Alliance 7.2

Migration Guide

Preliminary version

This document outlines the approach for migrating to Release 7.2 of the SWIFTNet Link and Alliance products. It provides detailed information about how to prepare for and complete the migration. The products that are impacted are SWIFTNet Link, Alliance Web Platform Server-Embedded, Alliance Gateway, Alliance Access, Alliance Entry, and Alliance Messaging Hub.

The final version of this document will be available by the end of August 2017, together with the Release Letters and Installation Guides for all platforms.

14 July 2017

Table of Contents

Preface

About this document

This document outlines the approach for migrating to Release 7.2 of the SWIFTNet Link and Alliance products. It provides detailed information about how to prepare for and complete the migration. The products that are impacted are SWIFTNet Link, Alliance Web Platform Server-Embedded, Alliance Gateway, Alliance Access, Alliance Entry, and Alliance Messaging Hub.

Disclaimer

This document is provided for information purposes only, and shall not be binding, nor shall it be construed as constituting any obligation, representation, or warranty on the part of SWIFT. The information in this document is the latest available at the date of its publication, and further changes can occur.

Intended audience

This document is for technical implementers and operational users of SWIFTNet Link and the Alliance products to help evaluate the impact of changes for Release 7.2 that will occur during the period 2017-2018.

Implementers and users can use this document to plan resources and prepare budget allocations.

1 Significant Changes since Previous Version

The following tables list the significant changes to the content of the Alliance 7.2 Migration Guide since the 09 June 2017.

This section does not include editorial or formatting changes that SWIFT makes to improve the usability and comprehension of the document.

New information

- A new section Advance Information for Release 7.2 has been added on page 5.
- A section about the Impact of using FileAct with Release 7.2 has been added on page 12.
- Information about HSM cards and Remote File Handler has been added to the section Preparation on page 22, which explains how to Migrate to SWIFTNet Link 7.2.

Updated information

- The section Preparation for migration on page 7 has been updated.
- The section Key Release Dates on page 8 has been updated.
- Section Operating System Requirements for Release 7.2 on page 10 now includes a link to a tip about the use of operating systems other than those qualified by SWIFT.
- The information in Changing to a Different Operating System on page 11 has been clarified.
- The section Convert Backups of Message and Event Log Archives on pages 31 and 34 includes more information about the conversion tool.

Information that was moved within the document

Information about Using FileAct with SWIFTNet 7.2 has moved to a new section 3 on page 12

2 Advance Information for Release 7.2

Advance information is provided for the following products:

- Alliance Access
- Alliance Entry
- Alliance Gateway (Including Remote API)
- Alliance Messaging Hub
- Alliance Web Platform Server-Embedded
- SWIFTNet Link
- SWIFT Web Access

The following documents have also been updated:

- SWIFTNet and Alliance Release Policy
- OS Levels and Patches Baseline
- Information for Hardening Supported Operating Systems

At any time, you can view a list of the recently updated documents on the **What's new** tab of the User Handbook Online.

3 Migration to Release 7.2

Functional overview

SWIFTNet 7.2 and Alliance 7.2 are mandatory technology releases for the Alliance product family. This release will continue to provide a highly secure and efficient SWIFT service for our customers in the years ahead.

This release combines a new operating system baseline with upgrades to the third-party products used within the SWIFT platform, inside Alliance products, and SWIFTNet Link. It will retain all the functionalities of the previous product releases and introduce FileAct enhancements.

Additionally, this change will offer some significant performance benefits to customers because it introduces 64-bit architecture while using the existing hardware.

For more information, see SWIFTNet 7.2 - Final Release Overview and Alliance 7.2 - Final Release Overview.

SWIFTNet CA Root Key

If you do not migrate to Release 7.2 by November 2018, then the root key renewal will cause any software release prior to SWIFTNet Link 7.2 to fail.

Approach

For all products and all operating systems supported, the migration approach will be to set up new environment separate from the existing infrastructure.

Using a new environment reduces the risk of business being interrupted during the migration period.

To migrate the products to release 7.2, you can either perform a fresh installation of release 7.2 software, or install release 7.2 using a prepared backup file to migrate the data from the current release.

The configuration data is migrated when you use the “Install from prepared backup file” option when installing the software.

The installation guides for the products will provide the required procedures to prepare and install from the backup file, and complete the installation.

People involved

People with the following roles will be involved during the migration:

- operating system Administrator
- SWIFT applications’ administrator
- Left and Right security officers (LSO, RSO) for Alliance Access
- Left and Right security officers (LSO, RSO) for Alliance Entry
- SWIFTNet security officers
- user with swift.com credentials to access to SWIFT Download Centre
- Alliance Gateway administrator
- Alliance Web Platform administrator

3.1 Migration Sequence

You must migrate SWIFTNet Link and the Alliance products to Release 7.2 by November 2018 in this order:

1. Alliance Web Platform Server-Embedded
2. Hardware Security Module (HSM) Cards and Tokens (if not using HSM box)
3. SWIFTNet Link
4. Alliance Gateway
5. Alliance Access, Alliance Entry, or Alliance Messaging Hub

Migration steps

The migration steps include the following:

1. Plan and prepare for the migration.
2. Prepare the secured new environment, with either:
   - new physical machine with qualified operating system installed, or
   - new virtual environment with qualified operating system installed
3. Prepare each application on the current environment.
4. Prepare a backup of each application on the current environment.
5. On the new environment, install each application or migrate it from its prepared backup in the recommended sequence.

Note *It will not be possible to upgrade your current system locally to the new release. You must perform either a fresh installation, or an installation from the prepared backup file.*

3.2 Preparation for migration

SWIFT recommends the following approach to prepare for and migrate to Release 7.2 by November 2018:

1. Read the information in this *Migration Guide* to assess the impact on the SWIFT environment on your premises.
2. Read the prerequisites for the migration of each product, and the preparation that is required for migrating the products to release 7.2.
   This document provides a summary of the prerequisites and an overview of the preparation and installation. However, the most up-to-date and detailed information is now available in the release letters and installation guides for the products. See Advance Information for Release 7.2 on page 5.
   An eLearning module Release 7.2: Plan Your Project is also available on SWIFTSmart.
3. Define when and how you prefer to implement the migration and create a plan for the migration.
4. Set up the secured new environment for Release 7.2. See Alliance - Security Guidance.
5. After general availability (31 August 2017), you can migrate the software. Note the important information about Impact of using FileAct with Release 7.2 on page 12.
6. See also the Knowledge Base tip, Alliance and SWIFTNet Release 7.2 - Mandatory Technical Upgrade Release - Frequently Asked Questions (FAQ) (5021016).

If you have questions about the prerequisites or the migration, you can consult the Knowledge Base or the Documentation (User Handbook Online).

3.3 Key Release Dates

These are a summary of the key dates.

Month	Item
March 2017	For software developers, availability of: • SWIFTNet 7.2 in Integration Testbed (ITB) • SWIFTNet Link 7.2 for software developers • Alliance Gateway 7.2 Developers Toolkit (DTK) software
August 2017	Availability of: • Alliance 7.2 product family (including SWIFTNet Link) for general distribution towards customers • Alliance Messaging Hub 3.6 • SWIFTNet 7.2 in the Production environment for live operations **Important!**: FileAct customers MUST NOT install SWIFTNet 7.2 or Alliance 7.2 in their production environment before end of November 2017 on systems used for FileAct flows pending confirmation from SWIFT.
September 2017	Availability of: • SWIFT Integration Layer 1.3
October 2017	Availability of: • Alliance Remote Gateway in the Production environment for Test and Training (T&T) operations
November 2017	Availability of • Alliance Remote Gateway in the Production environment for live operations
January 2018	Availability of: • Transaction Delivery Agent 7.2 for general distribution
November 2018	End of support for versions of Alliance and SWIFTNet prior to 7.2 Renewal of the SWIFTNet CA Root Key for all SWIFTNet certificates.

See the Release timeline for the latest information about release dates.

3.4 Hardware Requirements for Release 7.2

Technically, Alliance 7.2 does not require new hardware if the hardware is 64-bit and if a 64-bit operating system is used on the current system.

However, even if you already use a 64-bit hardware and 64-bit operating system, SWIFT recommends that you create a new environment for 7.2 because you can only migrate the products either by performing a fresh installation, or by installing from a prepared backup file.

Therefore, for all software products and all operating systems supported, the migration approach outlined in this document for release 7.2 is to use a new environment, with hardware or a new virtual OS environment that is separate from the existing infrastructure.

SWIFT recommends hardening your Operating System. The Information for Hardening Supported Operating Systems provides information about running systems in a hardened environment.

For information about system sizing (number of CPUs, memory, etc), see the Hardware reference for Release 7.2 on swift.com.

Considerations for hardware:

- The hardware must support the new operating system baseline and patch level.

  If you plan to use the hardware in your current environment for your new environment, then verify with your hardware vendor that the new operating system can be installed on the existing hardware.

  It is possible that some of your hardware components do not have appropriate drivers in the new versions of the Operating System. For older systems, the CPU model used might not be supported in the new OS version. Verify this with your hardware vendor.

- Hardware must perform well for the next five years.

  If your current hardware dates from the migration to release 7.0 in 2011, then the systems have aged to a point where it is unlikely that they will continue to function well for the next five years, and replacement would be strongly advised.

  On the other hand, if you recently changed hardware (for example, you have a policy to replace servers every five years), then these systems could be re-used without problem.

- Resource capacity must be able to meet consumption.

  Most systems are sized for emergency peak loads. This typically means that under normal circumstances the CPU load is less than 10%, the memory load is less than 20%, and there are no I/O queues to the disk subsystem. In these cases, replacement would not be driven by capacity need.

  However, for systems that consistently use more than 50% of any CPU-core or have significant queue build-up on the disk I/O, replacement should be considered to be able to handle future needs of the software, as well as business growth.

Related information

Are SWIFT products qualified on virtual machines? (Knowledge base tip 846849)

3.4.1 Disk Space Requirements

Release 7.2 of Alliance Web Platform Server-Embedded, Alliance Gateway, Alliance Access, and Alliance Entry will require more disk space than was needed for release 7.0.

Up to 20 GB is required depending on the OS platform that is used, and additional adequate space must be provided for operational data (messages, events etc,).

For more information, see the *Release Letters* and *Installation Guides* for the products. See Advance Information for Release 7.2 on page 5.

3.5 Operating System Requirements for Release 7.2

You cannot use current infrastructure

Release 7.2 of SWIFTNet Link and the Alliance products must be installed on a new environment and comply with the OS baseline.

Operating systems

The following operating systems will be used to qualify SWIFTNet Link 7.2, Alliance 7.2 products, and Alliance Messaging Hub 3.6:

- Windows Server 2016 Standard Edition
- AIX 7.2 with Technology Level (TL) 01 and Service Pack (SP) 1
- Oracle Solaris 11.3.7.5.0 for Oracle SPARC Enterprise Servers
- Red Hat Enterprise Linux operating system:
  - Red Hat Enterprise Linux 6.7, 64-bit, supported until 2020
  - Red Hat Enterprise Linux 7.2, 64-bit

There is no direct upgrade path for the following:

- from Windows 2008 to Windows 2016
- from Solaris 10 to Solaris 11
- from RHEL 6.4 to RHEL 7.x

For information about the support for operating systems higher than what is qualified with Release 7.2, see the knowledge base tip Can you install SWIFT products on Operating System or third-party software versions that are different from those on which they have been qualified? (1212959).

In addition, for Alliance Message Hub:

- Application Server:
  - IBM MQ 8.5.5.9 for AIX
  - JBoss EAP 6.4 for Red Hat Enterprise Linux
  - Weblogic 12.2.1 for Oracle Solaris
- Java Run-time (JDK): Java 8 for both AIX and Oracle Solaris

See also Qualification Details in the *Connectivity to SWIFT - OS Baselines and Patch Baseline.*

Web browsers

The Alliance Web Platform Server-Embedded GUI applications will be qualified with several web browsers. See section Alliance Web Platform Server-Embedded 7.2 prerequisites on page 14.

3.5.1 Changing to a Different Operating System

You can set up the new environment to use a different support operating system from the OS on your current system.

If you change the OS to Linux, you can use the “Install from prepared backup” option, which also migrates the configuration data from the current system.

If you change the OS to AIX, Oracle Solaris, or Windows, then the “Install from prepared backup” option is not possible. In this case, you must perform a fresh installation.

Migration to Linux

If you change the platform to Linux from AIX, Oracle Solaris, or Windows, the following is an overview of the steps involved:

1. For SWIFNet Link: Before installing or migrating to SWIFTNet Link 7.2, you must register the change of operating system using the form, SWIFTNet Link operating system change.
2. Create a prepared backup on AIX, Oracle Solaris, or Windows, as applicable
3. Install release 7.2 on Linux with the option, “Install 7.2 from prepared backup”.
4. For Alliance products excluding SWIFTNet Link, SWIFT recommends that you obtain a new license sheet and perform the relicensing after the migration.

Migration to AIX, Oracle Solaris, or Windows

If you can change the platform to AIX, Oracle Solaris, or Windows, from any other supported OS from release 7.0.x, then the following is an overview of the steps involved:

1. For SWIFTNet Link: Before installing SWIFTNet Link 7.2, you must register the change of operating system using the form, SWIFTNet Link operating system change.
2. Perform a fresh installation of Release 7.2 on the new environment. You **cannot** use the option, “Install 7.2 from prepared backup”.
3. Complete the configuration of Release 7.2 on the new environment.
4. Convert the message, event, and archive backups and restore them on the new system.

3.6 Help with the Migration

If you need more help with the migration to Release 7.2, you can contact the SWIFT Consultancy Service or discuss with your SWIFT Account Manager. You can also contact your hardware and software vendors about the new releases of their products.

Other resources, such as, SWIFTSmart eLearning, Alliance Managed Operations, the User Handbook Online (documentation), and the Knowledge Base on mySWIFT are available for you.

For information about how to contact SWIFT Support, see https://www.swift.com/contact-us/support.

4 Using FileAct with SWIFTNet 7.2

Both the sender and the receiver of FileAct messages must use at least:

1. SWIFTNet Link 7.0.50
2. Alliance Gateway 7.0.50 or higher
3. Alliance Access 7.1.30 or higher, or Alliance Entry 7.0.30 or higher

4.1 Impact of using FileAct with Release 7.2

An important impact of this release relates to the exchange of files using the FileAct service.

FileAct customers migrating to Release 7.2 cannot exchange files with counterparties that are not running the minimum supported version of Remote File Handler 7.0.50 or higher. This will only impact the FileAct traffic flow in real-time mode. There is no impact on FileAct in store-and-forward mode.

Important FileAct customers MUST NOT install SWIFTNet 7.2 or Alliance 7.2 in their production environment before end of November 2017 on systems used for FileAct flows pending confirmation from SWIFT.

Migration date for production

SWIFT will inform you about the readiness and migration date for using FileAct in production, and will confirm when you are authorised to install SWIFTNet 7.2 and Alliance 7.2 in your production environment.

If customers migrate to Release 7.2 in their production environment before this confirmation is received, they will need to roll back to the version of SWIFTNet and Alliance prior to Release 7.2 to resume their FileAct flows.

Testing FileAct with counterparties

SWIFT recommends that customers complete FileAct testing with Release 7.2 with their counterparties prior to November 2017. For testing, do not use systems that are used in your production environment.

If you are not sure whether your counterparty is running on SWIFTNet Link and Remote File Handler 7.0.50 at a minimum, then only complete the testing using FileAct in loopback mode or store-and-forward mode.

Note *To benefit fully from the FileAct Enhancements your counterparty(s) must also be on Release 7.2.*
Customers that start a new FileAct service after Release 7.2 must confirm that their counterparty(s) are running on the minimum Remote File Handler 7.0.50 baseline version in order to limit any possible compatibility issues.

Frequently asked questions

See the knowledge base tip FileAct Enhancements with Release 7.2 - Frequently Asked Questions (5021829), which outlines details about compatibility of the software versions for FileAct transfers.

4.2 Prerequisites

- Alliance Access 7.1.30 or Alliance Entry 7.1.30, or higher is required to connect to Alliance Gateway 7.2
- If third-party applications are used:
  - Remote API 7.0.50 or higher
  - Remote File Handler 7.0.50 or higher
- SWIFTNet 7.2 will support file sizes up to 2 GB for both real-time and store-and-forward. Check with your Messaging interface provider to confirm their support for the larger file size or check the conformance statement of your interface on swift.com.

4.3 FileAct Enhancements in SWIFTNet 7.2

Consider whether the following enhancements to FileAct in SWIFTNet 7.2 will impact the way that FileAct is implemented in your institution.

Elimination of Unknown status

Currently, a file transfer can result in an “Unknown” state; this implies manual intervention by the customer. Release 7.2 will no longer show “Unknown” and will provide the correct end state.

For real-time file transfers, this requires that both the sender and the receiver use SWIFTNet Link 7.2 and Remote File Handler 7.2.

Use of logical file name for reconciliation purposes

SWIFT has requested messaging interface vendors to include the logical file name in the delivery notification. This enables customers to reconcile their delivery notification with their file transfer based on the file name.

When the messaging interface provides the logical file name in the acknowledgement for store-and-forward traffic, then SWIFT can include the logical file name in the queue status report.

Customers can use a new system message xsys.008.001.02 report version 3 to request this report. The return system message xsys.009.001.03 report version 3 will include the logical file name.

Enhanced transfer efficiency

With the current FileAct implementation, when sending a single large file, FileAct does not fully use the available bandwidth. With Release 7.2, FileAct will be able to use all available bandwidth.

Dynamic control of concurrent file transfers

Customers can perform multiple file transfers simultaneously. FileAct automatically manages the file transfers based on the available bandwidth.

With Release 7.2, FileAct will dynamically and automatically manage file transfer based on the number of active file transfers. The concurrent file transfer limit has been removed in Release 7.2.

Customers may notice a difference in the file transfer monitoring. When sending a number of files, all file transfers will perform negotiation immediately and go into "Accepted" state.

Only a subset will move to "Ongoing" state based on available sender and correspondent resources. Other file transfers will start progressively based on available sender and correspondent resources.

File transfers resume automatically

If a file transfer is interrupted, the file transfer will resume automatically provided that the following conditions are met:

- The same systems are handling the file transfer after the interruption.
- The interruption does not last too long. (The default is 30 minutes.)
- Both systems are still up and running.

If these conditions are not met, then the file transfer fails.

5 Migration Prerequisites for Release 7.2

The detailed prerequisites are outlined for each product in their respective sections.

Minimum required releases

The following is a summary of the minimum releases from which you can migrate to Release 7.2:

- Alliance Web Platform Server-Embedded 7.0.70, and GUI packages
- SWIFTNet Link 7.0.50
- Alliance Gateway 7.0.50
- Alliance Access 7.1.23
- Alliance Entry 7.1.23

5.1 Alliance Web Platform Server-Embedded 7.2 prerequisites

- Minimum required release: Alliance Web Platform Server-Embedded 7.0.70 or higher
- Hosted Database is used: Oracle version 12.1 or higher
- With release 7.2, all TCP/IP connections will use Transport Layer Security (TLS) version 1.2 and the supported cryptographic algorithms will be restricted to:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Web browser requirements

Browsers must be running on Windows operating system and must be configured with TLS 1.2.

- Windows 7 (32-bit or 64-bit):
  - Internet Explorer 11 (either 32-bit or 64-bit where needed)
  - Firefox ESR 52.0 (either 32-bit or 64-bit where needed)
- Windows 10 (64-bit only):
  - Internet Explorer 11 (either 32-bit or 64-bit where needed)
  - Firefox ESR 52.0 (either 32-bit or 64-bit where needed)
  - Microsoft Edge (only in 64-bit)
  - Chrome 57 (only in 64-bit)

For more information, see the section about *Web Browser Settings* in the Alliance Web Platform 7.2 Installation Guide for the relevant platform.

Product release dependencies

Alliance Web Platform Server-Embedded 7.2 *is compatible* with:

- SWIFTNet Link 7.2
- Alliance Gateway 7.2
- Alliance Access 7.2
- Alliance Entry 7.2
- Packages:

  Access/Entry Configuration 7.2
  Access/Entry Monitoring 7.2
  Alliance Gateway Administration 7.2
  Alliance Message Management 7.2
  Alliance Relationship Management 7.2
  Alliance Web Platform Administration 7.2
  SWIFT WebAccess GUI

Alliance Web Platform Server-Embedded 7.2 *cannot* connect to:

- Alliance Gateway 7.0.x
- Alliance Access 7.1.x
- Alliance Entry 7.1.x
- Packages with a release prior to 7.2

5.2 Hardware Security Module Prerequisites

HSM box

SWIFTNet Link 7.2 is compatible with both software versions 6.0 and 6.1 of the HSM box. You can upgrade the HSM box software to version 6.1 either before or after migrating to SWIFTNet Link 7.2. For more information, see also HSM Box Software Upgrade Guide.

HSM Tokens and Cards

The HSM card and token models supported with SWIFTNet Link 7.0.x releases are not compatible with SWIFTNet Link 7.2, except for the HSM token model iKey 4000.

The HSM token model iKey 4000 is compatible with SWIFTNet Link 7.2 and supported during the migration to the new HSM token model eToken 5110, which needs to be completed by end November 2018.

Please also refer to the Knowledge base tip, HSM Token Refresh Entitlement & Frequently Asked Questions (5021623).

5.3 SWIFTNet Link 7.2 prerequisites

- Minimum required release: SWIFTNet Link 7.0.50 or higher
- If third-party applications are used: Remote File Handler 7.0.50 or higher
- If you plan to use an operating system that is different from your current system, then see the section, Changing to a Different Operating System on page 11.
- If you are using HSM cards or HSM tokens, make sure you have the new HSM Tokens.

MI Channel

If using SWIFTNet Link without Alliance Gateway for MI Channel:

- IBM MQ: Version 8.0.0.6 client installed on the new environment where Alliance Gateway 7.2 will be running

Product release dependencies

- SWIFTNet Link 7.2 is compatible with:
  - HSM box software versions 6.0 and 6.1
  - Remote File Handler 7.0.50
  - Alliance Gateway 7.2
- You can upgrade the HSM box software to version 6.1 either before or after migrating to SWIFTNet Link 7.2.
- SWIFTNet Link 7.0.50 or higher and SWIFTNet Link 7.2 can connect to the same HSM cluster.
- SWIFTNet Link 7.0.50 is *not compatible* Remote File Handler 7.2.
- SWIFTNet Link 7.2 is *not compatible* with Alliance Gateway 7.0.50.

5.4 Alliance Gateway 7.2 prerequisites

- Minimum required release: Alliance Gateway 7.0.50 or higher
- If you are using FileAct: then Alliance Access 7.1.30 or Alliance Entry 7.1.30, or higher is required to connect to Alliance Gateway 7.2
- If third-party applications are used:
  - Remote API 7.0.50 or higher
  - Remote File Handler 7.0.50 or higher
- IBM MQ: Version 8.0.0.6 of the client must be installed on the new environment where Alliance Gateway 7.2 will be running.
- With release 7.2, all TCP/IP connections will use Transport Layer Security (TLS) version 1.2 and the supported cryptographic algorithms will be restricted to:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Licensing

- SIPN BAND will be enforced to SIPN BAND -2. You must retrieve an updated license using Secure Channel before you install or migrate to release 7.2.

  Your current environment must be relicensed with a licence sheet that was created after 01 January 2016.
- Alliance Gateway 7.2 will no longer support the SOAP or WSHA licensing options. WSHA related data, and message partners that are configured with WHSA-only are not migrated.

  As of July 2017, all Alliance Gateway WSHA and or SOAP licenses have been updated when the WSHA and SOAP proxy is removed. You can retrieve the updated license via Secure Channel.
- If you remove the following licenses from release 7.2 and they were present in the release on which the backup was made, then there will be a warning about these packages is displayed and logged after the installation: 13:MQ HOST ADAPTER, 14:RA HOST ADAPTER, 57:COPY TO, 60:FTI, 61:FTA

Transaction Delivery Agent (TDA)

- Transaction Delivery Agent 7.2 will be released on 12 January 2018. Transaction Delivery Agent 7.2 will be available as a native 64-bit application and it will only support IBM MQ 8.0.0.6 Client.
- Support for Transaction Delivery Agent 4.0.1, 4.0.2, and 4.0.10 will end in November 2018, at which point you must install Transaction Delivery Agent 7.2.
- Transaction Delivery Agent 7.2 will require a fresh install on the new operating system baseline and the use of Remote API 7.2.

Product release dependencies

Alliance Gateway 7.2 is compatible with:

- Alliance Access 7.1.23, or higher
- Alliance Entry 7.1.23, or higher
- Alliance Messaging Hub 3.3.x, 3.4.x, 3.5.x, and 3.6
- Remote API 7.0.50, or higher
- Remote File Handler 7.0.50 or higher
- SWIFTNet Link 7.2

5.5 Alliance Access 7.2 prerequisites

- Minimum required release: Alliance Access 7.1.23 or higher
- Hosted Database is used: Oracle version 12.1 or higher
- IBM MQ: IBM MQ 8.0.0.6 client on the new environment where Alliance Access 7.2 will be running.

  Note *Alliance Access 7.2 will not support IBM MQ server mode.*

- Alliance Access SOAP Host Adapter: Make sure that the back office application using this connection can use SOAP Host Adapter and the latest crypto algorithm of TLSv1.2.

  Note *With release 7.2, all TCP/IP connections will use Transport Layer Security (TLS) version 1.2 and the supported cryptographic algorithms will be restricted to:*
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- Alliance Access with a third party ADK component: the component must be compatible with Alliance Access 7.2. If you have ADK components that are no longer used, you must remove them from Alliance Access 7.1.23, or higher, before migration to Alliance Access 7.2.

  Note *ADK components that were compatible with Alliance Access 7.1 are not compatible with Alliance Access 7.2. Please contact your vendor.*

- Alliance Access with a custom Integration Layer (IPLA) component: the IPLA component must be compatible with Alliance Access 7.2

  The following IPLA components are compatible with Alliance Access 7.2:

  - Connector for T2S version 1.2.10
  - Connector for Sanctions version 1.2.40
  - Connector for SWIFT gpi (all versions)

- Alliance Workstation is decommissioned:

  Make sure that operators and end-users of Alliance Access are trained to use the Alliance Web Platform GUI applications that replace Alliance Workstation.

- CASmf is decommissioned:

  - Remove all Message Partners that use CAS in Alliance Access 7.1.23, or higher.
  - Check that Alliance Access licensing does not have the option 18:CAS TCP/IP selected. You can retrieve the latest license sheet using Secure Channel.

CREST Over SWIFTNet:

- Tuxedo 12cR2 with patch RP089 or higher. The patch will be available for download from the Oracle website.
- Tuxedo will mandate that encryption keys have a minimum length of 128 bit. If it does not work because the client is using an old version of CRPI or NSL, you must manually change the key length back to 0. For more information, see *Encrypting Messages* in the *CREST over SWIFTNet - Customer Application Integration Guide* when it is available for Release 7.2.
- CRnet File Interface (CRFI) and CRnet Programming Interface (CRPI): configure Local authentication (LAU) between the back-office application and Alliance Access.
- CRnet Programming Interface (CRPI) clients: use the latest version of the CRPI client. CRPI client will remain in 32-bit mode, and will be supported on AIX, Linux, Windows, and Oracle Solaris.

  The current version of CRPI and NSL and the new CRPI 7.2 and NSL 7.2 can connect to Alliance Access 7.2.

  After the Alliance Access 7.2 migration, SWIFT recommends that you upgrade NSL and CRPI to the 7.2 versions.

Product release dependencies

- Alliance Access 7.1.23 or higher can connect to Alliance Gateway 7.2
- If FileAct is used, then Alliance Access 7.1.30 or higher is required to connect to Alliance Gateway 7.2
- Alliance Access 7.2 *cannot* connect to Alliance Gateway 7.0.x with SWIFTNet Link 7.0.x

5.6 Alliance Entry 7.2 prerequisites

- Minimum required release: Alliance Entry 7.1.23 or higher
- Alliance Workstation is decommissioned: make sure operators and end-users of Alliance Entry are trained to use the Alliance Web Platform applications that replace Alliance Workstation.

Product release dependencies

- Alliance Entry 7.1.23 or higher can connect to Alliance Gateway 7.2
- Alliance Entry 7.2 *cannot* connect to Alliance Gateway 7.0.x with SWIFTNet Link 7.0.x

5.7 Prerequisites for Alliance Messaging Hub

- Alliance Messaging Hub 3.3.x, 3.4.x, 3.5.x, and 3.6 are compatible with Alliance Gateway 7.2 and SWIFTNet Link 7.2. If you are already using AMH 3.3 or higher, then upgrading Alliance Messaging Hub is optional.
- To use Alliance Gateway 7.2 and SWIFTNet Link 7.2 with AMH 3.3.x, AMH 3.4.x, or AMH 3.5.x, you must perform additional actions on AMH. For more information, see AMH 3.3.x, 3.4.x, and 3.5.x on page 35.

Product release dependencies

- Alliance Messaging Hub 3.6 *cannot* connect to Alliance Gateway 7.0.x or SWIFTNet Link 7.0.x.

6 Migrate to Alliance Web Platform Server-Embedded 7.2

6.1 Prerequisites

- Upgrade Alliance Web Platform Server-Embedded to 7.0.70 or higher.
- If a hosted Database is used, then install Oracle version 12.1 or higher.
- With release 7.2, all TCP/IP connections will use Transport Layer Security (TLS) version 1.2 and the supported cryptographic algorithms will be restricted to:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Web browser requirements

Browsers must be running on Windows operating system and must be configured with TLS 1.2.

- Windows 7 (32-bit or 64-bit):
  - Internet Explorer 11 (either 32-bit or 64-bit where needed)
  - Firefox ESR 52.0 (either 32-bit or 64-bit where needed)
- Windows 10 (64-bit only):
  - Internet Explorer 11 (either 32-bit or 64-bit where needed)
  - Firefox ESR 52.0 (either 32-bit or 64-bit where needed)
  - Microsoft Edge (only in 64-bit)
  - Chrome 57 (only in 64-bit)

  For more information, see the section about *Web Browser Settings* in the Alliance Web Platform 7.2 Installation Guide for the relevant platform.

Product release dependencies

Alliance Web Platform Server-Embedded 7.2 *is compatible* with:

- SWIFTNet Link 7.2
- Alliance Gateway 7.2
- Alliance Access 7.2
- Alliance Entry 7.2
- Packages:

  Access/Entry Configuration 7.2
  Access/Entry Monitoring 7.2
  Alliance Gateway Administration 7.2
  Alliance Message Management 7.2
  Alliance Relationship Management 7.2
  Alliance Web Platform Administration 7.2
  SWIFT WebAccess GUI

Alliance Web Platform Server-Embedded 7.2 *cannot* connect to:

- Alliance Gateway 7.0.x
- Alliance Access 7.1.x
- Alliance Entry 7.1.x

6.2 Preparation

For specific instructions to complete the following, see the Alliance Web Platform Server-Embedded 7.2 Release Letter and Installation Guides.

Software owner

Create a user on the operating system who will be the owner of the software.

- **Windows**:

  As from release 7.2, you must have one user account on Windows that is not part of the Administrator group. This account will be the software owner and will manage the Alliance Web Platform Server-Embedded application. However, installation and un-installation must be done by an Administrator.

- **UNIX or Linux:**

  The installation can be performed by root and non-root. The non-root account will be the software owner and must have the required settings (the `ulimit` parameters and the IPC resources).

Embedded database on AIX

When using the embedded database on AIX, the I/O completion ports (iocp0) default setting must be changed from “Defined” to “Available”.

Hosted database

When using hosted database, create a new Oracle instance with AL32UTF8 character set.

6.3 Migration

You can migrate to Alliance Web Platform Server-Embedded 7.2 by installing from a prepared backup file that was created on Alliance Web Platform Server-Embedded 7.0.70 or higher. This backup file is used during the installation of Alliance Web Platform Server-Embedded 7.2.

6.3.1 Create a backup file

The backup file should be created on Alliance Web Platform Server-Embedded 7.0.70 or higher by using the “swp_backup” command. The backup file will contain all the configuration of your current release of Alliance Web Platform Server-Embedded.

6.3.2 Install from prepared backup

On the target system, run the installer for Alliance Web Platform Server-Embedded 7.2, and select the option "Install 7.2 from prepared backup".

During the installation all the data will be migrated from the prepared backup.

After Alliance Access GUI 7.2, Alliance Gateway Admin GUI 7.2 or SWIFT Web Access GUI 7.2 packages are installed, the custom groups will be visible in the Alliance Web Platform Server-Embedded 7.2 Administration GUI.

7 Migrate your Hardware Security Module

7.1 Prerequisites

HSM box

SWIFTNet Link 7.2 is compatible with both software versions 6.0 and 6.1 of the HSM box. You can upgrade the software of the HSM box software to 6.1 either before or after migrating to SWIFTNet Link 7.2. For more information, see also HSM Box Software Upgrade Guide.

HSM Tokens and Cards

The HSM token model iKey 4000 is compatible with SWIFTNet Link 7.2 and supported during the migration to the new HSM token model eToken 5110, which must be completed by end November 2018.

Please also refer to the Knowledge base tip, HSM Token Refresh Entitlement & Frequently Asked Questions (5021623).

7.2 Preparation

HSM card or HSM token

Important Make sure you have the new HSM tokens (eTokens 5110) before you start the migration.

Before migrating the certificates from the current hardware to the new HSM Tokens, log on to the SWIFTNet Online Operations Manager to set up the certificates for recovery, and obtain the activation secrets.

These will be required when migrating the certificates to the new HSM Token (eToken 5110). For more information about the recovery of certificates, see the SWIFTNet Online Operations Manager User Guide.

HSM box

When SWIFTNet Link is configured for HSM box, and you are re-using the same SWIFTNet Link IP address on the new system, you must de-register the old instance of SWIFTNet Link 7.0.50, or higher, from the HSM cluster.

7.3 Migration to HSM Box Software Version 6.1

HSM box

SWIFTNet Link 7.2 will install the HSM client 6.1. After the installation of SWIFTNet Link, you must register the SWIFTNet Link 7.2 instance with the HSM cluster using the new HSM client, which is a native 64-bit application.

Upgrade the HSM boxes from software version 6.0 to 6.1 using the HSM Box Software Upgrade Guide before November 2018. Once the upgrade is completed, no fallback to the HSM Box software version 6.0 is possible.

7.4 Migration to new HSM Token

SWIFTNet Link 7.2 will install the HSM token middleware, Safenet Authentication Client (SAC) 7.2, to provide support for new HSM token (eToken 5110). A maximum of 10 tokens are supported per SWIFTNet Link.

You must migrate the certificates from the current HSM tokens and HSM cards by recovering the certificate to the new hardware device. For more information about how to create or move a certificate to an HSM Token, see the SWIFTNet Link 7.2 Release Letter.

8 Migrate to SWIFTNet Link 7.2

8.1 Prerequisites

- You must be running SWIFTNet Link 7.0.50 or higher
- If third-party applications are used: Remote File Handler 7.0.50 or higher
- If you plan to use an operating system that is different from your current system, then see the section, Changing to a Different Operating System on page 11.
- If you are using HSM cards or HSM tokens, make sure you have the new HSM Tokens

MI Channel

If using SWIFTNet Link without Alliance Gateway for MI Channel:

- IBM MQ: Version 8.0.0.6 client installed on the new environment where Alliance Gateway 7.2 will be running.

Product release dependencies

- SWIFTNet Link 7.2 is compatible with:
  - HSM box software versions 6.0 and 6.1
  - Alliance Messaging Hub 3.3.x, 3.4.x, 3.5.x, and 3.6
  - Remote File Handler 7.0.50
  - Alliance Gateway 7.2
- You can upgrade the HSM box software to 6.1 either before or after migrating to SWIFTNet Link 7.2.
- SWIFTNet Link 7.0.50 and SWIFTNet Link 7.2 can connect to the same HSM cluster.
- SWIFTNet Link 7.0.50 *cannot* connect to Remote File Handler 7.2.
- SWIFTNet Link 7.2 is *not compatible* with Alliance Gateway 7.0.50.

8.2 Preparation

For specific instructions to complete the following, see the SWIFTNet Link 7.2 Release Letter and Installation Guides.

IP address change

If you change the IP address of your SWIFTNet Link instance, then you must Provision the IP address on your VPN box, or on your internal NATing device (switch, router, or firewall).

Implementations always occur during the weekend that starts on Saturday and ends on Sunday as per relevant Allowed Downtime Window (ADW) schedule.

The earliest possible implementation of an order that is validated by SWIFT as being correct is the second weekend following the date of submission.

HSM cards

The HSM cards are not compatible with SWIFTNet Link 7.2. If you use HSM cards, then before you migrate to SWIFTNet Link 7.2, a SWIFTNet Security officer must perform the Setting up a user for recovery procedure using SWIFTNet Online Operations Manager for all certificates that are stored on the HSM cards. This will generate the activation secrets that you will need after migration to recover the certificates onto the new HSM tokens. For more information, see also the how-to video, How to set up a business certificate for recovery (5019548).

If you migrate to SWIFTNet Link 7.2 without generating the activation secrets in advance, then a Security Officer can submit an offline intervention request using Secure Channel to Recover a PKI certificate. For more information, see the how-to video, How to submit Secure Channel Request and download the activation codes (5020117). The action of Recovering a PKI Certificate via Secure Channel is chargeable. For more information, see the Knowledge Base tip, Offline Intervention requests (57923).

Remote File Handler

If the Remote File Handler uses a parameter file (that contains the secrets of the verifier) to connect to SWIFTNet Link, then you must recreate the parameter file.

Once the new file is created, SWIFTNet Link must be updated with the new verifier value (if it is not set to automatic). For more information, see the Release Letter for Remote File Handler for SWIFTNet Link 7.2.

Software owner

Important The software owner of SWIFTNet Link must be the same owner as for Alliance Gateway, if you institution also uses Alliance Gateway.

If the user account for the software owner does not yet exist, then create a user on the operating system who will be the owner of the software.

UNIX or Linux:

The installation can be performed by root and non-root. The non-root account will be the software owner and must have the required settings (the `ulimit` parameters and the IPC resources).

8.3 Migration

SWIFTNet Link 7.2 can be installed from scratch or by using a backup file that was created on SWIFTNet Link 7.0.50 or higher. This file is provided during the installation of SWIFTNet Link 7.2.

8.3.1 Create a Backup File

On SWIFTNet Link 7.0.50 or higher, run the tool to create the backup file that will be used during the Installation of Release 7.2. The backup file will contain all the configuration of your current release of SWIFTNet Link. For more information about running the tool, see the SWIFTNet Link 7.2 Release Letter and Installation Guides.

8.3.2 Install from a Prepared Backup

Important During migration, the same SNL instance for 7.0.50 and 7.2 cannot be running concurrently.
If fallback is required, deregister the new system from the HSM cluster, turn off the new system, start up the old system and re-register to the HSM cluster to resume operations.

On the target system, run the installer for SWIFTNet Link 7.2, and select the option “Install R7.2 from R7 backup”.

If you have already migrated to the HSM Box software version 6.1, then you must register the SWIFTNet Link 7.2 instance with the HSM cluster using the new Luna 64-bit client.

9 Migrate to Alliance Gateway 7.2

9.1 Prerequisites

- Minimum required release: Alliance Gateway 7.0.50 or higher
- If Alliance Access is used for FileAct: Alliance Access 7.1.30 or higher
- If Alliance Entry is used for FileAct: Alliance Entry 7.1.30 or higher
- If third-party applications are used:
  - Remote API 7.0.50 or higher
  - Remote File Handler 7.0.50 or higher
- The IBM MQ 8.0.0.6 client must be installed on the new environment where Alliance Gateway 7.2 will be running.
- With release 7.2, all TCP/IP connections will use Transport Layer Security (TLS) version 1.2 and the supported cryptographic algorithms will be restricted to:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Licensing

- SIPN BAND will be enforced to SIPN BAND -2. You must retrieve an updated license using Secure Channel before you install or migrate to release 7.2.

  Your current environment must be relicensed with a licence sheet that was created after 01 January 2016.
- Alliance Gateway 7.2 will no longer support the SOAP or WSHA licensing options. WSHA related data, and message partners that are configured with WHSA-only are not migrated.

  As of July 2017, all Alliance Gateway WSHA and or SOAP licenses have been updated when the WSHA and SOAP proxy is removed. You can retrieve the updated license using Secure Channel.
- If you remove the following licenses from release 7.2 and they were present in a previous release on which the backup was made, then there will be a warning about these packages is displayed and logged at the end of the installation: 13:MQ HOST ADAPTER, 14:RA HOST ADAPTER, 57:COPY TO, 60:FTI, 61:FTA

Transaction Delivery Agent (TDA)

- Transaction Delivery Agent 7.2 will be released on 12 January 2018. Transaction Delivery Agent 7.2 will be available as a native 64-bit application and it will only support IBM MQ 8.0.0.6 Client.
- Support for Transaction Delivery Agent 4.0.1, 4.0.2, and 4.0.10 will end in November 2018, at which point you must install Transaction Delivery Agent 7.2.
- Transaction Delivery Agent 7.2 will require a fresh install on the new operating system baseline and the use of Remote API 7.2.

Product release dependencies

Alliance Gateway 7.2 is compatible with:

- Alliance Access 7.1.23, or higher
- Alliance Entry 7.1.23, or higher
- Alliance Messaging Hub 3.3.x, 3.4.x, 3.5.x, and 3.6
- Remote API 7.0.50
- SWIFTNet Link 7.2

9.2 Preparation

For specific instructions to complete the following, see the Alliance Gateway 7.2 Release Letter and Installation Guides.

Software owner

The software owner of Alliance Gateway must be the same owner as for SWIFTNet Link.

UNIX or Linux:

The installation can be performed by root and non-root. The non-root account will be the software owner and must have the required settings (the `ulimit` parameters and the IPC resources).

9.3 Migration

Alliance Gateway 7.2 can be installed from scratch or by using a backup file that was created on Alliance Gateway 7.0.50 or higher. This file is provided during the installation of Alliance Gateway 7.2.

9.3.1 Create a Backup File

Create a backup of the Alliance Gateway database using the sag_system command of Alliance Gateway 7.0.50. See Back Up the Alliance Gateway Database in the Alliance Gateway Administration and Operations Guide.

9.3.2 Create Archives

If you want to keep the Alliance Gateway events, then archive the Event Log:

- To archive from the Monitoring > Event Log page in Alliance Gateway Administration, see Event Log Search in the Alliance Gateway Administration and Operations Guide.
- To use the sag_system command to create the archive, see Archive the Alliance Gateway Event Log in the Alliance Gateway Administration and Operations Guide.

If you want to keep the file transfer information, then it must be archived. Make sure that no retries are ongoing.

- To archive from the Monitoring > File Transfer Monitoring page in Alliance Gateway Administration, see File Transfer Monitoring in the Alliance Gateway Administration and Operations Guide.
- To use the sag_system command to create the archive, see Archive the File Transfer History in the Alliance Gateway Administration and Operations Guide.

9.3.3 Install from a Prepared Backup

Install Alliance Gateway 7.2 from the prepared backup file.
All configuration data from 7.0.50 will be migrated except for the following:

- The file transfers data from FTA/FTI
- The events of the Alliance Gateway Event Journal
- The SERVER “sag_segres” configuration (because SWIFTNet Link is re-installed from scratch. Note that CLIENT “sag_segres” configuration is restored)
- The “sagta_ra.cfg” configuration (The file will be created during installation of Alliance Gateway 7.2 and will contain the hostname/IP address of the new system.)
- The “sag_configeventlog –switchMode”

When selecting the option “restore instance configuration file”, the migration restores those below instance configuration files:

- The SAG SSL certificate
- The SAG master key and related files
- The LDAP SSL certificates
- The MQ TAB file

10 Migrate to Alliance Access 7.2

10.1 Prerequisites

- Minimum required release: Alliance Access 7.1.23 or higher
- Hosted Database is used: Oracle version 12.1 or higher
- IBM MQ: IBM MQ 8.0.0.6 client on the new environment where Alliance Access 7.2 will be running.

  Note *Alliance Access 7.2 will not support IBM MQ server mode.*

- Alliance Access SOAP Host Adapter: Make sure that the back office application using this connection can use SOAP Host Adapter and the latest crypto algorithm of TLSv1.2.

  Note *With release 7.2, all TCP/IP connections will use Transport Layer Security (TLS) version 1.2 and the supported cryptographic algorithms will be restricted to:*
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- Alliance Access with a third party ADK component: the component must be compatible with Alliance Access 7.2. If you have ADK components that are no longer used, you must remove them from Alliance Access 7.1.23, or higher, before migration to Alliance Access 7.2.

  Note *ADK components that were compatible with Alliance Access 7.1 are not compatible with Alliance Access 7.2. Please contact your vendor.*

- Alliance Access with a custom Integration Layer (IPLA) component: the IPLA component must be compatible with Alliance Access 7.2

  The following IPLA components are compatible with Alliance Access 7.2:

  - Connector for T2S version 1.2.10
  - Connector for Sanctions version 1.2.40
  - Connector for SWIFT gpi (all versions)

  For other components, contact your vendor for more details.

- Alliance Workstation is decommissioned:

  Make sure that operators and end-users of Alliance Access are trained to use the Alliance Web Platform GUI applications that replace Alliance Workstation.

- CASmf is decommissioned:

  - Remove all Message Partners in Alliance Access 7.1.23 that use CAS.
  - Check that Alliance Access licensing does not have the option 18:CAS TCP/IP selected. You can retrieve the latest license sheet using Secure Channel.

CREST Over SWIFTNet:

- Tuxedo 12cR2 with patch RP089 or higher. The patch will be available for download from the Oracle website.
- Tuxedo will mandate that encryption keys have a minimum length of 128 bit. If it does not work because the client is using an old version of CRPI or NSL, you must manually change the key length back to 0. For more information, see *Encrypting Messages* in the *CREST over SWIFTNet - Customer Application Integration Guide* when it is available for Release 7.2.
- CRnet File Interface (CRFI) and CRnet Programming Interface (CRPI): configure Local authentication (LAU) between the back-office application and Alliance Access.
- CRnet Programming Interface (CRPI) clients: use the latest version of the CRPI client. CRPI client will remain in 32-bit mode, and will be supported on AIX, Linux, Windows, and Oracle Solaris.

The current version of CRPI and NSL and the new CRPI 7.2 and NSL 7.2 can connect to Alliance Access 7.2.

After the Alliance Access 7.2 migration, SWIFT recommends that you upgrade NSL and CRPI to the 7.2 versions.

Product release dependencies

- Alliance Access 7.1.23 or higher can connect to Alliance Gateway 7.2
- Alliance Access 7.2 *cannot* connect to Alliance Gateway 7.0.x with SWIFTNet Link 7.0.x

10.2 Preparation

For specific instructions to complete the following, see the Alliance Access 7.2 Release Letter and Installation Guides.

Software owner

Create a user on the operating system who will be the owner of the software.

- **Windows**:

  As from release 7.2, you must have one user account on Windows that is not part of the Administrator group. This account will be the software owner and will manage the Alliance Access application. However, installation and un-installation can be done by an Administrator.

- **UNIX or Linux:**

  The installation can be performed by root and non-root. The non-root account will be the software owner and must have the required settings (the `ulimit` parameters and the IPC resources).

Embedded database on AIX

When using the embedded database on AIX, the I/O completion ports (iocp0) default setting must be changed from “Defined” to “Available”.

Hosted database

When using hosted database, create a new Oracle instance with AL32UTF8 character set. Other requirements will be listed in the Installation guide of Release 7.2.

Firewall and ports

Open the ports that will be used by Alliance Access on the firewall.

If you will use the default ports, then you can find the list of ports in the Installation guides of the current version of Alliance Access 7.1.23.

If you are not sure which ports will be used, then after the migration, check the list of the ports on the system where release 7.2 was installed:

- UNIX: the files `/etc/services`
- Windows: `%WINDIR%\system32\drivers\etc`

Communication channels

Prepare all the communication channels that will be used between Alliance Access and the back-office applications.

When using CREST component, open the ports that will be used by CRPI and NSL to connect to Alliance Access on the firewall.

10.3 Migration

You can migrate to Alliance Access 7.2 by installing it on a new environment from a prepared backup file. The migration described in these phases is also applicable to Alliance Access with Hosted Database.

If you install Alliance Access 7.2 from a prepared backup, then you can migrate from Alliance Access 7.1.23 or higher, in several phases to limit downtime as much as possible.

1. Prepare a full backup of the current system, Alliance Access 7.1.23 or higher, and install Alliance Access 7.2 on the new environment from prepared backup. Update and check the configuration and prepare for going live. During this configuration phase, the current system continues to process live traffic.
2. Update the new environment using incremental backup files from the current system, and continue to use the current system for live traffic. You can create the incremental backups multiple times, but there must be at least one full backup done first.
3. When ready to complete the migration, use either a full backup or an incremental backup to bring the new system up-to-date. Switch over to using the new system.

This allows you to plan and implement the configuration phase in advance of going live with release 7.2.

10.3.1 Prepare the Backup File for Upgrade

SWIFT will provide a stand-alone **saa-prepare-backup** tool that generates the backup file (snapshot) that can be used to install Alliance Access 7.2 and migrate the data. The backups can be full or incremental (partial) and can be taken while Alliance Access is running.

These backups will inject on the target Alliance Access 7.2 system additional changes that happened on the source system since a previous snapshot.

The name of the backup file includes the date of the extraction and the type of the snapshot (full or incremental). The content is compressed and encrypted. The backup files are also restricted to the software owner user.

The backup files include:

Full backup	Incremental backup
All configuration data and RMA authorisations	Configuration: • Operators • Message Partners • Logical Terminals • Emission Profiles • Reception Profiles • Configuration parameters • Security Configuration parameters • RMA authorisations
Optionally, messages: • Backed-up archives • Archives • Live	Optionally, messages: • Backed-up archives (New ones) • Archives (New ones) • Live (Day with new messages)
Optionally, events: • Backed-up archives • Archives • Live	Optionally, events: • Backed-up archives (New ones) • Archives (New ones) • Live (Day with new messages)

10.3.2 Migration phase 1

1. On the current system for Alliance Access 7.1.23 or higher, take a full backup, using a stand-alone **saa-prepare-backup** tool from Alliance Access 7.2. The backup can be taken while Alliance Access 7.1.23 or higher is running.
2. On the new environment, where Alliance Access 7.2 will be installed, run the installer of 7.2 Release and install 7.2 from prepared backup (full snapshot).
3. Once the target Alliance Access 7.2 system is installed with the migrated data, you can start to make configuration changes and adaptations to ensure that this 7.2 system is fully operational.
4. All the configuration parameters that contain a path will be set to the default values of the target system. Therefore, you have to check the values and adapt them based on your configuration.

10.3.3 Migration phase 2

1. Before go-live date, stop the current system, that is Alliance Access 7.1.23, or higher, and take the final incremental backup.
2. On Alliance Access 7.1.23 or higher, launch the stand-alone tool and make the final snapshot.

   The second snapshot can generate an incremental (partial) or full snapshot, based on your choice. If you select incremental backup, then the snapshot will include only the changed data during run-time, listed in step 3 since the last full snapshot was taken.

3. On the new environment for Alliance Access 7.2, launch the installer and install again from the second prepared backup (incremental snapshot).

   The configuration data from the second (incremental) snapshot will be merged into the 7.2 instance to accommodate the changes that were already done.

   Therefore, in case of the incremental snapshot, the following will be migrated:

   - For the configuration information:

     - The missing entries are added
     - The existing entries are merged (for Operator, only the password related data is updated. For Message Partners, Logical Terminals, Emission Profiles, and Reception Profiles, only the session information is updated).

   - For the message information

     - The missing backed-up message archives are added.
     - The missing message archives are added and the destination related live messages days are dropped.
     - The missing Live messages are added and the destination related live messages days are dropped.

   - For the event information

     - The missing backed-up event archives are added.
     - The missing event archives are added and the destination related live messages days are dropped.
     - The missing Live events are added and the destination related live messages days are dropped.

   Note *The messages or events data from the same day are never merged. The data is replaced according to the above description.*

   The Reporting data will not be migrated. Only the Report Templates are transferred during the migration phases.

With these options, you are completely in control of the migration plan. Multiple full or partial snapshots can be run against the Alliance Access source instance allowing a flexible migration program to Alliance Access 7.2.

10.3.4 Convert Backups of Message and Event Log Archives

The backed-up archives performed between Alliance Access 6.2 and Alliance Access 7.1.23, or higher, cannot be restored into Alliance Access 7.2 immediately. Before they can be restored, they must be converted into a format accepted by Alliance Access 7.2.

SWIFT will provide a conversion tool in addition to the installation software of 7.2 to ease the conversion process. The tool can convert several backups simultaneously. The tool can be installed on a standalone system or on the Alliance Access system. See the Installation guide for information on how to install and use the tool.

It is highly advised to install the tool on another system as it consumes memory and CPU while running.

The tool will include an embedded database. There is no link between the conversion tool and Alliance Access 7.2 software. Both work separately of each other with its own database.

The hardware requirements, OS requirements and the disk space for the conversion tool are the same as for Alliance Access 7.2.

Note *If during the migration phases, the backed-up archives are not included in the snapshots, then you must convert them using the tool, prior to restoring them into Alliance Access 7.2.*

If during the migration phases, Live and Archived messages or journal events were not migrated, then you have to archive the Live data and then backup all the archives. After that, use the tool to convert the backups prior to restoring them into Alliance Access 7.2.

Note *The backed-up archives performed before Alliance Access 6.2 can be restored directly into Alliance Access 7.2. Those backups will not require the conversion.*

10.3.5 Migrate Alliance Access with CREST component

The current version of CRPI and NSL and the new CRPI 7.2 and NSL 7.2 can connect to Alliance Access 7.2. After the Alliance Access 7.2 migration, customers are advised to upgrade their NSL and CRPI to the 7.2 versions.

Currently, the end-users that have no CRNet role can perform some CRNet-related actions, such as exchanging CREST traffic. This will not be authorized as from release 7.2.

Release 7.2 provides more granular roles for CRNet. SWIFT strongly recommends that you assign roles to the current end-users.

11 Migration to Alliance Entry 7.2

11.1 Prerequisites

- Minimum required release: Alliance Entry 7.1.23 higher
- Alliance Workstation is decommissioned: make sure operators and end-users of Alliance Entry are trained to use the Alliance Web Platform applications that replace Alliance Workstation.

Product release dependencies

- Alliance Entry 7.1.23 or higher can connect to Alliance Gateway 7.2
- If FileAct is used, then Alliance Entry 7.1.30 or higher is required to connect to Alliance Gateway 7.2
- Alliance Entry 7.2 *cannot* connect to Alliance Gateway 7.0.x with SWIFTNet Link 7.0.x

11.2 Preparation

For specific instructions to complete the following, see the Alliance Entry 7.2 Release Letter and Installation Guides.

Software owner

Create a user on the operating system who will be the owner of the software.

As from release 7.2, you must have one user account on Windows that is not part of the Administrator group. This account will be the software owner and will manage the Alliance Entry application. However, installation and un-installation can be done by an Administrator.

Firewall and ports

Open the ports that will be used by Alliance Entry on the firewall.

If you will use the default ports, then you can find the list of ports in the Installation guides of the current version of Alliance Entry 7.1.23.

If you are not sure which ports will be used, then after the migration, check the list of the ports in on the system the Release 7.2 was installed:

Windows: `%WINDIR%\system32\drivers\etc`

Communication channels

Prepare all the communication channels that will be used between Alliance Entry and back-office applications.

11.3 Migration

You can migrate to Alliance Entry 7.2 by installing it on a new environment from a prepared backup file.

If you install Alliance Entry 7.2 from a prepared backup, then you can migrate from Alliance Entry 7.1.23 or higher, in several phases to limit downtime as much as possible.

1. Prepare a full backup of the current system, Alliance Entry 7.1.23 or higher, and install Alliance Access 7.2 on the new environment from prepared backup. Update and check the configuration and prepare for going live. During this configuration phase, the current system continues to process live traffic.
2. Update the new environment using incremental backup files from the current system, and continue to use the current system for live traffic. You can create the incremental backups multiple times, but there must be at least one full backup done first.
3. When ready to complete the migration, use either a full backup or an incremental backup to bring the new system up-to-date. Switch over to using the new system.

This allows you to plan and implement the configuration phase in advance of going live with release 7.2.

11.3.1 Prepare the Backup File for Upgrade

SWIFT will provide a stand-alone **saa-prepare-backup** tool that generates the backup file (snapshot) that can be used to install Alliance Entry 7.2 and migrate the data. The backups can be full or incremental (partial) and can be taken while Alliance Access is running.

These backups will inject on the target Alliance Entry 7.2 system additional changes that happened on the source system since a previous snapshot.

The name of the backup file includes the date of the extraction and the type of the snapshot (full or incremental). The content is compressed and encrypted. The backup files are also restricted to the software owner user.

The backup files include:

Full backup (snapshot)	Incremental backup
All configuration data and RMA authorisations	Configuration: • Operators • Message Partners • Logical Terminals • Emission Profiles • Reception Profiles • Configuration parameters • Security Configuration parameters • RMA authorisations
Optionally, messages: • Backed-up archives • Archives • Live	Optionally, messages: • Backed-up archives (New ones) • Archives (New ones) • Live (Day with new messages)
Optionally, events: • Backed-up archives • Archives • Live	Optionally, events: • Backed-up archives (New ones) • Archives (New ones) • Live (Day with new messages)

11.3.2 Migration phase 1

1. On the current system for Alliance Entry 7.1.23 or higher, take a full backup, using a stand-alone **saa-prepare-backup** tool from Alliance Entry 7.2. The backup can be taken while Alliance Entry 7.1.23 or higher is running.
2. On the new environment, where Alliance Entry 7.2 will be installed, run the installer of 7.2 Release and install 7.2 from prepared backup (full snapshot).
3. Once the target Alliance Entry 7.2 system is installed with the migrated data, you can start to make configuration changes and adaptations to ensure that this 7.2 system is fully operational.
4. All the configuration parameters that contain a path will be set to the default values of the target system. Therefore, you have to check the values and adapt them based on your configuration.

11.3.3 Migration phase 2

1. Before the go-live date , stop the current system, that is Alliance Entry 7.1.23 or higher, and take the final backup snapshot.
2. On the current system Entry 7.1.23, launch the stand-alone tool and make the final snapshot.

The second snapshot can generate an incremental (partial) or full snapshot, based on your choice. If you select incremental backup, then the snapshot will include only the changed data listed in step 3 since the last full snapshot was taken.

3. On the target system with Alliance Entry 7.2, launch the installer and install again from the second prepared backup (incremental snapshot).

   The configuration data from the second (incremental) snapshot will be merged into the 7.2 instance to accommodate the changes that were already done.

   Therefore, in case of incremental snapshot the following will be migrated:

   - For the configuration information:

     - The missing entries are added
     - The existing entries are merged (for Operator, only the password related data is updated. For Message Partners, Logical Terminals, Emission Profiles, and Reception Profiles, only the session information is updated).

   - For the message information

     - The missing backed-up message archives are added.
     - The missing message archives are added and the destination related live messages days are dropped.
     - The missing Live messages are added and the destination related live messages days are dropped.

   - For the event information

     - The missing backed-up event archives are added.
     - The missing event archives are added and the destination related live messages days are dropped.
     - The missing Live events are added and the destination related live messages days are dropped.

   Note *The messages or events data from the same day are never merged. The data is replaced according to the above description.*

   Note *The Reporting data will not be migrated. Only the Report Templates are transferred during the migration phases.*

11.3.4 Convert Backups of Message and Event Log Archives

The backed-up archives performed between Alliance Entry 7.0 and Alliance Entry 7.1.23 cannot be restored into Alliance Entry 7.2 immediately. Before they can be restored, they must be converted into a format accepted by Alliance Entry 7.2.

SWIFT will provide a conversion tool in addition to the installation software of 7.2 to ease the conversion process. The tool can convert several backups simultaneously. The tool can be installed on a standalone system or on the Alliance Entry system. See the Installation guide for information on how to install and use the tool.

It is highly advised to install the tool on another system as it consumes memory and CPU while running.

The tool will include an embedded database. There is no link between the conversion tool and Alliance Entry 7.2 software. Both work separately of each other with its own database.

The hardware requirements, OS requirements and the disk space for the conversion tool are the same as for Alliance Entry 7.2.

Note *If during the migration phases, the backed-up archives are not included in the snapshots, then you must convert them using the tool, prior to restoring them into Alliance Entry 7.2.*

If during the migration phases, Live and Archived messages or journal events were not migrated, then you have to archive the Live data and then backup all the archives. After that, use the tool to convert the backups prior to restoring them into Alliance Entry 7.2.

Note *The backed-up archives performed before Alliance Entry 7.0 can be restored directly into Alliance Entry 7.2. Those backups will not require the conversion.*

12 Using Alliance Messaging Hub with Release 7.2

Alliance Messaging Hub 3.3.x, 3.4.x, 3.5.x, and 3.6 are compatible with Alliance Gateway 7.2 and SWIFTNet Link 7.2. If you are already using AMH 3.3 or higher, then upgrading Alliance Messaging Hub is optional.

12.1 AMH 3.6

To benefit from the new FileAct enhancements in SWIFTNet 7.2, customers must migrate to AMH 3.6. You can find a description of the new features on page 13.

Note *Alliance Messaging Hub 3.6* is not compatible with *Alliance Gateway 7.0.x and SWIFTNet Link 7.0.x.*

Customers must first migrate to Alliance Gateway 7.2 and SWIFTNet Link to 7.2 before upgrading to AMH 3.6.

The *AMH Upgrade Notes* for AMH 3.6 will provide information on how to prepare for and install AMH 3.6.

For more information about the features in AMH 3.6, see the knowledge base tip, AMH - What to expect in release 3.6 (5021678).

12.2 AMH 3.3.x, 3.4.x, and 3.5.x

To use Alliance Gateway 7.2 and SWIFTNet Link 7.2 with AMH 3.3.x, AMH 3.4.x, or AMH 3.5.x, you must set the following JVM property on your application server to enable these cypher suites:

```
Dcom.swift.swtl.SSLCiphers=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_
RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_EMPTY
_RENEGOTIATION_INFO_SCSV
```

For more information, see your application server documentation.

13 Using Alliance Remote Gateway 7.2

Customers who connect Alliance Access or Alliance Entry to Alliance Remote Gateway can migrate their system in the Test and Training environment from October 2017, and in the Live environment from November 2017.

During the migration to release 7.2, SWIFT will provide:

- two concurrent environments (existing 7.1, new 7.2) in Test
- two concurrent environments (existing 7.1, new 7.2) in Live

Legal Notices