fields already exposed.

9.2.2 Transmission status

Overview

In previous Access/Entry release, in order to know the transmission status of an RMA authorisation, it was necessary to locate the associated RMA InterAct message with the Message File Application to determine the transmission status.

Since release 6.3, Access/Entry supports a new network transmission status for each authorisation to receive, directly providing the status of the underlying RMA InterAct message.

This transmission status can be seen directly from the Relationship Management Application. The possible values are:

- Waiting Transmission, the RMA InterAct message is waiting to be transmitted over SWIFTNet
- Transmission Failed, the RMA InterAct message failed delivery to SWIFT
- Sent to Correspondent, the RMA InterAct message has been sent over SWIFTNet and was received in the SWIFT central systems. This does not mean that the correspondent received the message already.
- Not delivered to Correspondent, the RMA InterAct message could not be delivered to the correspondent.
- Delivered to Correspondent: this status is only available when a delivery notification has been requested for the underlying RMA InterAct message.

The RMA application also allows to search for RMA authorisations based on their specific transmission status.

Enabled Status

Because of this new transmission status, the status of an authorisation will remain ‘enabled’, even if the underlying RMA InterAct message failed delivery.

Previously, the state was reset back to ‘Draft’ when the underlying RMA message could not be sent.

Full Support of 'Not Delivered to Correspondent'

In order to support the 'Not delivered to correspondent', Access 6.3 required that the underlying InterAct message was still present in the database. In most situations, this condition could not be satisfied, as the underlying InterAct message is usually already archived when the delivery notification failure is received after 14 days.

Access/Entry 7.0 internal reconciliation process has been enhanced to fully support the 'Not Delivered to Correspondent' RMA transmission status, even when the underlying RMA InterAct message has already been archived or removed from Access/Entry database.

9.2.3 Cleanup of obsolete authorisations

Access/Entry 7.0 now allows to clean up RMA authorisations for which there is no BIC defined in the Correspondent Information File (CIF). This operation is typically required when BIC entries are removed from the CIF, following a monthly BIC update, and an easy to use process is needed to identify the authorisations that are invalidated by this update.

A 2-step process allows cleaning up these authorisations without sending a RMA InterAct message. The process is as follows:

- Marking the authorisation as stale

  A specialised search will compare the existing authorisations against the BICs present in the CIF. A list will be displayed showing all authorisations for which there is no BIC in the CIF (either when the own BIC or the correspondent BIC is not present). From the list, an operator, with the appropriate permission, can optionally unmark the authorisations that should not be marked as stale.

  In case a customer has valid authorisations for internal BICs, not available in the CIF, it will be recommended to create internal entries in the CIF to avoid displaying these authorisations on each comparison search.

  This operation is only available on Web Platform.
- Deleting the authorisation from the RMA store

In the cleanup window for stale authorisations a new checkbox is provided: "Authorisations without BIC in Correspondent Info". The operator can select this new option to delete these authorisations.

This operation is only available on Web Platform.

This procedure does not cover the deletion of authorisations related to Test & Training BICs.

9.2.4 Automatic export on change

An operator, with the appropriate permission can configure the system to automatically export authorisations as soon as they are changed. The change can either result from a server action when receiving an RMA InterAct message, or from a user action done on Alliance Workstation or Alliance Web Platform.

The export type is partial and contains only 1 authorisation per file.

The file is generated on the server, with a unique file name, built with the BIC of the contained authorisation. This BIC information, included in the file name, will help distribute RMA changes over multiple systems (e.g. service bureau or multi instances configurations)

9.2.5 Auto Acceptance of modifications

Access/Entry supports a new security parameter "Auto Accept Updates". When this parameter is configured to "true", all incoming modifications of existing and enabled authorisations to send are automatically accepted by the Access/Entry server.

9.2.6 'Treated' attribute for query/answer

Each query/answer record has a new 'Treated' attribute indicating if the query/answer has been treated or not. This is a boolean variable with 2 possible values: yes/no. By default the 'Treated' attribute of a new query/answer is set to 'no'.

When viewing the details of a query/answer an operator, with appropriate entitlements, can manually set the treated status to 'yes'. Note that once the treated status of a query/answer has been set to 'yes', it cannot be set back to 'no'.

It is also possible to search for query/answer records based on their treated status.

9.2.7 Miscellaneous Enhancements

The following additional functional enhancements are available in Access/Entry:

- When an authorisation is modified an event will be logged in the Event Journal containing the new and old authorisation details. This event will always be journalised.
- During an automatic export of authorisation Access/Entry will make sure the back office cannot access the export file before writing is finished.
- The authorisation list report now contains the number of entries in the report (both when printing with or without details).

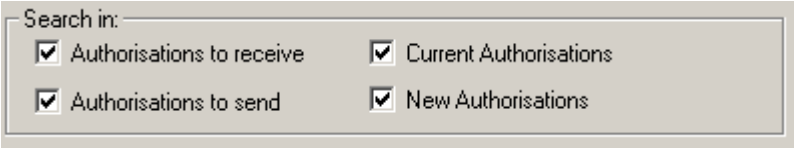
9.3 Usability Enhancements

This section lists various enhancements designed to make authorisation management easier.

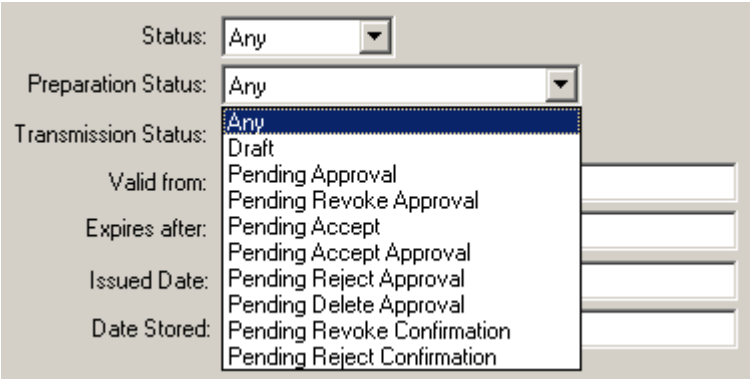
9.3.1 Excluding draft authorisations from search

The search functions now permits to only search for current authorisations and exclude new authorisations. New authorisations are authorisations having a status of draft, pending approval, pending accept, pending confirmation, ... Therefore the result will give only authorisations that can be used at that time.

This is implemented via a new checkbox "New Authorisations" in the Authorisation Search Criteria.



When this box is unselected, all new authorisations are excluded from the search. When selecting this checkbox, a dropdown field "Preparation Status" appears, listing all possible preparation statuses. The preparation status dropdown allows the selection of one of the internal statuses an authorisation can have (for example draft, pending reject approval, ...) or the value 'Any'.



9.3.2 Search for unilateral relationships

The search functions now permits to search for unilateral relationships, i.e. authorisation to receive without the corresponding authorisation to send and vice versa. This feature is only available on Web Platform.

The unilateral search will return authorisations that match the following:

- Own BIC, Correspondent BIC and Service (can optionally be filled in)
- The authorisation to receive is valid and the authorisation to send does not exist or is invalid
- The authorisation to send is valid and the authorisation to receive does not exist or is invalid

It is also possible to limit the search to authorisations to receive or authorisations to send instead of search for all unilateral authorisations.

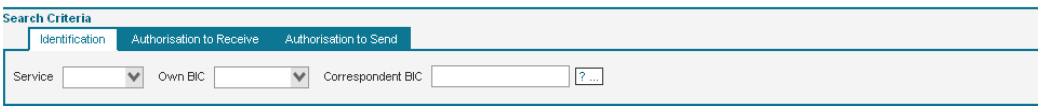
9.3.3 Search for all authorisation statuses

Up to now it was only possible to search for a specific authorisation status (i.e. enabled, revoked, draft, ...). It is now possible to search for all authorisation statuses (both current and new) in one search.

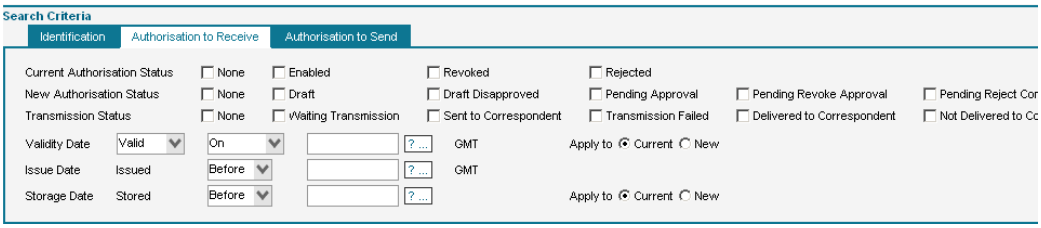
This feature is only available on Web Platform.

The general search window contains 3 tabs:

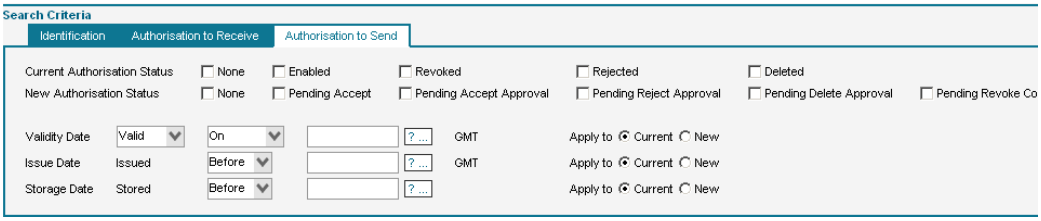
- Identification: Own BIC, Correspondent BIC and Service can optionally be filled in



- Authorisation to Receive: the current authorisation statuses are displayed as checkboxes. The possibilities are Enabled, Revoked and Rejected. The new authorisation statuses are displayed similarly with checkboxes.



- Authorisation to Send: the current authorisation statuses are displayed as checkboxes. The possibilities are Enabled, Revoked, Rejected and Deleted. The new authorisation statuses are displayed similarly with checkboxes.



It is possible to select any number of these checkboxes or none to search for everything.

9.3.4 Display enhancements

It is now easier to determine if an authorisation can be used for the sending and/or receiving of messages. This feature is provided as an extra column to quickly visualise the validity of an authorisation.

This feature is only available on Web Platform.

In the list of authorisations there is a new column "Validity" both for the authorisation to send and the authorisation to receive. The possible values are valid, not yet valid, expired, or invalid. Furthermore the summary screen also displays the start date and end date of time bound authorisations in two separate columns.

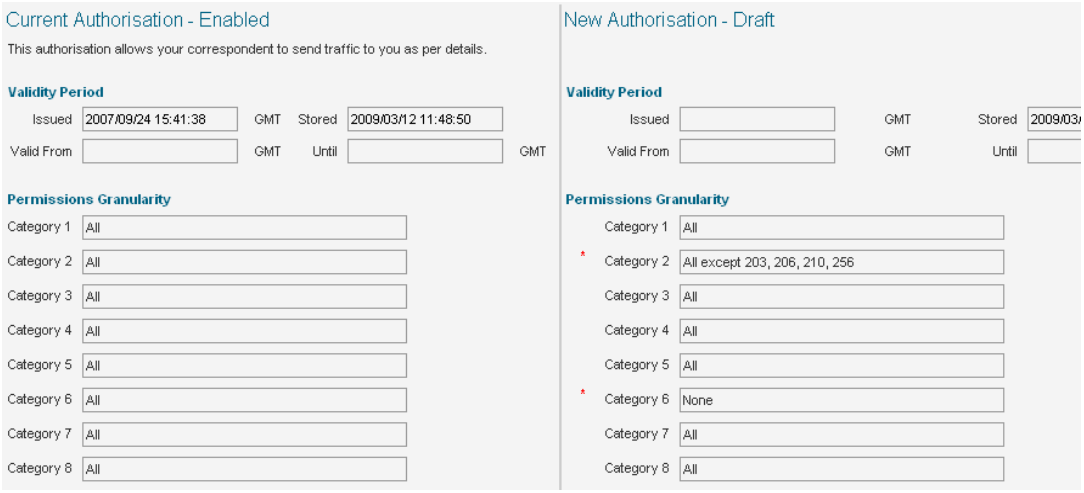
Another enhancement is the possibility to hide and move displayed columns in the summary screen. It allows customers to tune the display to their own needs. In order to differentiate between ‘authorisation to send’ and ‘authorisation to receive’ fields, the column names are prefixed with ‘S.’ and ‘R.’ respectively.

Authorisations

Change View | Add | Revoke

Own BIC	Correspondent	Service	R. Status	R. Validity	R. Start date	R. End date	R. Restr.
ABNKBE5A	SWANBEBB	swift.fin	/Draft				
AENTBEEA	SWANBEBB	swift.fin	Enabled/	Expired	01/01/2008	01/01/2009	
ALLIUS33	ALLIUS33	swift.fin	/Pending approval				
SWAMBEBB	AAAABEBB	swift.fin	Enabled/	Valid	01/01/2009	31/01/2009	
SWAMBEBB	SWAMBEBB	swift.fin	Enabled/Draft	Valid			*
SWANBE2A	SWAMBEBB	swift.fin	/Pending approval				
SWANBEBB	AAAABEBB	swift.fin	Enabled/	Valid			*

In the authorisation details of a granular authorisation it is visible at a glance which message types are allowed or not without the need to scroll multiple select boxes. This is done by textually displaying the permission. Furthermore, the difference between a current and a new authorisation is indicated by a red asterisk in the new authorisation.



9.3.5 Miscellaneous Enhancements

The following additional usability enhancements are available on Workstation and Web Platform:

- The reason field of a rejected authorisation is now included in the detailed printout.
- The behaviour when disapproving an authorisation-to-receive with no current authorisation in 'Pending Approval' preparation status is identical to the behaviour already implemented for an authorisation-to-receive with a current authorisation, i.e. the system sets the status back to ‘draft disapproved’. Before, the status was set back to ‘draft’.
- When manually exporting authorisations it is now prohibited to use the same file name for the distribution file and the report file. Before, the distribution file was overwritten by the report file.

The following additional usability enhancements are available on Web Platform only:

- When creating an authorisation or query, it is possible to search for the correspondent BIC in the Correspondent Information File (CIF). You can search for BIC's existing in the CIF, using various search criteria: institution, city, country code or partial BIC's.
- It is possible to define multiple correspondent BIC's when creating new authorisations (on top of the existing facility to specify multiple Own BICs). An authorisation to receive will then be issued for each combination of own BIC and correspondent BIC.
- A clone function is added, making it possible to create an authorisation to receive from an existing authorisation to receive.
- A reciprocate function is added, making it possible to create an authorisation to receive from an existing authorisation to send.
  The new authorisation will have the same attributes as the existing one, including granularity if allowed. This function can only be performed when an operator is viewing the details of the authorisation, so not from the list view.
- It is possible to perform accept, revoke, delete, reject or (dis-)approve actions in one go on a list of authorisations by selecting all authorisations that need to be handled. This does not require a specific permission.

10 Other Functional Enhancements

10.1 Installation

Silent Installation Mode

Access/Entry 7.0 installation procedure supports the installation of new releases, upgrades and patches in silent mode (i.e. without user interaction).

To support a silent, unattended installation, Access/Entry 7.0 is able to read all parameters required for the installation from an external text file.

To facilitate the initial creation of this text file, Access/Entry 7.0 installation procedure can be instructed to generate this parameter file, with all the installation parameters entered while executing the installation from the graphical interface, in interactive mode. The file can be further edited if needed.

This feature makes it easier to test and automate the installation of Access/Entry 7.0

Secure Channel Support

Secure Channel provides a new feature, allowing an operator to save the Access licence options into a text file (excluding master and installation passwords).

The Access/Entry installation procedure is able to read this file, avoiding the operator to key in licence information during installation and upgrades. This feature can benefit the customers licensing a large number of BIC codes.

Upgrade on a new system

Access/Entry 7.0 now supports a new installation option, allowing to install Access/Entry from scratch on a new system but keeping (and upgrading) the existing configuration.

In order to support this feature, the upgrade of an Access/Entry system must be done in two steps:

- The first step, the 'Prepare Backup File for Upgrade' procedure, must be executed on the existing 6.x system. This step does not upgrade the system but only exports its configuration into an internal ZIP file.
- The second step, the 'Install from Prepared Backup File', is a new installation option, available for Access/Entry 7.0, which is selected when the installation of Access/Entry system is done on a new system and the prior 6.x configuration needs to be injected and upgraded into this new system.

  During the installation, the ZIP file prepared during the first upgrade step needs to be provided, in order to provide the existing 6.x configuration to upgrade into the new system.

Note This ZIP file only contains configuration data. The operational data like messages and events is not included in this file, to avoid the potential risk of creating duplicate transactions.

In summary, compared to previous 6.x releases, this new installation option greatly facilitates the installation from scratch of an Access/Entry system on a new host.

This installation option is available both for UNIX and Windows:

- On UNIX, its use is optional.
- On Windows, the use of this procedure is **mandatory**. This is because Access/Entry 6.x is not compatible with Windows Server 2008 R2, and Access/Entry 7.0 is not compatible with Windows Server 2003.

  This incompatibility between the operating system and Access/Entry imposes that Access/Entry 7.0 is installed from scratch, on a fresh Windows 2008 R2 system. This new

installation option allows preserving the existing 6.X configuration when upgrading to 7.0, on Windows.

10.2 Application Service Profile Support

Access/Entry 7.0 provides support for the Application Service Profile (ASP).

ASP Package File

The ASP package file, published on a weekly basis on swift.com, provides the following information:

- FIN Copy Profile

  This is the information that used to be published in separate FCP files, that is now included in the ASP package. The ASP package contains the definition of all the FCPs known at the moment of publication.

- Application Service Profile

  This is the description of all the attributes of the services available on SWIFTNet. The service information can be grouped into 2 main categories:

  – The general service description (Signature, Repudiation, T/Y Copy settings, etc)

  – The RMA settings associated to this service.

  The ASP contains the definition of all the services provisioned on SWIFTNet at the moment of publication.

Access/Entry 7.0 support the FCP and ASP information contained in the ASP package.

FIN Copy Profile Update

Access/Entry 7.0 allows an administrator to open an ASP package file, and to select from the package the specific FCP(s) that must be loaded in Access.

Both Workstation 7.0 and Web Platform 7.0 can be used to load the ASP package and select the FCP information from the ASP package.

Note Access/Entry 7.0 only works with the ASP package to load FCP information. The FCP files, used to load FIN Copy Profile information in Access/Entry 6.x, are not supported by Access/Entry 7.0.

ASP Update

Access/Entry 7.0 must be regularly updated with the information contained in the ASP package, in order to ensure that the service definitions known by Access/Entry 7.0 are up to date with their provisioning on SWIFTNet 7.0.

Compared to the FCPs, all the ASPs provided in the ASP package are loaded in Access/Entry, regardless whether these services are actually used by the customer. Access/Entry 7.0 provides a mechanism to hide to the end users the services that are not used.

As an ASP package contains hundreds of services, they are by default loaded as hidden services in Access/Entry 7.0. The only exceptions are the ASPs requiring RMA support, which are visible by default.

In order to update the ASP information contained in the ASP package, Access/Entry 7.0 supports two methods:

- A new 'Application Service Profile' application, available on Web Platform 7.0 only, provides a graphical interface to load the application service profiles present in the ASP package.

  This application also deciding which services loaded from the ASP package should be visible to other GUI applications (such as the RMA application).

- A new tool `saa_manageasp` that allows loading the ASP package from a command line. This tool is documented in Appendix B of Access/Entry *Installation and Administration* guide.

Note Workstation 7.0 does not provide support for management of ASPs. Customers that are not using the Web Platform 7.0 should therefore use the `saa_manageasp` tool to load in Access/Entry 7.0 the services contained in an ASP package file.

10.3 SWIFTNet 7.0 Alignments

10.3.1 Message Copy

SWIFTNet 7.0 introduces copy functionality for InterAct messages exchanged in Store-and-Forward mode. With this functionality, SWIFT automatically copies the full InterAct message to a copy destination. It can be used to either simply copy a message for information purpose (T-copy), or to make delivery dependent on approval of a third party that must authorise the message delivery (Y-copy).

The service administrator decides on the message flows that are copied, and which options are used related to copy service.

Only full Store-and-Forward InterAct message copy is supported, partial message copy is not supported.

Access/Entry 7.0 can be used at the emission and reception ends of the message copy flows. Access 7.0 only can be used as a Central Institution in Y-copy or T-copy mode.

10.3.2 Message and File Distribution

Access/Entry 7.0 supports the possibility introduced by SWIFTNet 7.0 to send (over Store-and-Forward) a message or file to a distribution list. In this case, the customer sends the message or file only once, together with a distribution list that contains the recipients that need to receive it. Because the sender provides the recipient list, the sender has full control over the list and can change it over time or even use a different one for every exchange.

10.3.3 RMA for InterAct and FileAct

Refer to Section 9.1 "RMA beyond FIN" for more details.

10.3.4 Enhanced Store-and-Forward Delivery Options

Access/Entry 7.0 supports the following SWIFTNet 7.0 enhancements for the store-and-forward delivery options.

Output Channels

Access/Entry supports output channels introduced in SWIFTNet 7.0.

This support impacts the definition of reception profiles using store-and-forward delivery in the SWIFTNet Interface Application.

Through the use of output channels on a shared queue, Access/Entry 7.0 allows to receive InterAct and FileAct traffic exchanged in store-and-forward mode through multiple sessions accessing the same store-and-forward queue.

Restrict Traffic Delivery

With SWIFTNet release 6.3, Access already allows to restrict the traffic to be delivered from a queue and also to control the delivery order of this restricted traffic.

With the introduction of output channels in SWIFTNet 7.0, Access/Entry 7.0 extends the allowed values available for the choice of the delivery subset and of the delivery order in the definition of reception profile in the SWIFTNet Interface application.

Delivery Notifications as System Messages

With SWIFTNet 7.0, the (failed) delivery notifications become available in the form of normal system messages. Before this release, they were only available as store-and-forward primitives to developers, and could not be processed in the same way as system messages.

Access/Entry 7.0 permits to specify whether (failed) delivery notifications should be received a system messages, and supports the reception of these (failed) delivery notifications as system messages.

10.3.5 Session History Report

SWIFTNet 7.0 offers the functionality to request and receive information on past and closed sessions used for store-and-forward traffic sent (only when input channels are used) or store-and-forward traffic received (sessions are always used).

This feature is offered through new system messages that Access/Entry 7.0 can use from an updated deployment package for SWIFTNet system messages.

10.3.6 InterAct and FileAct Bulk Retrieval

Access/Entry 7.0 supports, via a deployment package, two new system messages: the message to request a bulk retrieval of InterAct and FileAct traffic and the message response indicating the S&F FileAct transactions containing the retrieved bulk traffic.

Note Access/Entry 7.0 does not implement a dedicated logic to analyse the response message and automatically download the bulk S&F FileAct files. The process to receive these S&F files will be similar to any other FileAct reception.

10.3.7 SWIFTNet Store and Forward System Recovery

Access/Entry 7.0 is able to detect a system recovery of the SWIFTNet Store and Forward system and to identify, using logic based on the SnFInputTime field, the InterAct and FileAct messages that must be re-sent to SWIFTNet.

Access/Entry 7.0 adds a PDE trailer to the identified messages and moves them to a dedicated queue, where they will need to be manually approved by an operator to be sent to SWIFTNet.

The graphical services required for this operation are available on Workstation 7.0 and Web Platform 7.0.

10.4 Alliance RMA 7.0 migration

When upgrading to 7.0, the existing Alliance RMA 6.0 and 6.3 customers will be using the Alliance Access 7.0 software distribution to upgrade their current system (i.e. there is no Alliance RMA 7.0 DVD).

Alliance RMA customers will receive a new licence file, configuring this Access 7.0 system to be used for RMA purpose only.

The Access 7.0 installation/upgrade procedure has been enhanced to support a direct migration from Alliance RMA 6.0/6.3, making the migration of the database and its configuration data transparent.

Some packages that are core functions of Access (like Message Preparation or Application Interface) are now licensed in this Access configuration for RMA only. As these applications are not required for RMA management, they will not be selected into the existing user profiles, during the migration. By default, these applications will not be visible on the Workstation or Web Platform.

Note The commercial 'Standalone RMA' product offering remains available, with its related options (RMA+, Web Services for RMA, Database Recovery).

10.5 Alliance Entry 7.0

Alliance Entry 7.0 inherits a number of Access 7.0 core features:

- C-ISAM database replacement with Oracle (transparent replacement during the upgrade procedure).
- FileAct support, limited to the File Transfer adapter, using XMLv2 based integration. The 'Direct FileAct' adapter is not available on Entry.
- RMA beyond FIN and ASP support.
- FIN Cold Start support
- LDAP support
- Enhanced duplication check
- Silent installation mode
- Operate as a Windows service

Other Access 7.0 features (like Web Services, Database Recovery, Direct FileAct adapter, operational integration and configuration management command-line based tools) are not supported by Entry 7.0.

The Web Platform is also available for Entry 7.0, including all the graphical services required for Entry (administration & monitoring, message management, RMA management).

WorkStation 7.0 remains available for Entry 7.0, in maintenance mode.

10.6 Gateway Connection Management

Access/Entry 7.0 simplifies the configuration and management of the Gateway connection.

This section summarises the new features, and highlights their potential impact on operational procedures and security management.

Embedded RA

Access/Entry 7.0 does not require anymore installing the RA software, needed for communicating with the Gateway. The RA software is included in the Access/Entry 7.0 installation (hence the term 'Embedded RA').

This evolution simplifies operations as there is no need to install and maintain the RA software anymore. It is also not necessary anymore to configure the RA instance.

Relaxed Mode

In previous releases, each Gateway connection defined in Access/Entry required the definition of an authoriser DN, linked to a certificate used in strict mode in Gateway. Access/Entry needed to provide certificate management features and HSM monitoring function to support the management of these certificates[2].

With the mandatory use of the Gateway to handle the SWIFTNet connection, Access/Entry 7.0 can rely on the functionality provided by the Gateway to simplify operations.

Access/Entry 7.0 stops using certificates adopted in Strict mode, but instead uses certificates adopted in Relaxed mode.

This change brings an important operational simplification to the setup and management of the Gateway connection. In this mode, the certificates operations (adoption, renewal, password changes, HSM assignation, etc) are entirely handled by Gateway, and are removed from Access/Entry 7.0. This enhancement also eliminates many of the operational issues linked to the

[2] The use of certificates adopted in strict mode usage comes from the days when Access/Entry interfaced directly to SWIFTNet Link.

de-synchronisation of certificate information between Access/Entry and Gateway (for example, when a certificate password is changed in Gateway but not in Access/Entry).

This enhancement changes the ownership of certificate password, affecting how communication between Access/Entry and Gateway is secured. The certificate password has to be known by a Gateway operator, in order to be able to adopt the certificate in Relaxed mode. An Access/Entry operator will not need to know this password anymore, as the certificates are not managed by Access/Entry. The LAU settings and SSL are still available. With the use of certificates in Relaxed mode, these settings are now mandated in order to secure the connection between Access/Entry and Gateway.

Additional Backup Gateway connections

Prior to Access 7.0, each Access Logical Terminal, SWIFTNet Emission/Reception profile could be defined with a primary and a secondary Alliance Gateway connection.

With Access 7.0, these entities support additional Gateway connections (up to 4). It will allow connection failover to additional Gateway systems, possibly located in another site/region than the prime Access (to cope with SWIFTNet connectivity loss in one region).

10.7 LDAP Support

Access/Entry 7.0 offers the possibility to use an existing LDAP (Lightweight Directory Access Protocol) directory to perform central user management for Access/Entry users. This functionality allows the customer to implement a centralised security for all its business critical applications (e.g. one operation in LDAP will allow to prevent a user to access any of your critical business applications).

The LDAP integration only impacts the Access/Entry authentication method. The Security Officers configure an existing operator account to validate its credentials against an LDAP repository instead of using the local username/password.

No licence update is required to use this feature.

10.7.1 Configuration

The connection to the LDAP server has to be configured in Access/Entry. It can only be configured by operators who have the appropriate permissions (configure LDAP and approve LDAP). Optionally a backup LDAP server can also be defined. When a backup server is configured, Access/Entry will automatically switch to this server when the primary LDAP server becomes unavailable. After a restart of the Alliance Access/Entry servers, the primary LDAP server is contacted again. To configure the LDAP servers, please refer to the *Alliance Access/Entry System Management Guide*, section Configuring LDAP Authentication.

There are now 3 authentication methods possible for operators: local authentication, one-time password and LDAP authentication. The Security Officers can configure each user individually in Access/Entry. To configure an operator for LDAP authentication, please refer to the *Alliance Access/Entry System Management Guide*, section Defining Operators.

10.7.2 Authentication logic

When an LDAP-enabled operator logs in to Access/Entry (either via Workstation or Web Platform), the operator has to provide its Access/Entry user name and its LDAP password. When Access/Entry detects that the authentication method is LDAP, it forwards the credentials to the configured LDAP server. If the LDAP authentication succeeds, the operator is allowed access. It allowed permissions remain configured in Access/Entry based on assigned Security Profile(s).

The login event generated when an operator logs in to Access/Entry indicates which authentication method was used.

The name constraints for the local (Alliance Access/Entry) operator names have been extended. They now can contain up to 150 characters, including characters like “@”, “.”, “_”, “-“, “:”. This allows the operator names in Access/Entry to be identical to the LDAP U-ID.

10.8 Message Prioritisation

The internal message priority of live messages is now changeable. This priority is only applicable within Access, so not on the SWIFT network. It is considered for sorting of the messages in a routing point (queue), provided that the routing point is configured to take the priority into account. Exit points must be modified to work in 'priority mode' instead of 'FIFO mode' (the default).

The priority is instance based and has a value between 1 (highest priority) and 9 (lowest priority). By default system messages have internal priority 3, urgent messages priority 5 and normal messages priority 7.

The instance priority can only be changed for live messages. It can be done either manually by an operator (on Workstation or Web Platform) or by a new routing rule action that can change the instance priority.

Priority change is possible both for incoming and outgoing messages. Please note that for messages coming from MQ Host Adapter, the back office application can link the MQ message priority to the internal priority.

10.8.1 Manual change of instance priority

The priority of an instance can be changed when viewing the details of a message on Workstation or Web Platform:

- In the message view, the instance priority change can be applied to a single message instance. The current priority is displayed and you can choose the new priority from a list.
- In the instance view, the priority change can be applied on a single message instance or on a list of selected instances.

Please refer to the *Daily Operations Guide*, section Changing the Priority of a Message Instance for how to manually change the message priority.

The Event Journal will log the event 2158 when an operator manually changes the priority of a message. Furthermore, this is also logged in the message history.

A specific permission is needed for an operator to be allowed to change the message priority: Message file - change priority.

10.8.2 Automatic change of instance priority

The definition of the routing rules actions for source and new message instances now include a new field "InstancePriority". This field allows either to keep the existing instance priority value or to assign a new value.

Please refer to the *System Management Guide*, section Routing Rules for how to change message priority via routing rules.

When the priority has changed due to a routing rule, this is logged in the message history

10.9 Supportability Enhancement

Access/Entry 7.0 provides system and integrity checks available in Access/Entry Configuration GUI package on Web Platform to rapidly assess the Alliance Access/Entry environment:

- The system check quickly determines if the operating system configuration is compliant with the SWIFT configuration requirements for Access/Entry. 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 coordinate with your system administrator and take the actions required to make the alignments during scheduled maintenance.
- The software integrity check verifies the integrity of the files for the installed Access/Entry software. The result of the check indicates whether any software files were added, removed, or updated.

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

10.10 FIN Cold Start Support

Access/Entry can be configured to automatically process the undelivered message report (MT082) received after a FIN cold start. It will analyse the content of these messages to re-queue the required messages for transmission.

10.10.1 Configuration

The FIN cold start information must be configured in Access/Entry. This configuration is subject to the four-eyes principle.

The configuration allows specifying FINCopy services for which messages should not be resent.

The date and time of the generation of the most recent undelivered message report before the service interruption must not be provided as it is included in the specific undelivered message report (MT082) received after a FIN cold start. This date and time is published on swift.com.

For information on how to configure and approve the FIN cold start information, please refer to the *Daily Operations Guide*, section FIN Cold Start.

10.10.2 FIN cold start procedure

When the configuration is approved, Access/Entry verifies whether the undelivered message report (MT082) received for each LT refers to a FIN cold start.

If this is the case, Access/Entry will identify the messages that should be re-queued for retransmission to SWIFT:

- The messages in the MT082 that were not delivered to the correspondent
- The messages that were sent to SWIFT after the date/time of the MT082

These messages are re-activated with a PDE indication in a dedicated queue _MP_recovery. An operator, with appropriate entitlements (Message Approval - Treat Recovered Message) can then authorise the emission of these messages to SWIFT. This operation is available on Workstation and Web Platform.

When the FIN cold start procedure is finished, an operator with the correct permission (SWIFT Support - Report FCS) can generate a report giving a summary of the messages that were successfully processed during the FIN cold start. The report also gives more detailed information for the messages that could not be resent. The report is stored on the server.

10.11 Obsolete functions

Some features have been phased out of Access/Entry 7.0. The list below details the features removed and the reasons for their removal/suppression:

- USE/BKE

  USE/BKE has been replaced by Hardware Security Modules (HSM) and Relationship Management Application (RMA) infrastructure and is no longer used.
- SWIFTNet Phase2 Migration

  The migration is completed for all customers.
- RA and Certificate Management

  The Remote API is now embedded in Alliance Access/Entry. The connection with Alliance Gateway is now relaxed, which means all certificates handling is done on Alliance Gateway.
- CAS LU 6.2, Telex/Testkey/Fax, X.25, Dial-up, Devices, ST200-ATE

  Modernisation of Alliance Access connection methods.

Note The upgrade procedure will remove any asynchronous line or terminal type device that is still defined in the database.

- Mirrored-disks Support

  Use of Oracle technology for database.

- Local 103 Addition

  To allow the installation of multiple FINCopy profiles with the same CID.
  As of release 7.0, the FIN-Copy field in the Header tab for a manually created message or the tag 103 for batch input must be defined explicitly.

- alliance_root Script

  Security enhancement

Note Some functions should be run with the root account.

- System date/time Check at startup

  Upon server start, Alliance Access/Entry no longer checks the system date/time versus the database time.

Legal Notices