

Alliance Cloud

Getting Started

This document describes the different tasks customers must perform to get started with Alliance Cloud. These tasks include how to set up tokens, channel certificates, and application channels, how to configure the Alliance Cloud connectivity options, and how to get started with the Admin centre, Message management, and Event log modules.

03 July 2025

Link to this document: <https://www2.swift.com/go/book/book200729>

Table of Contents

Preface	5
Significant Changes	6
1 What is Alliance Cloud?	8
2 How does Alliance Cloud Work?	9
3 Before you Start with Alliance Cloud	12
4 Alliance Cloud Getting Started Roadmap	14
5 Alliance Cloud Getting Started Checklist	15
6 Checklist for Customers Migrating to Alliance Cloud	21
7 Alliance Cloud Support Page	23
8 Ordering	24
8.1 Order Alliance Cloud	24
8.2 Request an Additional Connected BIC	29
8.3 Add a BIC to Existing Alliance Cloud	30
8.4 Central Activation of FIN for New BICs	31
8.5 Migrate your SwiftNet Services to Alliance Cloud	32
8.6 Migrate your FIN Services to Alliance Cloud	33
9 Security Officer Tasks	35
9.1 Order Personal Tokens from Swift	38
9.2 Create Back-up Security Officers	39
9.3 Create a Distinguished Name (DN)	41
9.4 Set Up a User for Certification	42
9.5 Authorise the DN and Retrieve Activation Secrets	44
9.6 Assign RBAC Roles	46
9.7 Approve the Assigned RBAC Roles	52
9.8 Activate Token	53
9.9 Token Renewal	55
9.10 Channel Certificate Recovery	55
9.11 New Online Security Officer Requirements when Migrating to Alliance Cloud	56
10 Alliance Cloud Administrator Tasks: User and Role Management	58
10.1 Initial Login by Alliance Cloud Users	60
11 Message Management Administrator Tasks	62
11.1 Add an Application Channel in Alliance Cloud	64

11.2 Application Channel Limitations	64
12 Swift Integration Layer (SIL) Installation and Configuration Tasks	66
12.1 Swift Integration Layer End of Support in 2026	68
12.2 Alliance Cloud Connector	68
12.3 Configure and Use Swift Integration Layer	69
12.4 Use Active/Standby for SIL Instances	78
12.5 Test SIL Connectivity with Alliance Cloud	80
13 Alliance Cloud MQ Connector Installation and Configuration Tasks	82
13.1 Use Active/Standby for MQ Connector Instances	83
14 Swift Messaging API Tasks	85
15 Message Management Operator Tasks	86
16 Event Log Administrator Tasks	88
17 Relationship Management Portal Tasks	89
17.1 Relationship Management (RMA) Administrator Tasks	89
17.2 Relationship Management (RMA) Operator Tasks	90
18 Set up the Environment for Alliance Cloud	92
18.1 Web Browser Configuration	92
18.2 TLS Security	93
18.3 Configure Firewall Settings	93
18.4 Install Token Software	98
18.5 Internet Access Inclusion/Exclusion (Optional)	98
19 Test your Message Flows	100
20 Plan Volume and Throughput Tests for Alliance Cloud	101
21 Delivery Subset Sharing Mode and Throughput Tasks	102
22 Request Activation on the Live Environment	104
23 Online Help	105
24 Swift Training	106
24.1 Swift Smart Modules for Alliance Cloud	106
25 Terminology	107
Appendix A About Alliance Cloud	111
A.1 Alliance Cloud Modules	111
A.2 Types of Alliance Cloud Users, Roles, and Related Functions	111

A.3 Roles, Users, Units, and Business Entities	114
A.4 Workflows	115
A.5 Message Creation, Verification, Repair, and Approval	116
A.6 Swift Standards	118
A.7 Unsupported Messages and Exceptions in Alliance Cloud	124
A.8 Token-Based Certificates and Channel Certificates	127
A.9 Application Channels	128
A.10 Alliance Cloud Connectivity Options	129
Legal Notices	131

Preface

Purpose of the document

This document describes the different tasks customers must perform to get started with Alliance Cloud. These tasks include how to set up tokens, channel certificates, and application channels, how to configure the Alliance Cloud connectivity options, and how to get started with the Admin centre, Message management, and Event log modules.

For more information about workflows, how to manage security officers, tokens and channel certificates, how to configure application channels in Swift Integration Layer (SIL) or in the Alliance Cloud Connectors, and how to use the File, REST, MQ, and Swift Messaging API channels, see the [Alliance Cloud Operations Guide](#).

Audience

This document is for the following users:

- all Alliance Cloud users
- security officers
- system administrators
- staff who will install and configure Swift Integration Layer

For Business Connect

If you use Alliance Cloud in the context of Business Connect, or you are an Alliance Cloud user planning to switch to Business Connect, then read the [Business Connect Getting Started](#) guide first. Some information in the *Alliance Cloud Getting Started* does not apply or works differently for Business Connect customers.

Terminology

For more information about the acronyms and terms used in this document, see [Terminology](#) on page 107. See also the [Swift Glossary](#).

Related documentation

- [Alliance Cloud - API Connector - Getting Started](#)
- [Alliance Cloud - API Connector - Getting Started with the SDK](#)
- [Alliance Cloud - API Connector - JSON Format Reference](#)
- [Alliance Cloud - API Connector - Release Letter for the SDK](#)
- [Alliance Cloud Connectors - Release Letter - MQ Connector](#)
- [Alliance Cloud Operations Guide](#)
- [Alliance Cloud Release Letter](#)
- [Alliance Cloud Security Guidance](#)
- [Alliance Cloud Service Description](#)
- [RMA Evolution Frequently Asked Questions](#)
- [Relationship Management Portal Getting Started](#)
- [Relationship Management Portal User Guide](#)
- [Swift Integration Layer 2.4.0 Release Letter](#)
- [Swift Integration Layer User Guide](#)
- [SwiftNet Online Operations Manager User Guide](#)

Significant Changes

The following tables list all significant changes to the content of the *Alliance Cloud Getting Started* guide since the following previous editions. These tables do not include editorial changes that Swift makes to improve the usability and comprehension of the document.

New and updated information since the April 2025 edition

Description	Location
This topic summarises the Alliance Cloud connectivity options.	Alliance Cloud Connectivity Options on page 129
A checklist is available for customers who are migrating to Alliance Cloud from another Swift interface, such as Alliance Access or Alliance Lite2.	Checklist for Customers Migrating to Alliance Cloud on page 21
If you need to create more than 10 application channels, then contact Swift Professional Services or the Swift Product team to request assistance in finding the optimal configuration.	Application Channel Limitations on page 64
This topic describes how customers can request activation of high throughput, change the delivery subset sharing mode, and remove custom delivery subsets along with the deadlines before migration or activation. Some of these tasks are only for migrating customers.	Delivery Subset Sharing Mode and Throughput Tasks on page 102
Web browser information has been updated.	Web Browser Configuration on page 92
Transport Layer Security-intercepting security solutions may prevent connection to some Swift services, especially the services that rely on personal tokens for mutual authentication. These solutions should not interrupt the TLS flow for Swift services.	TLS Security on page 93
The firewall settings information now includes the Alliance Cloud Connectors and the Swift Messaging API.	Configure Firewall Settings on page 93

New and updated information since the 19 February 2025 edition

Description	Location
The Alliance Cloud MQ Connector enables customers to set up IBM MQ queues to exchange FIN and InterAct messages with Alliance Cloud.	Alliance Cloud Getting Started Checklist on page 15 Alliance Cloud MQ Connector Installation and Configuration Tasks on page 82
Before requesting an additional connected BIC for an existing Alliance Cloud group, the Alliance Cloud group (business entity) must be created. It will be created between one and two weeks after you order Alliance Cloud for your main BIC.	Request an Additional Connected BIC on page 29

New and updated information since the 22 October 2024 edition

Description	Location
The ordering section has been updated to include information for new Alliance Cloud customers and migrating customers.	Ordering on page 24
This topic describes how to migrate or create new security officers in different migration scenarios to Alliance Cloud.	New Online Security Officer Requirements when Migrating to Alliance Cloud on page 56

Description	Location
A Knowledge Base article explains how to plan volume and throughput tests.	Plan Volume and Throughput Tests for Alliance Cloud on page 101
The Alliance Cloud Support page includes useful links to important Alliance Cloud news and resources.	Alliance Cloud Support Page on page 23

New and updated information since the 29 August 2024 edition

Description	Location
If your institution plans to use the archive feature of Alliance Cloud, then you must use an application channel that does not allow outgoing messages in your archiving configuration.	Application Channels on page 128
You can activate future mode only during the future mode testing period. Information about when this period starts has been added to this topic.	Future mode on page 118
This topic describes the suggested RBAC roles for security officers in institutions using Alliance Access that migrate to Alliance Cloud.	RBAC roles for Migrating Alliance Access Customers on page 51

New information since the 13 August 2024 edition

Description	Location
New topic that explains the steps to follow if Swift Integration Layer (SIL) cannot successfully connect to Alliance Cloud.	Test SIL Connectivity with Alliance Cloud on page 80
New topic with information for firewall configuration for the Swift Messaging API	Application-to-Application: Swift Messaging API on page 96

Updated information since the June 2024 edition

Description	Location
Clarification about Alliance Connect Connectivity pack(s)	Order Alliance Cloud on page 24
User access restriction between BICs in a business entity	Add a BIC to Existing Alliance Cloud on page 30
You can disable internet access to Alliance Cloud.	Internet Access Inclusion/Exclusion (Optional) on page 98

Updated information since the May 2024 edition

Description	Location
The Distinguished Names (DNs) for back-up security officers <u>must</u> be created under a <u>level 2 DN</u> .	Create Back-up Security Officers on page 39

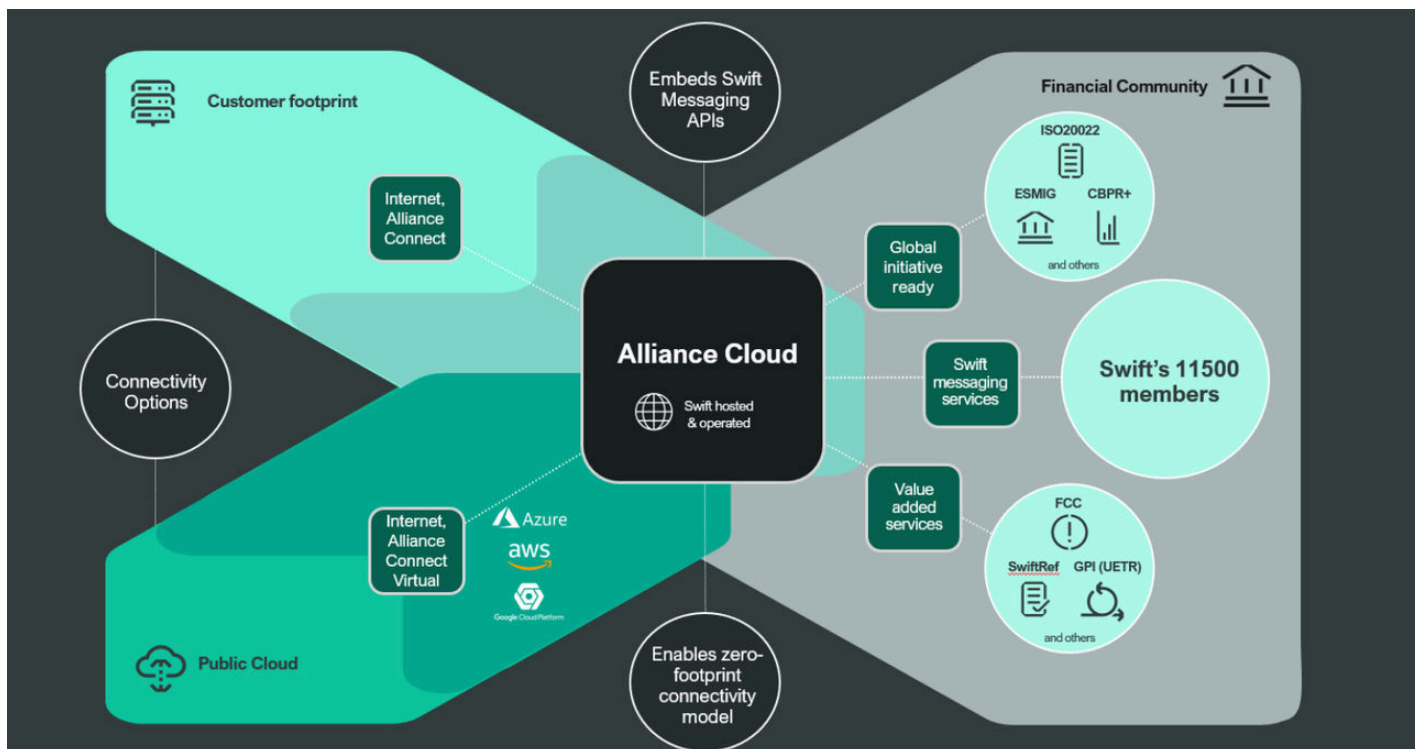
1 What is Alliance Cloud?

Alliance Cloud is a universal channel to the financial community and to Swift value-added services and initiatives. It offers a window to Swift messaging services. It facilitates smooth integration with your back office, enabling application-to-application flows.

Alliance Cloud provides:

- Manual message creation capabilities for MT (FIN) business messages (such as a fin.103) and FIN system messages. For information about MX formats for manual message creation, see Knowledge Base article [5025814](#): **Alliance Cloud message management functionalities**.
- Access to value-added services including the Relationship Management Portal, Reference Data (SwiftRef), Swift GPI (global payments innovation), Transaction Screening, and Payment Controls Services
- Seamless integration with your back office for application-to-application flows
- Message processing flow configuration
- Access to message details and history
- Access to the audit event log

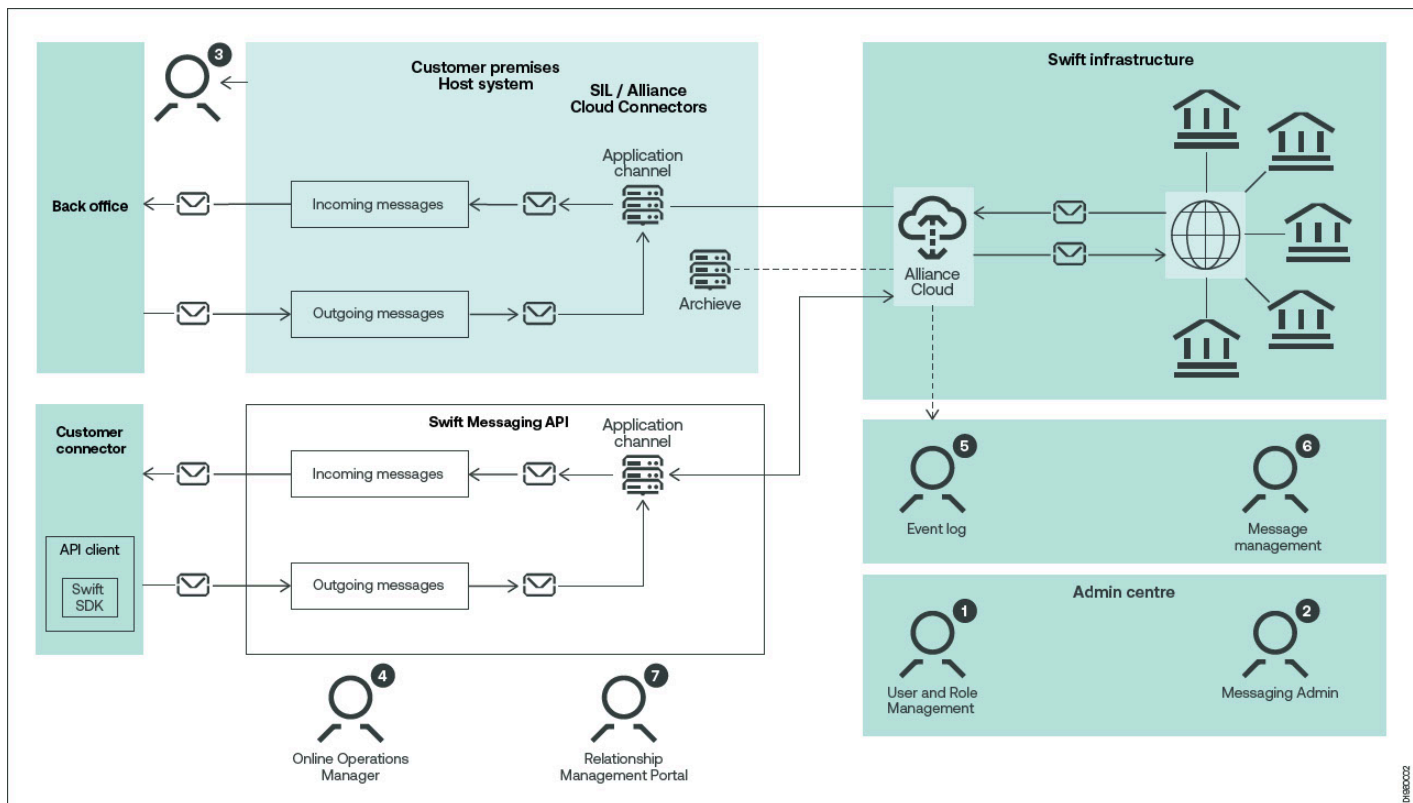
Different Alliance Cloud connectivity options are available to exchange messages between your back office and Alliance Cloud.



2 How does Alliance Cloud Work?

Customers can send messages and files automatically with Alliance Cloud. In the Message management module, customers can also manually create MT (FIN) business messages (such as a fin.103) and FIN system messages. For information about MX formats for manual message creation, see Knowledge Base article [5025814: Alliance Cloud message management functionalities](#).

A browser-based GUI provides access to the Admin centre, Message management, and Event log modules. The role that is assigned to each user determines which modules they can access.



The following users are involved in the initial configuration and the day-to-day use and management of Alliance Cloud.

In some smaller institutions, a user may have multiple roles. Make sure that you follow your organisation's security policies.

The security officers, the SIL administrator (also known as the SIL_Owner), and the Alliance Cloud Connectors administrator perform tasks to get started with Alliance Cloud. They do not configure or use the Alliance Cloud GUI itself.

Your institution must designate different administrators. The security officers will create the Distinguished Names (DN) and assign the RBAC (Role-Based Access Control) roles to each Alliance Cloud administrator and user. The Alliance Cloud administrators will automatically receive the **Administrator** role in Alliance Cloud during the first login. The Alliance Cloud administrators will then create the other administrators and users in the Alliance Cloud GUI.

User Role	Description	More information
1	Alliance Cloud administrators: user and role management These administrators define users and roles in the Admin centre and assign roles to users. An institution must have at least two of these administrators. They are assigned the Administrator role in Alliance Cloud. They work closely with: - Security officers, who provide the information related to application channels - Message management administrators	Alliance Cloud Administrator Tasks: User and Role Management on page 58
2	Message management administrator Message management administrators create, manage, and approve application channels and units, and configure workflows. They are assigned the Message management configurator role in Alliance Cloud. They work closely with: - Security officers, who provide the information related to application channels - Alliance Cloud administrators - SIL administrators	Message Management Administrator Tasks on page 62
3	System administrator, the SIL administrator (the SIL_Owner), and the Alliance Cloud Connectors administrator System administrators install Swift Integration Layer or the Swift Microgateway and Alliance Cloud Connectors. They are also responsible for the installation of applications which require admin rights and for the configuration of firewalls. SIL administrators use the SIL GUI to configure SIL after installation, download the channel certificate (if applicable), and test and start application channels. Alliance Cloud Connector administrators use the Connector GUI to configure the Connector after installation, download the channel certificate (if applicable), and test and start application channels. SIL and Alliance Cloud Connector administrators work closely with: - Security officers, who provide the information related to application channels - Message management administrators	Swift Integration Layer (SIL) Installation and Configuration Tasks on page 66 Alliance Cloud MQ Connector Installation and Configuration Tasks on page 82 Set up the Environment for Alliance Cloud on page 92
4	Security officer Security officers play an important role in the certification process for Alliance Cloud users and application channels. Security officers: - Manage certification through the SwiftNet Online Operations Manager (O2M). - Create the user identity with a Distinguished Name (DN), a user name, and a certificate. - Give the personal token password and activation code to all Alliance Cloud administrators and users. - Create the DNs and certificates to be used for application channels. - Give the DNs created for each application channel to the SIL administrator, the Alliance Cloud Connector administrator, and the Message management administrator. - Manage Role-Based Access Control for Swift services. - For channel certificates: give the activation secrets to the SIL administrator Each institution must have at least two security officers. Security officers must liaise with all Alliance Cloud users and work closely with administrators and the SIL and Alliance Cloud Connector administrators.	Security Officer Tasks on page 35
5	Event log administrator The Event log administrator views and investigates events.	Event Log Administrator Tasks on page 88
6	Message management operator Message management operators can manually create messages, view and search for messages, and approve messages based on the specific conditions and criteria configured in the workflow. Approval requires a signature before the message is sent to Swift. These operators can also redistribute messages manually to the back office. They are assigned the Message management operator role in Alliance Cloud.	Message Management Operator Tasks on page 86
7	Relationship Management administrator and operator Relationship Management authorisations are managed in the Relationship Management Portal.	Relationship Management (RMA) Administrator Tasks on page 89

User Role	Description	More information
		Relationship Management (RMA) Operator Tasks on page 90

Related information
[Alliance Cloud Getting Started Checklist](#) on page 15

3 Before you Start with Alliance Cloud

Overview of Alliance Cloud implementation process

There are four main phases in the implementation of Alliance Cloud. Make sure that you are familiar with these phases and that you know who will be responsible for these tasks in your institution. For the complete list of tasks, see the [Alliance Cloud Getting Started Checklist](#) on page 15.

1. **Ordering and provisioning**

2. **Installation and configuration**

Set up your environment, perform all security-related tasks related to Distinguished Names and tokens, and log in to Alliance Cloud. Create roles and users in Alliance Cloud. Create application channels and configure workflows Alliance Cloud. Install and configure your Alliance Cloud connectivity option or options (see [Alliance Cloud Connectivity Options](#) on page 129).

3. **Testing**

Note *This step applies only to migrating customers and not to new Swift customers.*

Request the migration of your Test and Training (T&T) flows from your existing solution to Alliance Cloud.

Test your message flows.

4. **Go live**

Review the training options

Swift offers both tailored training and self-paced e-learning modules on Swift Smart, which is an interactive, cloud-based training service. See [Swift Training](#) on page 106.

Set up your environment

Ensure that your system administrator (or staff responsible for the Swift installation) has completed the actions described in [Set up the Environment for Alliance Cloud](#) on page 92.

Set up your security officers

A security officer manages security matters for one customer (8-character business identifier code [BIC]).

If you are a new Swift customer, then you must set up your online and offline security officers. Your institution must have at least two security officers. Swift registers the first two security officers per customer (8-character BIC) as part of the registration process. Offline security officers are for emergency situations through the Secure Channel application. The two roles can be combined (that is, one security officer can have both the online and the offline role) or separated depending on the security policies of your institution.

For back-up purposes, Swift recommends the creation of two additional online and offline back-up security officers. See [Create Back-up Security Officers](#) on page 39.

Security officer tasks include creating Distinguished Names (DNs), assigning RBAC roles, and recovering and revoking certificates in SwiftNet Online Operations Manager (O2M).

For customers migrating to Alliance Cloud, see also [New Online Security Officer Requirements when Migrating to Alliance Cloud](#) on page 56.

Set up your administrators

Before you start using Alliance Cloud, you must designate two Alliance Cloud administrators. These administrators will create all other users, including the Message management administrators.

Before connecting to Alliance Cloud, these Alliance Cloud administrators must be created and set up for certification in O2M. They must also activate their tokens.

The security officers will create the two Alliance Cloud administrators in O2M and assign them the **admin** RBAC role for the **swift.alliancecloud** and **swift.alliancecloud!p** services.

When the Alliance Cloud administrators log in to Alliance Cloud for the first time, they automatically receive the **Administrator** role in Alliance Cloud.

Set up your Relationship Management Portal administrators and operators

Relationship Management authorisations are managed in the Relationship Management Portal, not in Alliance Cloud.

Your institution's security officers must assign and approve the appropriate [RMA RBAC roles](#) to users in your institution in the SwiftNet Online Operations Manager (O2M).

About your personal certificate

Users require a Swift token with a personal certificate stored on it. This certificate uniquely identifies the user. It enables the user to establish a secure connection to Alliance Cloud and to sign a transaction before Alliance Cloud sends the transaction to the Swift network.

Token software and browser configuration

Personal Token Software and SConnect must be installed on all PCs on which a Swift personal token will be used for Alliance Cloud.

Customers can download the Personal Token Software from the Swift Certificate Centre or the [Download Centre](#). All Swift services and products that use a token require this software.

SConnect is a browser extension that enables applications and websites to communicate with tokens without Java. To connect to an application portal with a token, SConnect installation is required.

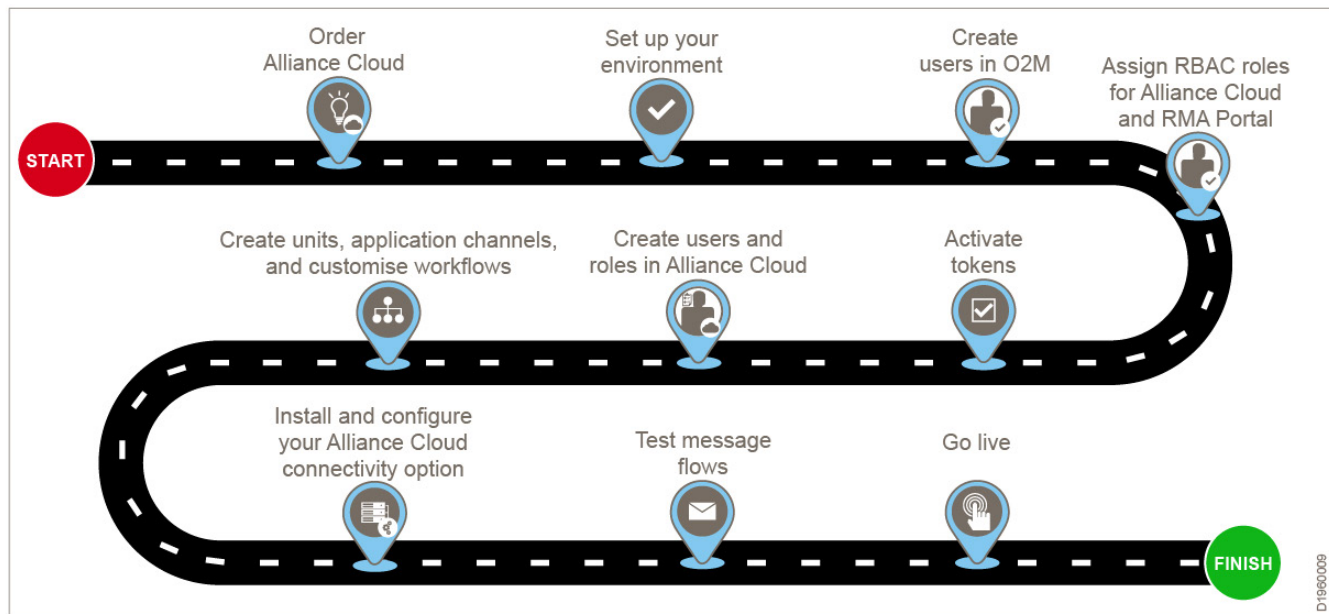
These are one-off procedures that must be completed to have the necessary software to connect, configure, and to read the certificates on personal tokens.

For more information about how to install the software and about qualified web browsers, see [Set up the Environment for Alliance Cloud](#) on page 92.

4 Alliance Cloud Getting Started Roadmap

This topic provides a graphical overview of the tasks involved in setting up Alliance Cloud.

For a complete list of tasks, see the [Alliance Cloud Getting Started Checklist](#) on page 15.



Related information

[Terminology](#) on page 107

5 Alliance Cloud Getting Started Checklist

This topic provides a high-level summary of the tasks involved in setting up Alliance Cloud.

You can print this checklist and go through it step by step to make sure all installation and configuration tasks have been completed.

Customers migrating from another Swift interface must also ensure that all tasks in the [Checklist for Customers Migrating to Alliance Cloud](#) on page 21 (see the next section) have been completed.

Links have been added throughout the document to make it easy for you to jump back to this checklist.

For more information about the training options for Alliance Cloud, see [Swift Training](#) on page 106.

For more information about the terms used in the following table, see [Terminology](#) on page 107.

Checklist tasks

The checklist includes tasks for the following roles:

- [Staff responsible for Alliance Cloud implementation](#) on page 15
- [Your system administrator or staff responsible for the Swift installation](#) on page 16
- [Security officers](#) on page 16
- [System administrator \(for SIL installation\)](#) on page 17
- [SIL administrator \(SIL_Owner\)](#) on page 17
- [System administrator \(for MQ Connector and Swift Microgateway installation\)](#) on page 18
- [MQ Connector administrator](#) on page 18
- [Swift Messaging API developer/API Client administrator](#) on page 18
- [All Alliance Cloud personal token users and the SIL administrator \(for application channels\)](#) on page 18
- [Alliance Cloud administrators: user and role management](#) on page 18
- [Message management administrator](#) on page 19
- [Relationship Management Portal administrator and operator](#) on page 19
- [Staff involved in sending and receiving files and messages](#) on page 19
- [Other considerations](#) on page 20

Staff responsible for Alliance Cloud implementation

✓	Task	Reference information
	Read this first	How does Alliance Cloud Work? on page 9
	You must receive a quotation from your Swift account manager before you can order. You will need the quotation reference to complete the Alliance Cloud order form.	
	Familiarise yourself with the Alliance Cloud implementation process.	Before you Start with Alliance Cloud on page 12
	If you are an existing Swift customer and need an additional BIC for Alliance Cloud, then you must first complete the Request additional connected BIC form before ordering Alliance Cloud.	Ordering on page 24
	Order Alliance Cloud on page 24 For new customers and customers migrating from a Swift interface	
	Speak with a Swift consultant about your connectivity options to use with Alliance Cloud. You may have to order the following: • Alliance Connect for MV-SIPN connectivity (multi-vendor secure IP network)	

✓	Task	Reference information
	A new Swift Local Link (SLL) if you are migrating to a cloud-based solution	
	<i>Optional:</i> order the Alliance Cloud Care Package if you would like to enhance the level of support that you receive from Swift.	
	Note <i>This task applies only to migrating customers and not to new Swift customers.</i> Review your message reception registry (MRR) rules in SwiftNet Online Operations Manager (O2M) with your Swift consultant before going live.	"Routing Rules Management" in the SwiftNet Online Operations Manager User Guide
	<i>Optional:</i> add your BIC to an existing Alliance Cloud set-up.	Add a BIC to Existing Alliance Cloud on page 30
	KYC Security Attestation Your Swift consultant will guide you through this process. It must be completed after you have implemented Alliance Cloud and before you go live.	Security Attestation
	For migrating customers: remove custom delivery subsets. <i>As required:</i> request activation of high throughput and change the delivery subset sharing mode.	Delivery Subset Sharing Mode and Throughput Tasks on page 102
	After completing all tasks in this checklist and having successfully tested in the Test and Training environment, you must request activation on the live environment.	Request Activation on the Live Environment on page 104

Your system administrator or staff responsible for the Swift installation

✓	Task	Reference information
	Read this first	Set up the Environment for Alliance Cloud on page 92
	Review the operating system requirements for Swift Integration Layer. Swift Integration Layer can be installed on Red Hat Enterprise Linux and Windows.	"Operating System Requirements" in the Swift Integration Layer 2.4.0 Release Letter
	Review the qualified browsers for Alliance Cloud.	Web Browser Configuration on page 92
	For MV-SIPN connectivity only: Install and configure DNS server	Knowledge Base article 5018095
	Configure the firewalls.	Configure Firewall Settings on page 93
	Install the Personal Token Software on all PCs on which a Swift personal token will be used for Alliance Cloud (Windows only).	Install Token Software on page 98
	Install SConnect on all PCs on which a Swift personal token will be used for Alliance Cloud.	Get Started with SConnect on swift.com.
	Configure your browser.	Web Browser Configuration on page 92

Security officers

✓	Task	Reference information
	Read this first	Before you Start with Alliance Cloud on page 12
	<i>Migrating customers:</i> verify if you can re-use your security officers	New Online Security Officer Requirements when Migrating to Alliance Cloud on page 56
	<i>New customers:</i> provide the names of two initial security officers during onboarding.	Security Officer Tasks on page 35
	<i>New customers:</i> register security officers on swift.com.	How to become a swift.com user.
	<i>New customers:</i> obtain the secure code card from Swift and activate the card in Secure Channel.	How to get access to Secure Channel?
	<i>New customers:</i> request activation of security officer personal token certificate in Secure Channel.	Secure Channel User Guide > Create Security Requests (with delivery of new secrets)

✓	Task	Reference information
		Important In Secure Channel, make sure that you select the option: Activate initial SO on personal token .
	<i>New customers:</i> activate security officer personal token.	Secure Channel User Guide > Activate a Personal Token
	<i>New customers</i> and other customers as appropriate: order Swift personal tokens.	Order Personal Tokens from Swift on page 38
	In O2M, create a DN for two Alliance Cloud administrators, for each Alliance Cloud user, and for each application channel. Contact the SIL administrator (SIL_Owner) to agree on the DNs for the application channels. Equivalent DNs are needed for the application channels to use the active/stand-by feature for SIL instances.	Create a Distinguished Name (DN) on page 41
	In O2M, for each DN created, set it up for certification	Set Up a User for Certification on page 42
	In O2M, authorise the DN and retrieve the activation secrets. Note The User Name field in O2M must be completed for each DN.	Authorise the DN and Retrieve Activation Secrets on page 44
	In O2M, assign RBAC roles to the two Alliance Cloud administrators, to all Alliance Cloud users, and to all application channels. In O2M, assign RBAC roles to the Relationship Management Portal administrator and operators.	Assign RBAC Roles on page 46
	In O2M, approve RBAC roles.	Approve the Assigned RBAC Roles on page 52
	Make sure that users activate their tokens in the Swift Certificate Centre.	Activate Token on page 53
	You can disable internet access and only connect to Alliance Cloud through the multi-vendor secure IP network (MV-SIPN) connectivity (VPN box).	Internet Access Inclusion/Exclusion (Optional) on page 98

System administrator (for SIL installation)

✓	Task	Reference information
	Read this first	Swift Integration Layer (SIL) Installation and Configuration Tasks on page 66
	Download Swift Integration Layer (SIL) from the Download Centre. You can do so only after receiving an e-mail from Swift that confirms that Alliance Cloud has been provisioned for your institution.	Download Centre
	Check the system requirements and prerequisites.	Swift Integration Layer 2.4.0 Release Letter
	Install Swift Integration Layer on Linux (RHEL) or Windows.	Swift Integration Layer 2.4.0 Release Letter
	Decide whether you will use the active/standby feature for SIL.	Use Active/Standby for SIL Instances on page 78

SIL administrator (SIL_Owner)

✓	Task	Reference information
	Read this first	Swift Integration Layer (SIL) Installation and Configuration Tasks on page 66
	Configure SIL for Alliance Cloud using the SIL GUI and start the application channel(s).	SIL GUI for Alliance Cloud Configuration on page 70 Log in to the SIL GUI on page 71
	If personal tokens are used, then make sure that the certificates have been correctly imported into SIL.	See the Certificates page in the SIL GUI. You can also check using the SIL command line. See List Certificates in SIL in the <i>Swift Integration Layer User Guide</i> .

✓	Task	Reference information
	If you have a problem and need to send configuration and logging information to Swift Support, then use the <code>sil support collectinfo</code> command.	SIL Support Commands on page 77
	If you plan to use the Software Developer Kit (SDK) for the Alliance Cloud API Connector for RESTful APIs, then consult the available documentation.	Alliance Cloud API Connector documentation on the Knowledge Centre

System administrator (for MQ Connector and Swift Microgateway installation)

✓	Task	Reference information
	Read this first	Alliance Cloud MQ Connector Installation and Configuration Tasks on page 82
	Download the latest version of the Alliance Cloud MQ Connector along with its lightweight footprint (Swift Microgateway) from the Download Centre . You can do so only after receiving an e-mail from Swift that confirms that Alliance Cloud has been provisioned for your institution.	Download Centre
	Install the Alliance Cloud MQ Connector and the Swift Microgateway.	MQ Connector Release Letter Swift Microgateway Installation Guide
	Decide whether you will use the active/standby feature.	Use Active/Standby for MQ Connector Instances on page 83

MQ Connector administrator

✓	Task	Reference information
	Read this first	Alliance Cloud MQ Connector Installation and Configuration Tasks on page 82
	Set up the connectivity to the MQ server manually or using CCDT files.	Alliance Cloud Operations Guide
	Assign valid certificates to MQ application channels during its creation.	
	Manage (create, edit, delete) MQ application channels and the subsequent emission and reception destinations.	
	Start and stop the fully configured MQ application channels to enable the flow of messages between back-office applications and Alliance Cloud.	

Swift Messaging API developer/API Client administrator

For more information, see the [Swift Messaging API Getting Started](#).

All Alliance Cloud personal token users and the SIL administrator (for application channels)

✓	Task	Reference information
	Activate token in the Swift Certificate Centre.	Activate Token on page 53

Alliance Cloud administrators: user and role management

✓	Task	Reference information
	Read this first	Alliance Cloud Administrator Tasks: User and Role Management on page 58
	Make sure the prerequisite tasks are completed.	Prerequisites on page 58
	Log in to Alliance Cloud. Only Alliance Cloud administrators can perform the initial login to Alliance Cloud.	https://swift-alliancecloud.browse.swiftnet.sipn.swift.com
	In the Alliance Cloud Admin centre, set up roles and related permissions for Alliance Cloud users.	Online help is available in the Alliance Cloud application after you log in.

✓	Task	Reference information
	In the Alliance Cloud Admin centre, create users and assign them roles. See also Initial Login by Alliance Cloud Users on page 60.	
	In the Alliance Cloud Admin centre, the second Alliance Cloud administrator must log in to approve any newly created users.	

Message management administrator

✓	Task	Reference information
	Read this first	Message Management Administrator Tasks on page 62
	Make sure the prerequisite tasks are completed.	Prerequisites on page 62
	Important The Alliance Cloud administrator must assign the Message management configurator role to you, which gives you the permissions to create, manage, and approve application channels, units, and workflows.	
	Log in to Alliance Cloud.	https://swift-alliancecloud.browse.swiftnet.sipn.swift.com
	Design the connection to the back office with the SIL administrator.	"File and REST Application Channels " in the Alliance Cloud Operations Guide
	In the Alliance Cloud Admin centre, create the application channel. If your institution plans to use the active/standby feature for your Alliance Cloud connectivity option instances, then you must create the application channels using the Common DN used in O2M (ignoring the numbered common name segment, such as %1) . Contact your institution's administrator for your Alliance Cloud connectivity option for more information.	Add an Application Channel in Alliance Cloud on page 64
	In the Alliance Cloud Admin centre, create units.	Online help is available in the Alliance Cloud application after you log in.
	In the Alliance Cloud Admin centre, design and configure the workflows.	

Relationship Management Portal administrator and operator

Relationship Management authorisations are managed in the Relationship Management Portal, not in Alliance Cloud.

✓	Task	Reference information
	Read this first	Relationship Management Portal Tasks on page 89

Staff involved in sending and receiving files and messages

✓	Task	Reference information
	Note <i>This task applies only if you send and receive files using Straight File Processing (STP).</i> Review the File and REST application channel information.	"File and REST Application Channels " in the Alliance Cloud Operations Guide
	Test your message flows	Test your Message Flows on page 100

Other considerations

✓	Task	Reference information
	If FIN is currently hosted on an interface that is not controlled by Swift, then you must ensure that the logical terminal is properly logged out before the migration date, and remains so.	Request Activation on the Live Environment on page 104

Related information

[Alliance Cloud Getting Started Roadmap](#) on page 14

6 Checklist for Customers Migrating to Alliance Cloud

This checklist is for customers who are migrating from another Swift interface, such as Alliance Access or Alliance Lite2.

All tasks must be completed before the allowable downtime window of the migration weekend.

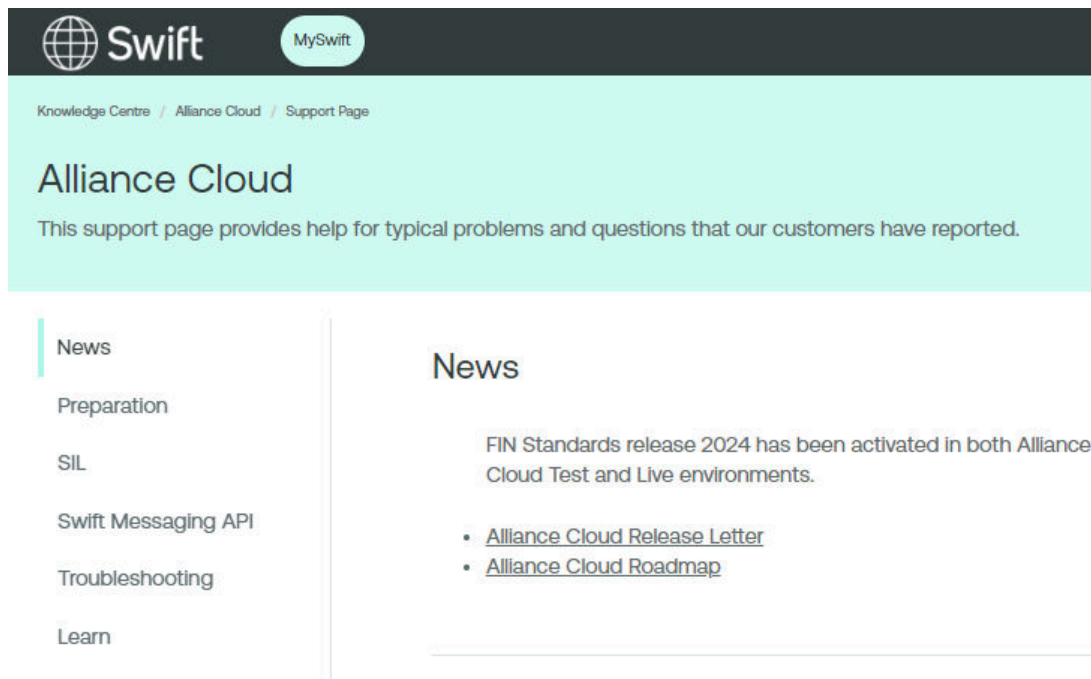
Interface	Time frame	Task
All	At the start of the project kick-off meeting	Follow the instructions in the Alliance Cloud Getting Started Checklist on page 15. Ignore tasks that are marked for new customers.
All		Identify your offline security officers See also New Online Security Officer Requirements when Migrating to Alliance Cloud on page 56.
All	Before the migration weekend	Make sure that the offline security officers with the access to Secure Channel and secure code cards are available on the first day of testing after the migration. See also Secure Channel User Guide .
Alliance Access / Alliance Entry	Before the migration weekend	- Check the allowable downtime window (ADW) of Alliance Cloud especially the end of the ADW (05.00 AM GMT on Sunday). See Swift Service Alert. - Log out of logical terminals at the end of the last business day before migration. If you want to keep your logical terminals connected until the start of the Alliance Cloud maintenance, then check the maintenance windows (see Swift Service Alert). - Keep your reception profiles open through the weekend to collect traffic, which may arrive between the last business day in Alliance Access and the first business day in Alliance Cloud. - Maintain the Gateway connectivity throughout the migration weekend. - Disable automatic login/select of FIN logical terminals. - Disable the emission profile(s) of the migrated services. - If you need help with retrieving messages, then contact Swift Support. For more information about these tasks, see the Alliance Access Configuration Guide .
	Directly after ADW of switch over to Alliance Cloud	- Connect your back office to Alliance Access to consume messages received before the switchover to Alliance Cloud. - Make sure that the emission profiles are disabled for the migrated services. - Disable reception profiles for the migrated service(s).
	As from 7 days after completing the migration	- Deactivate reception profiles (emission profiles must be already deactivated). - Disable the Gateway connectivity. - Disable the logical terminal. - Disable all Alliance Access operators. - Terminate the Alliance Access licence on swift.com. <i>Screening Services:</i> Handle all message alerts on Transaction Screening and Payment Controls before the end of the business day.
Alliance Lite2	Before migration weekend	- Make sure there are no messages that require manual intervention and finish the processing before migration. - Finish all message processing for services that will migrate or all services depending on your migration setup. - Do not disconnect AutoClient.
	Directly after migration weekend	- Check the GUI for any messages possibly received in the time frame after the end of the business day and before the switch to Alliance Cloud. - Check for the new messages coming from AutoClient after the weekend of migration to collect messages from legacy queues. Messages received between the end of the last business day before migration and connecting to Alliance Cloud.
PKI	As from 7 days after finishing the migration	- Revoke and delete Business and Lite certificates with the following policy IDs: 1.3.21.6.2 (business certificate stored on HSM) 1.3.21.6.3.10.200.5 (personal HSM certificate) 1.3.21.6.6.10.100.1 (lite certificate stored on HSM)

Interface	Time frame	Task
Does not apply to Alliance Lite2 customers		See the SwiftNet PKI Certificate Administration Guide. - Make sure that only personal token and channel certificates are present in SwiftNet Online Operations Manager (O2M) - Choose your security officer setting: 4-eyes or 2-eyes.
Alliance Gateway/SwiftNet Link	Before the migration weekend	Do not disable the connectivity between messaging applications and SwiftNet/FIN services to ensure the continuity of the message/file reception.
	As from 7 days after finishing the migration	- Terminate the SNL licence and each respective connectivity pack on swift.com. - Revoke SwiftNet certificates. - Disable virtual SwiftNet users. - Disable routing endpoints. - Disable message partners. - De-register HSM boxes from SwiftNet Link. - Terminate the / licence on swift.com. See also the Alliance Gateway Administration and Operations Guide and the Hardware Security Module Box SA7 - Operations Guide
Alliance Web Platform Server-Embedded	One week after the migration	- Disable the Alliance Web Platform admin users. - Stop Alliance Web Platform services on Alliance Web Platform servers See the Alliance Web Platform Server-Embedded Administration and Operations Guide.
Value-added services For customers that use Transaction Screening and Payment Controls	One week after the migration	Check for the open alerts (Transaction Screening and Payment Controls) All messages alerted by the screening services will be delivered in the legacy queues. The legacy queues are not acquired by Alliance Cloud. See the Payment Controls User Guide and the Transaction Screening User Guide.

7 Alliance Cloud Support Page

The Alliance Cloud Support page includes useful links to important Alliance Cloud news and resources.

We recommend that you bookmark this page for easy access.



The screenshot shows the Alliance Cloud Support Page. At the top, there is a dark header with the Swift logo and a 'MySwift' button. Below the header, a light blue banner contains the text 'Alliance Cloud' and a description: 'This support page provides help for typical problems and questions that our customers have reported.' To the left of the main content is a sidebar with a list of links: 'News', 'Preparation', 'SIL', 'Swift Messaging API', 'Troubleshooting', and 'Learn'. The 'News' link is highlighted with a blue bar. The main content area, titled 'News', contains a paragraph stating 'FIN Standards release 2024 has been activated in both Alliance Cloud Test and Live environments.' followed by two bullet points: 'Alliance Cloud Release Letter' and 'Alliance Cloud Roadmap', both of which are underlined links.

Swift MySwift

Knowledge Centre / Alliance Cloud / Support Page

Alliance Cloud

This support page provides help for typical problems and questions that our customers have reported.

- News
- Preparation
- SIL
- Swift Messaging API
- Troubleshooting
- Learn

News

FIN Standards release 2024 has been activated in both Alliance Cloud Test and Live environments.

- [Alliance Cloud Release Letter](#)
- [Alliance Cloud Roadmap](#)

8 Ordering

This section describes the ordering activities for new Alliance Cloud customers and customers who are migrating to Alliance Cloud from another Swift interface.

	For new customers	For migrating customers
Order Alliance Cloud on page 24	✓ Mandatory	✓ Mandatory
Order messaging services <u>other than</u> FIN, FINplus, and FileAct on swift.com > Ordering . You can order the FIN, FINplus, and FileAct services using the Alliance Cloud order form mentioned above.	✓ Optional - as needed	n/a
Request an Additional Connected BIC on page 29	✓ Optional - You can do this after becoming a Swift customer.	✓ Optional
Add a BIC to Existing Alliance Cloud on page 30	✓ Optional	✓ Optional
Central Activation of FIN for New BICs on page 31	✓ Mandatory if you have <u>not</u> requested Swift Professional Services to help you with the implementation of Alliance Cloud	n/a
Migrate your SwiftNet Services to Alliance Cloud on page 32	n/a	✓ Mandatory if you use SwiftNet
Migrate your FIN Services to Alliance Cloud on page 33	n/a	✓ Mandatory if you use FIN

Simplified migration for Alliance Lite2 customers

Alliance Lite2 customers can benefit from a simplified migration to Alliance Cloud using a specific order form that is not available publicly on swift.com. During this simplified migration, users, roles, and message templates are transferred to Alliance Cloud. Before using this specific order form, an assessment is needed. Contact your account manager if you want to migrate your Alliance Lite2 BIC using this simplified migration.

If you have already ordered the migration of your Alliance Lite2 BIC through the Alliance Cloud e-order described in this guide, then you cannot change the order to a simplified migration.

8.1 Order Alliance Cloud

New Alliance Cloud customers and customers migrating from a Swift interface use the same order form to order Alliance Cloud.

This task must be completed by a user with a swift.com account that has ordering privileges.

While completing this form, you can also order the MQ Connector and the File Connector (optional). Certain steps apply only to new customers, such as ordering the FIN, FINplus, and FileAct messaging services.

Before you begin

Read the following information before you order Alliance Cloud:

1. **Quotation reference**
You must receive a quotation from your Swift account manager before you can order Alliance Cloud. You must add the quotation reference to the order.
2. **Invoicing**
For more information about pricing, contact your Swift account manager.
Only the **ordering** BIC is invoiced for Alliance Cloud
The invoice will cover all BICs in the new set-up.
Additional BICs are charged at a fixed rate.
The billing plan start date is different for new or existing Swift customers. For more information, see [Ordering, Invoicing, and Payment](#).
3. **Personal tokens**
You can choose to not receive personal tokens. You will not receive a discount if you do so. If you decide to order personal tokens later, then you will need to pay for them.

Procedure

1. Log in to the Alliance Cloud self-service ordering [portal](#) and start to order Alliance Cloud.

Note

You can save the order at any step and submit it later.

Swift | MySwift

ALLIANCE CLOUD CONFIGURATION PORTAL

Welcome to the Alliance Cloud Configuration Portal

What would you like to do today?

Order Alliance Cloud

Start ordering your brand new environment today.

Order Alliance Cloud

Overview of configuration requests

The section below presents the overview of your existing configuration requests. Use links in Action column to manage your requests.

Request ID	Requesting BIC	Impacted BIC(s)	Request Type	Requested on	Requested by
------------	----------------	-----------------	--------------	--------------	--------------

2. Enter the required information.
- a. **The BIC ordering Alliance Cloud:** For this step you must have the Swift commercial quotation reference.
- b. Confirm the connectivity details.

If you are ordering Alliance Cloud as a direct customer, then select **No**.
If you are joining Alliance Cloud through a Business Connect Provider, then see also the documentation on the [Knowledge Centre](#).

Swift | MySwift

Registered Customer Information

Confirm your identity and the BIC ordering Alliance Cloud. Check your contact details. If you need to change any information, click here: <https://www2.swift.com/idm/>

Entity Full Legal Name

BIC8

Registered User Name

Registered Email Address

Registered Telephone Number

Ordering references

Select the Primary BIC ordering Alliance Cloud subscription.

Ordering BIC ? *

Your own Purchase Order Reference ?

Swift Commercial Quotation Reference ? *

Connectivity Details

BIC to be connected through Business Connect Provider? ?

☐ Yes

☒ No

Cancel Order

Save

Next >>

3. You will be prompted to select additional BICs from your institution’s traffic aggregation hierarchy that will be part of the same Alliance Cloud business entity. The ordering BIC is the name of the business entity. As per the quotation, if the BIC is not in the Swift commercial quotation, then the order will not be successful.

For more information about business entities, see [Terminology](#) on page 107.

Swift | MySwift

Alliance Cloud Ordering

CO-10017

1

2

3

4

5

Order Reference

BIC Configuration

Option(s)

Security & Shipping

Order Summary

Select additional BICs that will use Alliance Cloud

Subscribing BICs

1 Business Identifier Code (BIC)

Add BIC

Cancel Order

<< Back

Save

Next >>

4. *Optional* - Add the Alliance Cloud MQ Connector or the File Connector option (or both). You can also order these options at a later stage using a separate order form: **Add or Remove Connector to/from Alliance Cloud** on the [Alliance Cloud ordering page](#).

Alliance Cloud Ordering

Add Options
Please select options that you would like to add to your Alliance Cloud instance.

Order Reference BIC Configuration **Option(s)** Security & Shipping Order Summary

Options
Please select options that you would like to add to your Alliance Cloud subscription.

Alliance Cloud MQ Connector
The Alliance Cloud MQ Connector enables Swift messages to be exchanged between Alliance Cloud and customer's back-office applications using IBM MQ technology. Please select this option only if it's part of the quotation shared by Swift, otherwise the order might be rejected.

Add MQ Connector +

Alliance Cloud File Connector
The Alliance Cloud File Connector allows Swift messages to be exchanged between Alliance Cloud and customer's back-office applications using a file-based connectivity method. Please select this option only if it is included in the quotation provided by Swift, otherwise, the order may be rejected.

Add File Connector +

Cancel Order Back Save Continue

5. *For new customers only:* select the appropriate messaging service. You can select FIN, FileAct, both services, or none of the two.

If you select FIN, then the subscription also includes the FINplus service.

If you need other services, then you must order them on swift.com > [Ordering](#).

Alliance Cloud Ordering
CO-10017

Order Reference BIC Configuration Option(s) **Service Configuration** Security & Shipping Order Summary

Add FIN or FileAct services

Include subscription to SWIFT messaging services for [redacted] does not currently subscribe to Swift messaging services FIN and FileAct. You can include the subscription to these Swift messaging services in this order form.

The Pilot ("test & training") version of the selected service(s) will be provisioned immediately, while the Live version will be provisioned only when the initial setup is completed and confirmed to be functional.

☐ FIN ⓘ
☒ FileAct ⓘ

The first subscription to Swift messaging services automatically includes a subscription to SwiftNet PKI.

For more information about the FIN and SwiftNet messaging services or [SwiftNet PKI](#), see the related service description and other documentation in the [User Handbook Online](#).

The provision and use of the FIN and SwiftNet messaging services and SwiftNet PKI are governed by the [Swift General Terms and Conditions](#).

Cancel Order << Back Save Next >>

6. If you do not want to receive personal tokens, then select the check box and click **Next**. If you want to order the tokens, then select an offline security officer (defined in swift.com) for shipment of the personal tokens.

An offline security officer has access to offline tools only, such as Secure Channel and the swift.com user administration tool: Identity Management.

The address used on this page will not be saved in your swift.com account. It will be used only for the token shipment.

Important You must have at least one active offline security officer before continuing. If none of the security officers in the drop-down list are suitable for this step, then when you select *None of the above*, the portal prompts you to register a new security officer in [Secure Channel](#). See the [Secure Channel User Guide](#).

Swift | MySwift

Alliance Cloud Ordering

CO-10017

1

Order Reference

2

BIC Configuration

3

Option(s)

4

Service Configuration

5

Security & Shipping

6

Order Summary

Identify a security officer

☐ I do not want to receive Swift personal tokens

Please select the checkbox if you wish to skip token shipment

Customer Security Officers

Select the Security Officer to receive the initial token passwords (PIN)

Select the Security Officer *

Shipping address

Provide the shipping address for the tokens.

Title *

▼

First Name *

Last Name *

Email *

Intl. Code *

Phone Number *

Legal Entity Name *

Building Name

Street name 1 *

Street name 2

Street Number

Postal Code

Country *

State / Region / Province

City *

VAT *

BE

BRUXELLES

I am exempted from Value Added Tax (VAT) for European Union(EU) customers only ▼

For European Union (EU) customers only: Swift will apply the Value Added Tax (VAT) exemption as from the moment you provide us with the supporting documentation to evidence the EU VAT exemption.

No credit notes will be made for invoices prior to your VAT exemption confirmation in our systems.

Cancel Order

<< Back

Save

Next >>

7. Review the order summary. If all of the information is correct, then click Finish and Submit.
- An order summary will be sent to your email address.
8. After the order is submitted, the information is visible on the initial Alliance Cloud ordering page under **Overview of configuration requests** with the status *Pending Validation*. If the order status is set to **New**, then this means the order has not been submitted.

Overview of configuration requests

The section below presents the overview of your existing configuration requests. Use links in Action column to manage your requests.

Request ID	Requesting BIC	Impacted BIC(s)	Request Type	Requested on	Requested by	Requested for	Scheduled for	Status	Action
No items									

- You will receive an e-mail notification after Swift validates and processes the order.
9. Swift Professional Services will contact you to assist with the implementation process to connect to Alliance Cloud and to discuss connectivity options.

Connectivity options

You may have to order the following:

- If you intend to use MV-SIPN (multi-vendor secure IP network), and you will not reuse your existing MV-SIPN connectivity, then you must order Alliance Connect (for Alliance Cloud).
You will need some technical information from your IT department to complete the order form.

Upon request, Swift can force your user and SIL traffic through your MV-SIPN connectivity thus preventing access through the Internet. See Knowledge Base article [5026197](#).

For more information about Alliance Connect, visit swift.com.

- If you intend to use MV-SIPN with a Public Cloud deployment, then you must order Alliance Connect Virtual. For more information about Alliance Connect Virtual, visit swift.com.
- Order Swift Local Link (SLL). Complete this form if you already have an Alliance Connect subscription.
An SLL enables traffic between a multi-vendor secure IP network and a host, identified by an IP address.
- If you intend to use internet connectivity (that is, no MV-SIPN), then no specific connectivity ordering is required. In this case, only certificates or tokens can be used with Swift Integration Layer.
- If you plan to use the Connectivity Pack of another BIC in your traffic hierarchy, see also Knowledge Base article [6000292](#) - **Channel service subscription order form**.

What to do next

- **Care Alliance Cloud**

After the Alliance Cloud ordering process is completed, you can optionally complete a separate order form for the Alliance Cloud Care Package. This package offers an enhanced level of support from Swift. Care Alliance Cloud is charged for all BICs in the same set-up. For more information, see "Service Packages" in the Swift Care Services Service Description.

- **Optional - request an additional BIC**

If you want to add another BIC after you have ordered Alliance Cloud, then see Request an Additional Connected BIC on page 29.

8.2 Request an Additional Connected BIC

This topic explains how as an existing Swift customer, you can register an additional, connected BIC for your institution to subscribe to Alliance Cloud.

The additional BIC will be part of your legal entity. The BIC that you will receive will have the same first six characters as your primary BIC.

Before you begin

Before requesting an additional connected BIC for an existing Alliance Cloud group, the Alliance Cloud group (business entity) must be created. It will be created between one and two weeks after you order Alliance Cloud for your main BIC.

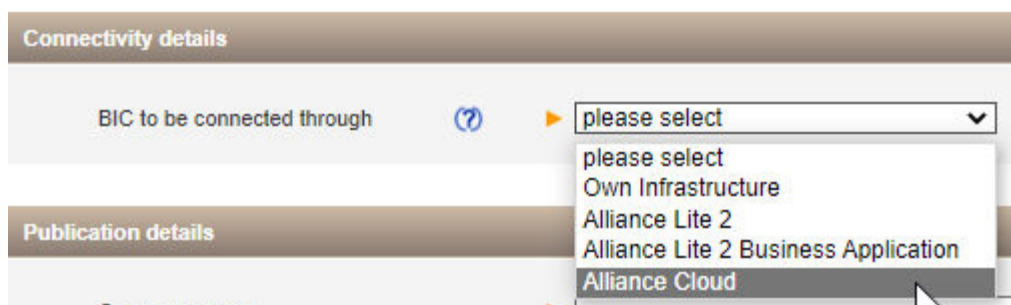
Procedure

1. Ask your Swift account manager for a quotation.

If the BIC will be hosted by an existing Alliance Cloud, then the recurring charges for hosting the new BIC (and Care Alliance Cloud, if relevant) will be invoiced to the owner of the selected Alliance Cloud group. The new BIC will benefit from all entitlements for the BICs hosted on Alliance Cloud: fees for BIC registration, PKI management, SwiftSmart, the User Handbook, and so on.

If the owner of the Alliance Cloud group is another customer, then that customer needs a separate quotation.

2. Go to the **Order a Business Identifier Code (BIC)** page on swift.com. Scroll down to the section **Additional BIC (8-char)**. Complete the **Request additional connected BIC** form.
3. In the **Connectivity details** section, select **Alliance Cloud**.



The system checks whether the new BIC can be added to an existing Alliance Cloud, or whether a new Alliance Cloud must be ordered.

4. After the BIC is created, Swift will inform you about the next step by e-mail based on your ordering scenario:
 - order a new Alliance Cloud
 - or**
 - ask the selected Alliance Cloud owner to add your BIC to their existing Alliance Cloud set-up.

What to do next

[Add a BIC to Existing Alliance Cloud](#) on page 30

8.3 Add a BIC to Existing Alliance Cloud

For new BICs and BICs migrating to Alliance Cloud

You can add a BIC to an existing Alliance Cloud set-up (that is an Alliance Cloud business entity) using the procedure explained in this topic.

The default roles are configured with permissions that apply to all of the BICs in the customer's set-up, including the BICs that are added later. Users can further define custom roles limiting the access to one or multiple BICs.

If you have custom roles with permissions based on BICs, then you must either update these roles to include the newly added BIC or create new roles with permissions based on this newly added BIC.

Before you begin

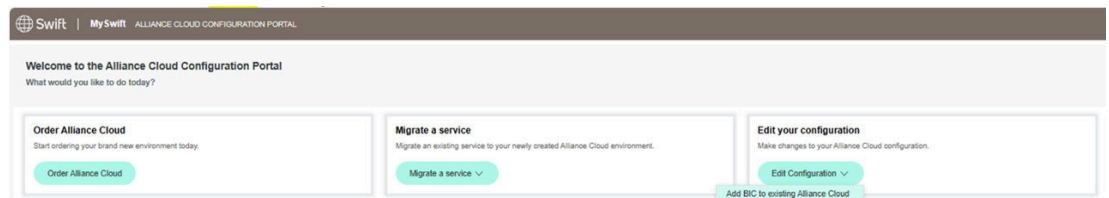
The Alliance Cloud set-up must be owned by your institution or by a member of your own traffic hierarchy. Traffic hierarchy means that Swift users are part of the same corporate group registered for the purposes of Swift traffic aggregation. For more information, see **5. Report a change in Traffic Aggregation Hierarchy** on swift.com > [Change your Legal or Publication information..](#)

You also need a valid security officer to whom Swift will send the personal tokens and the initial password.

For new BICs, you must first order as explained in [Request an Additional Connected BIC](#) on page 29.

Procedure

1. Ask your Swift account manager for a quotation. The quotation will be shared with the owner of the Alliance Cloud set-up that you want to join.
2. The owner of the Alliance Cloud set-up that you want to join must submit a request to change their Alliance Cloud and add your BIC. To do so, log in to the Alliance Cloud self-service ordering [portal](#).
3. Click [Edit configuration](#) > [Add BIC to existing Alliance Cloud](#).



4. Select one BIC from the list of all BICs that could be added. You then identify the security officer responsible for the implementation and the shipping address for the tokens.

The list of BICs includes BICs that could join an existing Alliance Cloud. They must be part of the same traffic aggregation hierarchy, and must not already be on Alliance Cloud.
5. *For new BICs only:* select the appropriate messaging service. You can select FIN, FileAct, both services, or none of the two.

If you select FIN, then the subscription also includes the FINplus service.
If you need other services, then you must order them on [swift.com](#) > [Ordering](#).
6. The person who places the order will receive an e-mail confirming that Swift has acknowledged the request. Swift will then validate the order. After the order is successfully validated, you will be informed by e-mail.

8.4 Central Activation of FIN for New BICs

For new Alliance Cloud customers (not a migration of an existing BIC)

If you have not requested Swift Professional Services to help you with the implementation of Alliance Cloud, then you must inform Swift's joining team by email that you have performed the mandatory onboarding steps described in this topic.

Note *If you have opted for the assistance of Swift Professional Services, then the central activation request of FIN will be handled by your consultant.*

You must have performed the following steps already:

1. You ordered a new BIC that will use FIN and received the confirmation from Swift (joining.generic@swift.com) that this FIN BIC has been provisioned on the network
2. You ordered an additional BIC on Alliance Cloud and received confirmation that the BIC is activated on Alliance Cloud in the Test and the Live Environments.

After the two previous steps, your FIN traffic is still not centrally activated although the FIN LT is already active on Alliance Cloud.

You must now confirm the following to Swift by email (joining.generic@swift.com) to request the central activation of FIN.

1. You performed thorough testing for BIC <XXXXXXXX> on the Alliance Cloud Test environment, and you are ready to activate the FIN traffic on the Live network.

2. You have no outstanding invoices.
3. You understand the Swift [Customer Security Programme \(CSP\)](#) and performed the [KYC Security Attestation](#).
4. FIN activation expected <Date>
The deadline is on a Tuesday end of day. The activation date must be no later than five days before a Swift maintenance window. See the [Swift Service Alert page](#).

To complete your security attestation, please access the online tool [KYC Security Attestation \(KYC-SA\) application](#).

After Swift receives this email, the joining team will make some final checks and activate your FIN traffic centrally on the network at the date you select or the closest date possible. You will receive the confirmation of the central activation date of FIN for your new BIC.

8.5 Migrate your SwiftNet Services to Alliance Cloud

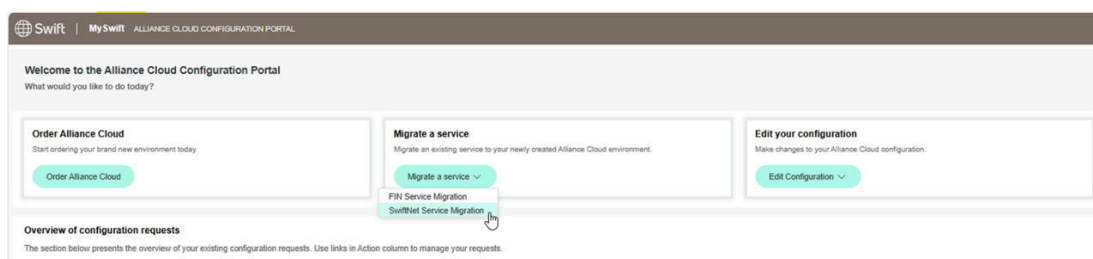
This topic describes how to migrate your SwiftNet services if you are migrating to Alliance Cloud from another messaging interface.

Before you begin

You must have ordering privileges for the main Alliance Cloud BIC for which SwiftNet services are being migrated.

Procedure

1. Log in to the Alliance Cloud self-service ordering [portal](#) and select [SwiftNet Service Migration](#).
You can save the order at any step and submit it later.

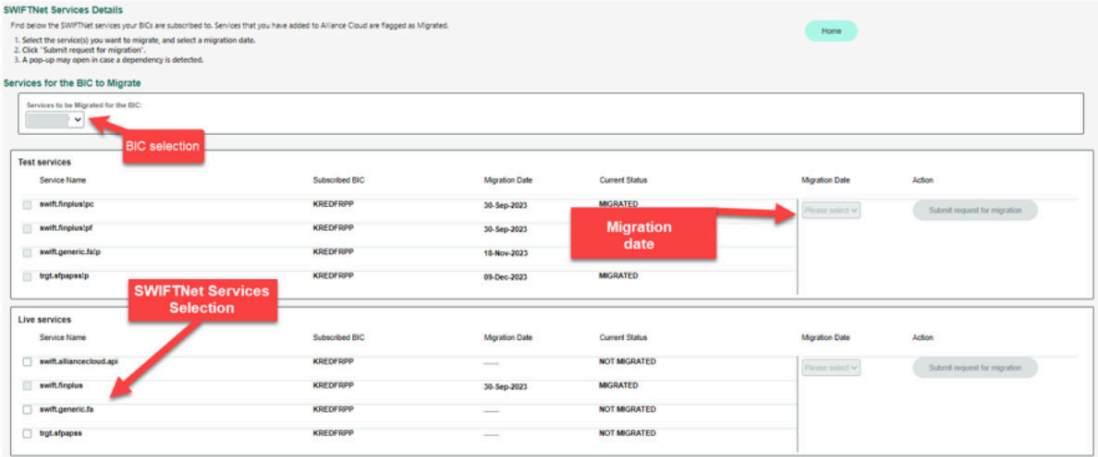


2. Select the BIC, the SwiftNet services to be migrated, and a migration date. After the request is submitted, you will receive a *Migration requested* e-mail notification that summarises the request.

After Swift validates and processes the request, you will receive a *Migration completed* e-mail notification with a summary of the migrated service or services.

Note You can migrate one or more services at the same time.

Note If you migrate from Alliance Lite2, then the migration dates are limited to the Alliance Lite2 provisioning dates. For more information, contact your Swift Consultant.



8.6 Migrate your FIN Services to Alliance Cloud

This topic describes how to migrate your FIN services if you are migrating from another messaging interface to Alliance Cloud.

Swift recommends that you migrate FINplus together with FIN. You can also migrate FINplus first and migrate FIN at a later stage. You cannot migrate FIN before FINplus.

Important Alliance Cloud supports default FIN delivery subsets (SYSTEM, URGENT, NORMAL). If you use customised delivery subsets, then you must reset them to the default value by sending a system message (MT 047). For more information, see [Plan Volume and Throughput Tests for Alliance Cloud](#) on page 101 and Knowledge Base article [5018976 Activation of MT047 \(FIN Delivery Subset Redefinition Request\)](#).

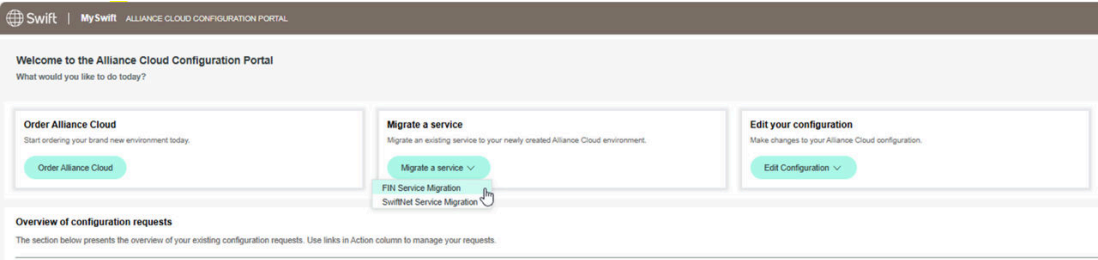
Before you begin

You must have ordering privileges for the main Alliance Cloud BIC for which FIN service(s) are being migrated.

Procedure

1. Log in to the Alliance Cloud self-service ordering [portal](#) and select [FIN Service Migration](#).

Note You must wait on average 15 minutes after the SwiftNet services migration e-order has been submitted before you can proceed with the FIN service migration.



2. Select the BIC, the FIN services to be migrated, and the migration date. After the request is submitted, you will receive a *Migration requested* e-mail notification that summarises the request.

After Swift validates and processes the request, you will receive a *Migration completed* e-mail notification with a summary of the migrated FIN service or services.

FIN Service Migration

Find below the FIN service your BICs are subscribed to.

1. Select FIN Test or FIN Live service you want to migrate and the date of the migration.
2. Click "Dependencies" to validate your choice. This will open a pop-up window with the identified dependencies (if any).
3. When the dependencies are resolved, the button "Submit" will get enabled. Click it to finalize your request.

FIN Service details

BIC	Test BIC	Test Migration Date	FIN Test Migration status	Live Migration Date	FIN Live Migration status	Migration Dependency	Action
		30-Sep-2023	MIGRATED	30-Sep-2023	MIGRATION IN PROGRESS	Dependency	

Swift recommends that you migrate FINplus together with FIN. You can also migrate FINplus first and migrate FIN at a later stage. You cannot migrate FIN before FINplus.

Note *If you migrate from Alliance Lite2, then the migration dates are limited to the Alliance Lite2 provisioning dates. For more information, contact your Swift Consultant.*

WARNING

IMPORTANT MESSAGE
FIN Plus must be migrated together with FIN.

When migrating **swift.finplus**, please make sure that FIN is also migrated on the same date.

When migrating **swift.finplus!pc** or **swift.finplus!pf**, please make sure that both **swift.finplus!pc** and **swift.finplus!pf** are migrated together, and that TFIN is also migrated on the same date.

The requests to migrate FIN and/or TFIN must be submitted on a different screen, accessible through the Alliance Cloud portal.

☐ I understand the risk, and will schedule FIN service migration accordingly

Cancel Submit

Important

- If you are migrating FIN from Alliance Lite2, when requesting TFIN (or FIN) migration, the portal will ask you to ensure that all Pilot (or Live) SwiftNet services are migrated at the latest by the same date.
- If you are migrating from a non-Cloud interface (that is, not Alliance Lite2), when requesting TFIN (or FIN) migration, the portal will remind you to take all steps to disconnect the logical terminal from your current interface shortly before your migration date.

Warning If you do not disconnect the logical terminal from your current interface before the migration date, after the maintenance window your FIN traffic will be balanced between Alliance Cloud and your previous interface. The FIN logical terminal will be unstable, and you run the risk of messages being received on Alliance Cloud after they have been received on your previous interface.

9 Security Officer Tasks

Alliance Cloud security officers do the initial set-up required for Swift personal tokens, application channels, and channel certificates (if applicable). This includes creating Distinguished Names (DNs) and assigning RBAC roles in SwiftNet Online Operations Manager (O2M).

Your institution must have at least two security officers (SO).

☒ Click [here](#) to go to the Getting Started checklist.

For migrating Swift customers

For Alliance Lite2, Alliance Access and Alliance Remote Gateway customers, and Service Bureaux, see [New Online Security Officer Requirements when Migrating to Alliance Cloud](#) on page 56.

For new Swift customers

1. Customers will provide the names of the two initial security officers to Swift during the onboarding process. In the e-form, the customer will provide the Distinguished Names (DNs) of the two security officers certificates.
The recommended DN naming convention for Alliance Cloud security officers is as follows:
`cn=so<N>, o=<BIC8>, o=swift`
where <N> is a positive integer.
Example
`cn=so1, o=bankbebb, o=swift`
2. Register the two offline security officers on swift.com. For more information, see [How to become a swift.com user](#).
3. Obtain the secure code card from Swift and [activate](#) the card on Secure Channel.
As part of the registration process, two security officers are defined and will receive their secure code card from Swift.
Security officers require a secure code card to perform security requests and maintenance tasks within the Secure Channel application. One secure code card is required for each security officer per BIC.
For more information, see [How to get access to Secure Channel?](#)
4. The two initial security officers must request activation of their personal token certificates and create a download password. See the *Secure Channel User Guide* > [Create Security Requests \(with delivery of new secrets\)](#).

Important In Secure Channel, make sure that you select the option: **Activate initial SO on personal token**.

The security officers receive an e-mail from Secure Channel. The e-mail contains links to the Swift Certificate Centre.

5. The two security officers must activate their token on the Swift Certificate Centre. See the *Secure Channel User Guide* > [Activate a Personal Token](#).
To complete this procedure, each security officer needs their token, the initial token password, along with the **Secure Channel Request ID** and **Download Password** from step 4 on page 35

Note *The Alliance Cloud subscription includes a set of tokens (one set for each BIC on Alliance Cloud).*
When you order tokens, they are sent to the first security officer. The second security officer receives the initial token password by e-mail.
The security officer can also order additional tokens. See step 6 on page 37.

Access to functionality for 4-Eyes Authorisations

During customer implementation, Swift assigns initial security officers the RBAC roles SWIFT.LRA//CertificateAdministration4eyes and SWIFT.RBAC//Delegator4eyes. The 4-eyes authorisation scheme requires the participation of two separate security officers to perform certain tasks.

If you have the standard SWIFT.LRA//CertificateAdministration or SWIFT.RBAC//Delegator roles, then you must ungrant them. If you do not do that, then the standard roles take precedence over the 4-eyes roles.

If a security officer with 4-eyes roles initiated the requests, then the standard roles are sufficient to authorise the requests.

Security officer tasks

1. The first security officer creates a Distinguished Name (DN) for the Alliance Cloud administrators (at least two are required) and for each Alliance Cloud user in *SwiftNet Online Operations Manager (O2M)*. See [Create a Distinguished Name \(DN\)](#) on page 41.
2. The first security officer [Set Up a User for Certification](#) on page 42.
3. Assign the RBAC roles as follows. See [Assign RBAC Roles](#) on page 46. See also [RBAC roles for Migrating Alliance Access Customers](#) on page 51.

You must also assign the appropriate RBAC roles to staff who will manage authorisations in the Relationship Management Portal. For more information, see [Role-Based Access Control Requirements](#) in the [Relationship Management Portal Getting Started](#).

In O2M, the security officers must grant the **admin** or **user** role to each user's DN under the **swift.alliancecloud** service and/or the **swift.alliancecloud!p** Test and Training (T&T) service.

RBAC role	Who to assign role to
admin	Alliance Cloud administrator If you will be an Alliance Cloud administrator as well as security officer (cumulative role), then you can assign this admin RBAC role to yourself.
user	All Alliance Cloud users To perform tasks, Alliance Cloud users must have the appropriate RBAC role assigned by the first security officer. This creates the four-eyes code.

4. Give the two sets of four-eyes code for each DN to the second security officer: one 4-eyes code for the creation of the DN and one four-eyes code for the RBAC roles.
5. The second security officer must do the following:
 - Authorise the DN.
 - Make sure that **User Name** field in O2M is filled in for each DN.
 - Copy the activation secrets and pass them securely to each personal token user along with the token and the initial personal token password.
 - Approve the RBAC roles.

The second security officer must perform the four-eyes authorisation of the action before midnight GMT of the next calendar day.

See [Authorise the DN and Retrieve Activation Secrets](#) on page 44 and [Approve the Assigned RBAC Roles](#) on page 52.

6. Ensure that the users activate their own tokens.
7. [Internet Access Inclusion/Exclusion \(Optional\)](#) on page 98

Note *Order personal tokens from Swift if needed.*

You will receive a box of 10 tokens. You can order more tokens if needed. Plan also for sufficient spare tokens in case of replacement. To do this, liaise with the Alliance Cloud administrator to know how many tokens to order. See [Order Personal Tokens from Swift](#) on page 38.

*Swift will send the initial token password by **e-mail** to the address in the order form.*

Application channel-related tasks

Application channels are the link between any of the Alliance Cloud connectivity options and Alliance Cloud. They must be defined in both environments, but are not needed if you do not connect your back-office applications to Alliance Cloud.

One SIL or one Alliance Cloud Connectors instance can have different applications channels to connect to multiple back offices.

Application channels require either a token certificate or a channel certificate. Channel certificates are only available to integrate with the back-office over MV-SIPN (multi-vendor secure IP network). For more information, see "Application Channels" in the [Alliance Cloud Operations Guide](#).

1. In the SwiftNet Online Operations Manager (O2M), create a DN for each application channel. If you connect through MV-SIPN using a channel certificate, then you select the **Channel** option in O2M. If you connect using a personal token (over the Internet or through MV-SIPN), then you create an application channel using the **Personal token** option in O2M. If your institution plans to use the active/standby feature for SIL or Alliance Cloud Connectors instances, then the application channels must be created using equivalent DNs. Contact your institution's Alliance Cloud connectivity option administrator to confirm how many DNs are needed and if equivalent DNs should be defined. See [Create a Distinguished Name \(DN\)](#) on page 41.
2. [Set Up a User for Certification](#) on page 42
For application channels that use Swift personal tokens, make sure that **User Name** field in O2M is filled in for each DN.
3. Give the DNs created for each application channel to both the Alliance Cloud connectivity option administrator and the Message management administrator.
4. *For personal tokens:* copy the activation secrets and pass them securely to the Alliance Cloud connectivity option administrator, along with the token and the initial token password.
5. *For channel certificates:* copy the activation secrets (reference number and authorisation code) and pass them to the Alliance Cloud connectivity option administrator. The Alliance Cloud connectivity option administrator needs the secrets to download the channel certificate into the appropriate Alliance Cloud connectivity option, Swift Integration Layer, the Alliance Cloud Connectors, or the Swift Messaging API-related API client.
6. [Authorise the DN and Retrieve Activation Secrets](#) on page 44.
7. [Assign RBAC Roles](#) on page 46.
For application channel certificates, you must assign the **access_to_service** RBAC role which is under the **swift.alliancecloud.sil** service for Live and under **swift.alliancecloud.sillp** for T&T. This applies to application channels connecting with a token and a channel (disk) certificate.

For the Swift Messaging API, you must assign the **Alliance Cloud API Live** and **Alliance Cloud API Test** RBAC roles. See also the [Swift Messaging API Getting Started](#).

If the application channels are identified by equivalent DNs, then they must share the same RBAC roles. See step 1 on page 37.

8. [Approve the Assigned RBAC Roles](#) on page 52.

Related information

[Knowledge Base article 5022495 - How-to videos about personal tokens](#)

9.1 Order Personal Tokens from Swift

You must evaluate the number of tokens required for your institution, taking into account the number of users who will use them. Plan also for sufficient spare tokens in case of replacement.

Some services, such as Alliance Cloud, include an initial pack of 10 personal tokens as part of the subscription.

Each BIC added to Alliance Cloud includes a pack of 10 personal tokens.

Before you begin

Only an administrator or security officer can order personal tokens for an institution.

For more information about how to designate your security officer, see the [Secure Channel User Guide](#) or visit the [Secure Channel](#) home page.

Procedure

1. Open the [personal tokens order form](#). You must log in to www.swift.com to access the order form.

Personal Tokens order

Enter the requested information.

The orange arrow icon ► indicates mandatory fields

Please use below form to order personal tokens.

Registered customer information

Institution that you order for

BIC		► ++ Institution BICs ++ ▼
Your own order reference		►
Sales partner		► S.W.I.F.T. SCRL ▼
SWIFT commercial quotation reference		
SWIFT account manager email address		

Tokens ordering

Please indicate the number of pack of tokens you want to order:

Quantity of pack of 10 tokens	►	1
Password of the new tokens		► Keep using the old password ▼

Personal tokens are delivered in packs of 10. You must order at least one pack. In the **Tokens ordering** section above, 10 tokens have been ordered as one pack.

2. Go to the **Shipping details** section.

The screenshot shows a 'Shipping details' form with a blue header. Below the header, there is a instruction: 'Specify the (shipping) contact name below who will receive the tokens. Do not use a P.O box address as a person will have to sign for the reception of tokens'. The form contains several fields: 'Token shipping details' with a dropdown 'Define a new shipping address'; 'Gender' with a dropdown 'please select'; 'Family name', 'First name', and 'E-mail' with text input fields; 'Phone number' with a dropdown '+' and a text input field; 'Building name and floor' with a text input field; 'Street name' with a text input field; 'House number' with a text input field; 'Postal/ZIP code' with a text input field; 'Country' with a dropdown 'please select'; 'State' with a dropdown 'please select'; 'City' with a dropdown 'please select a country first' and a text input field; and 'VAT' with a dropdown 'please select'. There are also blue question mark icons next to 'Phone number', 'Building name and floor', 'Street name', 'House number', and 'City'.

3. Complete the appropriate fields and click [Continue](#).

You will receive an acknowledgement e-mail at the address you provide in the **E-mail** field in the shipping details. This e-mail confirms that your order has been received. Expect the delivery of the personal tokens within a few weeks.

Swift will send the initial token password by **e-mail** to the e-mail address that was used in the order form.

Related information

[Ordering](#)

9.2 Create Back-up Security Officers

For back-up purposes, Swift recommends the creation of two additional security officers with both online and offline roles.

This means that your institution will have four operators with security officer permissions. This is very useful when one of the two original security officers is unavailable or forgets their password. Some security-related actions and tasks can only be done when both security officers are present.

An online security officer has access to SwiftNet Online Operations Manager and the Swift Certificate Centre. An offline security officer has access to Secure Channel and the Identity Management tool on www.swift.com.

It is assumed that the two initial security officers have the 4-eyes authorisation scheme activated. This means that these security officers have RBAC roles SWIFT.LRA//CertificateAdministration4eyes and SWIFT.RBAC//Delegator4eyes assigned to themselves in SwiftNet Online Operations Manager (O2M).

Before you begin

If you have blank tokens available, then you can use these tokens for the back-up security officers.

Otherwise you must order new tokens on www.swift.com > [Order Personal Tokens](#).

Procedure

1. Create back-up online security officers.

1. In O2M, an existing security officer must create a DN for each back-up security officer. See [Create a Distinguished Name \(DN\)](#) on page 41.

Important The DNs for back-up security officers must be created under a [level 2 DN](#) (and not a level 3 DN) as shown in the following example.

The recommended DN naming convention for Alliance Cloud security officers is as follows:

cn=so<N>, o=<BIC8>, o=swift

where <N> is a positive number.

Example

cn=so3, o=bankbebb, o=swift

2. The two existing security officers must then follow the steps in these procedures:

- a. [Set Up a User for Certification](#) on page 42
- b. [Authorise the DN and Retrieve Activation Secrets](#) on page 44
- c. [Assign RBAC Roles](#) on page 46
- d. [Approve the Assigned RBAC Roles](#) on page 52

2. Activate token

3. The back-up security officers must activate their tokens. See [Activate Token](#) on page 53.

3. Create back-up offline security officers - recommended

4. The same online security officers must create an account on swift.com > [mySWIFT](#) if they have not already done so.

See the [swift.com Registration User Guide](#).

5. An existing security officer must add the new security officers in Secure Channel.

See "Register (Add) a New Offline Security Officer" in the Secure Channel [User Guide](#).

6. In Secure Channel, another security officer must approve the requests.

See "Approve a New Offline Security Officer" in the Secure Channel [User Guide](#).

Swift sends the new back-up security officers a personal secure code card by courier service that enables them to use Secure Channel.

9.3 Create a Distinguished Name (DN)

In SwiftNet Online Operations Manager, a security officer must assign (register) a Distinguished Name (DN) for each personal token user and each Swift Integration Layer application channel.

Procedure

- One of the security officers must log in to the SwiftNet Online Operations Manager over MV-SIPN or the Internet with their Swift personal token inserted in their PC or laptop. Open the browser and type into the address bar the URL: **https://o2m.browse.swiftnet.sipn.swift.com**
- Go to **Security > Certificate Management - User** and click the **User certs** tab.
- In the tree view, determine where in the hierarchy the new user is to be positioned. This position in the tree determines the unique distinguished name created for the new user. Swift recommends that you minimise the number of levels used in the tree to facilitate maintenance of the tree. Put the user under an existing node by clicking that node to select it. The DN has a size limit of 100 characters. No spaces are allowed.

Example of a DN: cn=john-doe,ou=departmentname,o=bankbebb,o=swift, where:

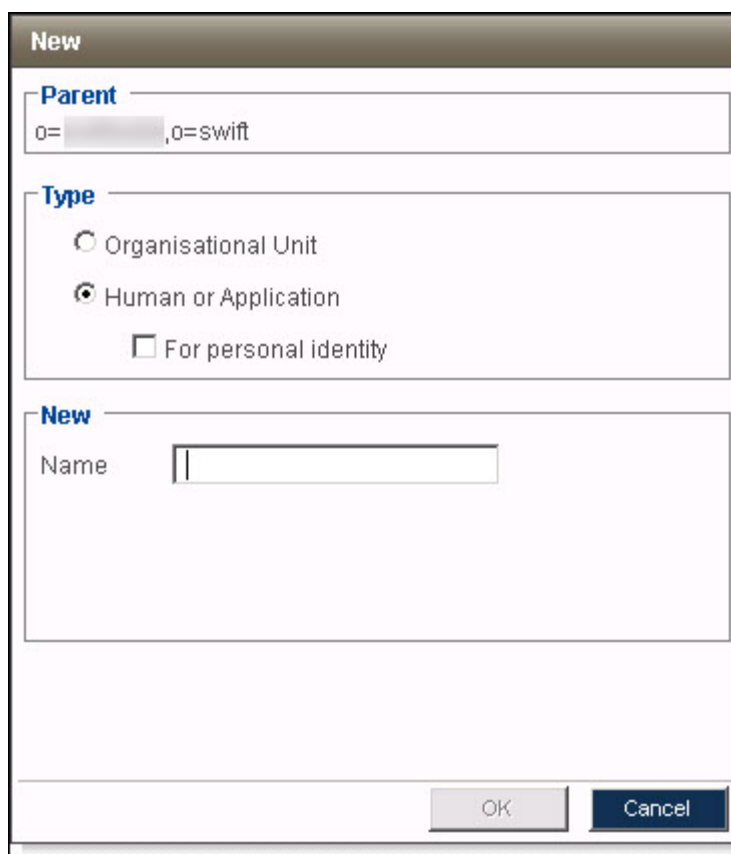
- the cn= segment has the name of the token holder (Mandatory)
- the ou= segment allows you to group multiple users under the same organisation unit in your tree (Optional)
- the first o= segment contains your live BIC, whatever the environment, live or test (Mandatory), where o is the letter o (oscar), and not 0 (zero)

- Click **New**.

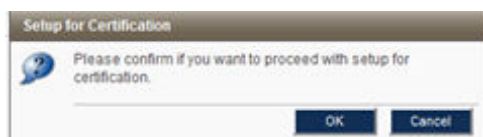
The **New** window appears.
Select the type **Human or Application** and type the name.
Type the name in the **Name** field. For human users, type the **firstname-lastname**. Example: john-doe
Use a maximum of 20 characters (alphanumeric characters and hyphens are allowed). The first character entered must be an alphabetic character.

Important If your institution plans to use the active/standby feature for SIL instances, then the application channels must be created using equivalent DNs. Contact your institution's SIL administrator for more information.
To use DN equivalence, type a % followed by one or two digits in the **Name** field. For example, %01.

DN application channel 1	cn=%01,cn=appch1,cn=<server-x>,o=bankbebb,o=swift cn=%02,cn=appch1,cn=<server-x>,o=bankbebb,o=swift
DN application channel 2	cn=%01,cn=appch2,cn=<server-x>,o=bankbebb,o=swift cn=%02,cn=appch2,cn=<server-x>,o=bankbebb,o=swift



5. Click **OK**.
6. In the **Please sign to confirm window**, click **Sign** then type your token password.
7. A confirmation window appears and asks you if you want to set up the user for certification.



8. Click **OK**.

What to do next

[Set Up a User for Certification](#) on page 42.

- ☒ Click [here](#) to go to the Getting Started checklist.

9.4 Set Up a User for Certification

Once new users are registered, they must be set up for certification.

This procedure generates the activation secret that are required in the certification process. Only security officers who have a user profile containing the role required for certificate administration can perform the set-up for certification.

Before you begin

[Create a Distinguished Name \(DN\)](#) on page 41

Procedure

1. Go to a **Certificate Management** page and click the **User Certs** tab.
2. In the tree view, double-click a node to open its details.
3. Click **Certify**.

The **Setup for Certification** window appears.

Setup for Certification

Distinguished Name

cn=,ou=be,o=swcsbeb2,o=swift

☒ I confirm ' is the certificate holder's verified personal identity.

Certificate Class

☐ Business

☐ Lite

☐ Personal HSM

☒ Personal token

☐ Channel

Password Policy

☐ Human Password

☐ Application Password

☐ Level 6 (Minimum)

☒ Level 8 (Medium)

☐ Level 12 (Maximum)

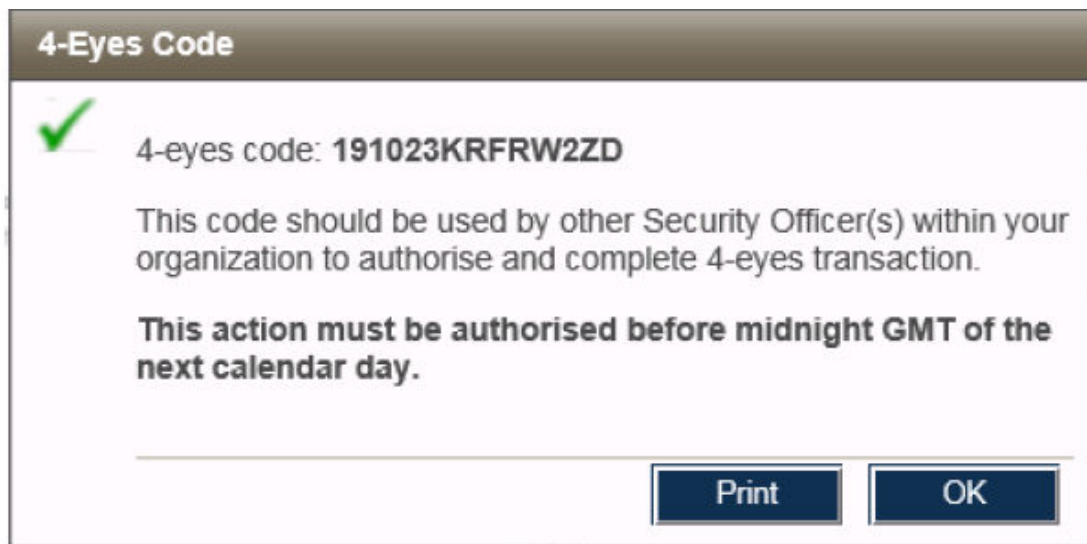
OK Cancel

4. For human users, select the check box next to **I confirm...**
5. Select the certificate class:
Personal token or **Channel** (for a channel certificate used for MV-SIPN (multi-vendor secure IP network)).
6. Select the password policy. Choose from **Level 6**, **Level 8**, and **Level 12**. The password policy determines the minimum password complexity for a user when a token is activated or reset.

For guidance on choosing a password policy, see the [SwiftNet PKI Certificate Administration Guide](#).

7. Click .
8. Click in the **Please sign to confirm window**.

The **4-Eyes Code** window appears. This window displays a 14-digit code. Copy the full name of the created DN for reference later.



9. Copy or print the 4-eyes code and click .
- Give the 4-eyes code to another security officer. The other security officer must perform the four-eyes authorisation of the action before midnight GMT of the next calendar day. For more information, see [Authorise the DN and Retrieve Activation Secrets](#) on page 44.
10. Click to quit the *SwiftNet Online Operations Manager* when you have created all of the users. Close the window and log out from Browse.

What to do next

The other security officer must authorise the action. See [Authorise the DN and Retrieve Activation Secrets](#) on page 44. This procedure also explains how to complete the important step of filling in the **User Name** field for all Swift personal tokens.

- ☒ Click [here](#) to go to the Getting Started checklist.

9.5 Authorise the DN and Retrieve Activation Secrets

The security officer who created the DN cannot authorise the DN. Another security officer must perform the authorisation procedure.

Use the 4-eyes code to retrieve and authorise the action of the requesting security officer.

Procedure

1. The other security officer must log in to *SwiftNet Online Operations Manager*.
2. Go to the **Security > 4-eyes Authorisation** page.
3. Enter the 14-digit 4-eyes code that you received from the security officer who created the DN and click .

The details of the action to authorise appear in the right pane.

Once the retrieval is done, the **Authorise** button is enabled.

SWIFTNet Online Operations Manager

Home | Print View | Help | Log Off

Security | Messaging | Reports | Administration

Home > Security > 4-eyes Authorisations

Logged on as: [User Icon]

Type in or paste the code below:

▶ 191113Q0K2TLPC ✕

Action to Authorise

Authorising a 4-eyes action
Please provide the 4-eyes code in the text field. Click Retrieve to display the details of the request to be authorised.

Four Eyes Code List (1 total)

Request Time	Code	Service	Request Type	Target DN
12-Nov-2019 1	191113Q0K2TLPC	SWIFT.LRA	CertificationSel	cn= ,ou=users,o= ,o=swift

Requests Approvals Retrieve Authorise Reset

© SWIFT 2019

Privacy statement

4. Verify the details and click **Authorise**.
5. Enter your token password and click **OK**.
- An **Operation Successful** window appears.
6. Click **OK**.
7. Go to **Security > Certificate Management - User**.
8. Double-click the DN that the first security officer has created to display the information for the DN.
9. **Mandatory:** For all Swift personal token users (including application channels that use personal tokens): click the pencil icon to the right of the **User Name** field and type the name of the user. You can optionally add a description. Click the **Save** link.

This is the name created by a security officer to identify an individual user. It has the format **firstname-lastname**. The name is case sensitive and can also be differentiated by the use of white space. For instance, **John Doe** and **johndoe** are considered to be different. Swift recommends that you use the same **firstname-lastname** used in [4](#) on page 41 unless the DN uses a generic name.

This name is required for audit purposes, as some DNs do not use the format **firstname-lastname** but use a generic name such as **operator1**.

Important This step is mandatory as users will not be able to log in to Alliance Cloud if this field is not filled in.

A maximum of 32 characters can be used. The valid character set consists of uppercase and lowercase alphanumeric characters, whitespace, and the following special characters:
, . : - _ ' "

The screenshot shows a web interface titled "Certificate Information" with a "Collapse All" and "Expand All" link. Below the title is a tab labeled "testnd". The form contains the following fields: "Distinguished Name" with the value "cn= , ou= , o= swift", "User Name" (empty), "Description" (empty), and "Status" with the value "Registered". At the bottom left is a "Manage Roles" link with a small icon, and at the bottom right are "Certify" and "Delete" buttons.

10. Click **OK**.

After a few moments the information for the user is updated.

11. **For personal tokens:** Click **+** to the left of the **Activation Secrets** field to display the Activation Code.

The screenshot shows a web interface titled "Activation Secrets". It contains a single text field labeled "Activation Code" with the value "E67N-SI3R-AY44-43NI-K2RE-7FE6-RIAQ". At the bottom left is a "Manage Roles" link with a small icon, and at the bottom right is a "Disable" button.

12. Copy the activation code and give it to the personal token user.

Give also the initial password to the operator. The initial password was sent by Swift to one of the security officers. It is the same for all tokens. The operator needs this password to activate the token on the Swift Certificate Centre.

13. **For channel certificates:** Click **+** to the left of the **Activation Secrets** field to display the Reference Number and the Authorisation Code.
- **Reference Number:** an eight-digit number
 - **Authorisation Code:** three groups of four characters. The letters are in upper-case.

The screenshot shows a web interface titled "Activation Secrets". It contains two text fields: "Reference Number" with the value "23381982" and "Authorisation Code" with the value "S8NW-D8D6-KVGR".

14. Copy the activation secrets and pass them to the SIL administrator. This person will need the secrets to download the channel certificate into Swift Integration Layer.
15. Click **Log Off** to quit the *SwiftNet Online Operations Manager*.

What to do next

- ☒ Click [here](#) to go to the Getting Started checklist.

9.6 Assign RBAC Roles

RBAC roles (Role-Based Access Control) are roles that can be assigned to operators to determine what the operator is allowed to access.

To perform tasks, operators must have the RBAC roles assigned by the first Alliance Cloud security officer. This creates the four-eyes code.

The first security officer then provides the four-eyes code to the second security officer who logs in and approves the action.

The security officers must grant the **admin** or **user** role to each user's DN on the **swift.alliancecloud** service and the **swift.alliancecloud!p** Test and Training (T&T) service.

Each user needs one of the following roles to access Alliance Cloud:

- **admin**: this grants administrator privileges to the Alliance Cloud administrators who set up Alliance Cloud
- **user**: this grants normal user privileges (that is, non-administrator) to the user.

When a user logs in to Alliance Cloud for the first time, the initial user account is created with the setup corresponding to the RBAC roles of the DN used to connect.

For application channel certificates, you must assign the **access_to_service** RBAC role which is under the **swift.alliancecloud.sil** service for Live and under **swift.alliancecloud.sil!p** for T&T. This applies to application channels connecting with a token and a channel (disk) certificate.

For the Swift Messaging API, you must assign the **Alliance Cloud API Live** and **Alliance Cloud API Test** RBAC roles. See also the [Swift Messaging API Getting Started](#).

Relationship Management Portal

You must also assign the appropriate RBAC roles to staff who will manage authorisations in the Relationship Management Portal. For more information, see [Role-Based Access Control Requirements](#) in the [Relationship Management Portal Getting Started](#).

Procedure

1. Log in to the *SwiftNet Online Operations Manager* (O2M) service: <https://o2m.browse.swiftnet.sipn.swift.com>
2. Click **Security > Role Management**.

A window appears that displays a tree view with user nodes and the **Role Information** pane on the right side of the window.

3. Double-click a user on the tree view and assign the necessary RBAC roles to the token DN for both the live environment and to for the test environment.

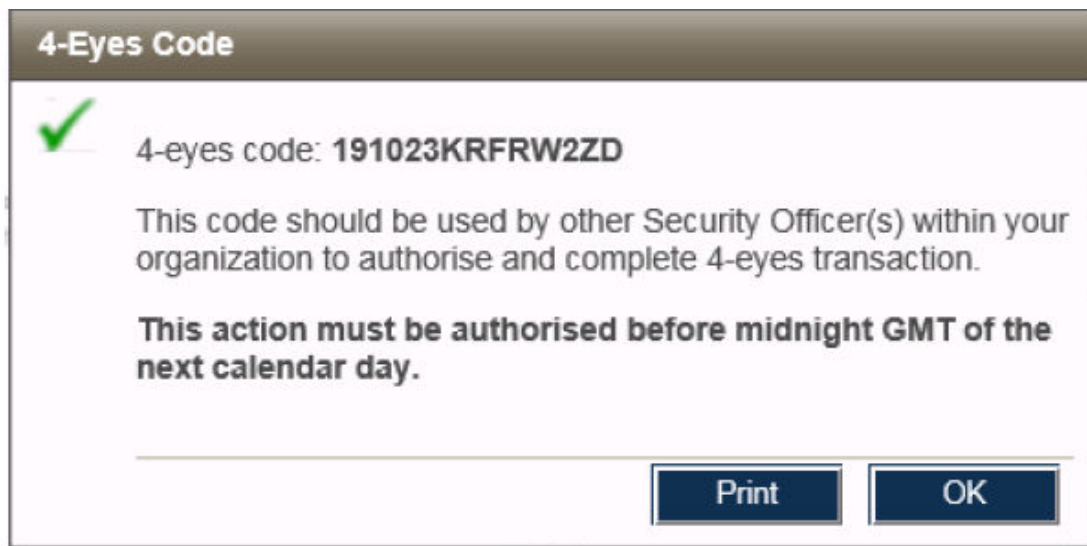
For the initial setup, you must grant the **admin** role to the first two Alliance Cloud administrators. If you have additional users created already, you can grant them the **user** role.

We recommend that you also grant the **SWIFT.RBAC/Normal User** role. This enables users to access O2M and view their own roles.

For more information about Distinguished Names, see the [SwiftNet PKI Certificate Administration Guide > Distinguished Name Equivalence](#).

8. Enter your password and click .

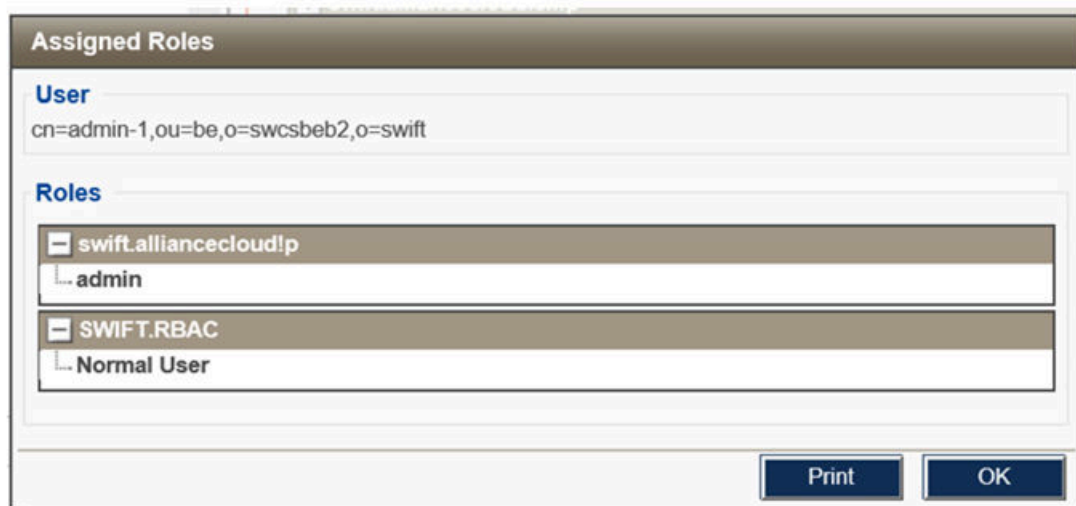
The **4-Eyes Code** window appears providing you with a 4-eyes code number that the second security officer needs to approve the roles that are assigned to the user. It also provides additional information about the token. An example **4-Eyes code** is as follows:



9. Click to complete the RBAC role assigning procedure.

The assigned roles should be as follows:

Alliance Cloud administrators



Alliance Cloud users

Assigned Roles

User
cn=user-token-1,ou=be,o=swcsbeb2,o=swift

Roles

☒ swift.alliancecloud!p
... user
☒ SWIFT.RBAC
... Normal User

Print OK

SIL application channel connecting with a channel (disk) certificate

Assigned Roles

User
cn=silrhel,ou=be,o=swcsbeb2,o=swift

Roles

☒ swift.alliancecloud.sil!p
... access_to_service
☒ SWIFT.RBAC
... Normal User

Print OK

SIL application channel connecting with a personal token

Assigned Roles

User
cn=siltoken,ou=support,o=swcsbeb2,o=swift

Roles

☒ swift.alliancecloud.sil!p
... access_to_service
☒ SWIFT.RBAC
... Normal User

Print OK

What to do next

[Approve the Assigned RBAC Roles on page 52](#)

☒ Click [here](#) to go to the Getting Started checklist.

9.6.1 RBAC roles for Migrating Alliance Access Customers

This topic describes the suggested RBAC roles for security officers in institutions using Alliance Access that migrate to Alliance Cloud.

SWIFT.LRA/CertificateAdminsistrator4eyes

SWIFT.RBAC/Auditor

SWIFT.RBAC/Delegator4eyes/SWIFT.RBAC/Viewer

SWIFT.RBAC/Delegator4eyes/AnyBusinessService/Dummy

SWIFT.RBAC/Delegator4eyes/swift.rug/SiteManager

SWIFT.RBAC/Normal User

SWIFT.RBAC/Viewer

SWIFT.rug/SiteManager

SWIFT.RBAC/Delegator4eyes/SWIFT.LRA/CertificateAdminsistrator4eyes

SWIFT.RBAC/Delegator4eyes/SWIFT.RBAC/Delegator4eyes

SWIFT.RBAC/Delegator4eyes/SWIFT.RBAC/Normal User

SWIFT.RBAC/Delegator4eyes/SWIFT.RBAC/Auditor

SWIFT.RBAC/Delegator4eyes/SWIFT.LRA/Auditor

SWIFT.LRA/Auditor

9.7 Approve the Assigned RBAC Roles

Procedure

1. If the first security officer assigned the RBAC roles, then the second security officer must approve the RBAC roles.
2. On the **SwiftNet Online Operations Manager** window, click **Security > 4-eyes Authorisations**.
3. In the text box as indicated on the screen, type or paste the code that the first security officer received at the end of the procedure for assigning the RBAC roles.
4. Click **Retrieve**.

The details of the action to authorise appear in the right pane.

SWIFTNet Online Operations Manager

Home | Print View | Help | Log Off

Home > Security > 4-eyes Authorisations

Logged on as: [User Icon]

Type in or paste the code below:

▶ 191113Q0K2TLPC ✕

Action to Authorise

Authorising a 4-eyes action
Please provide the 4-eyes code in the text field. Click Retrieve to display the details of the request to be authorised.

Four Eyes Code List (1 total)

Request Time	Code	Service	Request Type	Target DN
12-Nov-2019 1	191113Q0K2TLPC	SWIFT.LRA	CertificationSe	cn=, ou=users,o=, o=swift

Requests Approvals Retrieve Authorise Reset

© SWIFT 2019

Privacy statement

5. Verify the details and click **Authorise**.

SWIFTNet Online Operations Manager

Home | Print View | Help | Log Off

Security Messaging Reports Administration

Home Security 4-eyes Authorisations Logged on as

Type in or paste the code below:

191113Q0K2TLPC

Action to Authorise

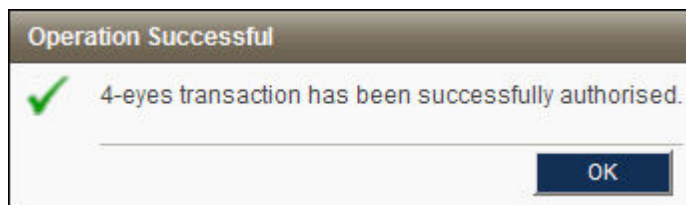
Action	Setup for Certification
Request Time	12-Nov-2019 19:20:31 (GMT)
Requestor	cn=, ou=users, o=swift
Message Content	
Target DN	cn=, ou=users, o=swift
Certificate Type	Unmanaged
Password Policy	Level 6 (Minimum)

Requests Approvals Retrieve Authorise Reset

© SWIFT 2019

Privacy statement

The **Operation Successful** confirmation window appears.



6. Click **OK**.

For more information about **SwiftNet Online Operations Manager**, see the [SwiftNet Online Operations Manager User Guide](#).

What to do next

- ☒ Click [here](#) to go to the Getting Started checklist.

9.8 Activate Token

A token requires activation before use. Activation requires you to have your token, the initial token password selected by one of your security officers, activation codes, and access to the [Swift Certificate Centre](#) from a PC that has an installation of token software and SConnect.

About this task

When you first receive your personal token, the token is **inactive** because it does not yet contain the private key to your digital certificate. Activation generates a public and private key pair. You must activate your token on the Swift Certificate Centre before you can use it for Swift services. The public key is sent for registration with the SwiftNet PKI authority. The private key never leaves the token.

Tip To view the video version of this task, see KB video [5019642](#).

Procedure

1. Navigate to <https://www.swift.com/certificates> for connection over the Internet, or to <https://scc.swiftnet.sipn.swift.com> for connection over MV-SIPN.
The **Swift Certificate Centre** window appears.
2. Insert your token into a free USB port of your computer.
3. Click **Login**.
The **Confirm Certificate** window appears.
4. Select the certificate and click **OK**.
The **Log on to eToken** window appears.
5. Type the initial password that was supplied with the token in the **Password** field and click **OK**.
You receive your token from the one of your security officers, and the initial password from another security officer.
6. You may have to provide the password a second time.
The **Swift Certificate Centre Login** window appears.
7. Type the initial password that was supplied with the token in the **Enter your token password** field and click **Login**.
The **Token Activation** window appears.
8. In the **Enter Activation Code** window, type the activation code that you received from your security officer, or enter it using copy-and-paste and click **Validate**.
If there is a problem with the activation code, then re-enter the code and click **Validate** again.
Note The activation code is required only once to complete the activation. After activation is complete, this code cannot be reused.
9. You must now set your own password for the token. Read the password policy rules on the **Change password** window, then complete the following fields:

Current Password	Enter the initial password that was supplied with the token.
New Password	Provide a strong password. Use the following guidelines when creating a password: • the minimum length varies according to the password policy • the maximum possible password length is twenty characters • You can use the following characters: • 0-9 A-Z a-z and space • ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ • you cannot use accented characters (for example, é or ö)
Confirm new password	Re-enter the new password.

- Note** Passwords expire. The token password policy determines how often you must change your password.
10. Click **Change**.
Your private key is now being generated on the token and the public key is being certified by Swift.

The **Activation complete** window appears.

Your personal token is ready for use now that it stores your certificate and a private key that is password protected.

The **Activation complete** window displays the following information about the certificate on your token:

DN	The Distinguished Name of your certificate.
Expires	The date and time at which the certificate expires.

Click [Logout](#) to quit the Swift Certificate Centre.

What to do next

☒ Click [here](#) to go to the Getting Started checklist.

Related information

[Swift Certificate Centre Portal User Guide](#)

9.9 Token Renewal

A token certificate is valid for two years.

Make sure that you and all users in your institution with a token renew the token certificate before its expiry date. This will avoid having to reset the token.

Certificate reports

As a security officer, you can run certificate reports in SwiftNet Online Operations Manager to list your institution's certificates. The reports list the key characteristics for each certificate, such as the Distinguished Name, the policy ID, and the expiration date. For more information, see [Certificate Reports in SwiftNet Online Operations Manager User Guide](#).

Related information

[KB article 5020138-How to verify the expiration date of a certificate on a token](#)

9.10 Channel Certificate Recovery

A channel certificate is valid for two years.

It is not possible to renew a channel certificate. When the certificate expires, your channel certificate can no longer connect to Alliance Cloud.

To continue using Alliance Cloud with a channel certificate, your security officer must recover the certificate. Then the Alliance Cloud connectivity option administrator must import the new certificate into the appropriate software: Swift Integration Layer, the Alliance Cloud Connectors, or the Swift Messaging API-related API client.

For more information, see [Recover a Channel Certificate](#) in the *Alliance Cloud Operations Guide*. See also [Certificate Reports in SwiftNet Online Operations Manager User Guide](#).

9.11 New Online Security Officer Requirements when Migrating to Alliance Cloud

This topic describes when new online security officers are needed in different migration scenarios to Alliance Cloud.

Interface	Security officers can be re-used	Are RBAC roles modified during migration?	Next steps
Alliance Lite2	Yes	Yes, during the migration to Alliance Cloud, Swift assigns additional Role-Based Access Control (RBAC) roles to align with default roles assigned to standard SwiftNet online security officers, with the exception of 4 eyes security settings that are preserved. The RBAC roles are added when the BIC is activated in Alliance Cloud Test and Training. The roles added are as follows: • SWIFT.RBAC/Delegator4eyes/SWIFT.LRA/CertificateAdminsitrator4eyes • SWIFT.RBAC/Delegator4eyes/SWIFT.RBAC/Delegator4eyes • SWIFT.RBAC/Delegator4eyes/SWIFT.RBAC/Normal User • SWIFT.RBAC/Delegator4eyes/SWIFT.RBAC/Auditor • SWIFT.RBAC/Delegator4eyes/SWIFT.LRA/Auditor • SWIFT.LRA/Auditor	With those additional RBAC roles, these online security officers can create online back-up security officers. See Create Back-up Security Officers on page 39.
Alliance Access managed by the BIC	If certificates are on HSM, then the security officers' DNs cannot be re-used. New online security officer DNs on personal tokens must be created by the existing online security officers. The certificate recovery process cannot change the certificate type from HSM to personal token.	No	Create Back-up Security Officers on page 39.
Alliance Access managed by a third party	If certificates are on HSM, then the security officers' DNs cannot be re-used. New online security officer DNs on personal tokens must be created by the existing online security officers. The certificate recovery process cannot change the certificate type from	No	Two situations can occur: 1. PKI is managed (PKI delegation) by the third-party provider. In this case, the third party must create two new online security officer DNs. The PKI delegation should remain until the Live traffic is migrated to Alliance Cloud. 2. PKI is not managed by a third party (no PKI delegation) or the BIC already has two online security officers DNs on HSM. In this case, the existing online security officers can create two new security officers DNs on personal tokens. See Create Back-up Security Officers on page 39.

Interface	Security officers can be re-used	Are RBAC roles modified during migration?	Next steps
	HSM to personal token.		If there is an issue with the third party provider, then two new security officer DN's must be requested using the Secure Channel Free Text request. The new online security officers will have default SwiftNet online security officer RBAC roles. It is recommended to restrict the RBAC roles to 4-eyes. See the Secure Channel User Guide .
Alliance Remote Gateway	Yes, but with limited RBAC roles (backup security officers cannot be created). Requesting two new online security officers is the only possible option.	No	Two new online security officer DN's must be requested using the Secure Channel Free Text request. These new online security officers will have default online SwiftNet security officer RBAC roles. It is recommended to restrict the RBAC roles to 4-eyes. See the Secure Channel User Guide .

10 Alliance Cloud Administrator Tasks: User and Role Management

Alliance Cloud administrators define users and roles in the Admin centre and assign roles (permissions) to users.

The Alliance Cloud administrator must liaise with the security officers to complete some of the tasks described in this section.

☒ Click [here](#) to go to the Getting Started checklist.

Prerequisites

Before you can log in to Alliance Cloud, make sure that the following tasks are completed:

1. To access the Swift Certificate Centre, make sure that one of your colleagues, such as your system administrator, has installed the Swift Personal Token Software (available on the [Download Centre](#)) **and** SConnect on the PC where you will use the Swift personal token. These are one-off tasks that must be completed to have the necessary software to connect, configure, and to read the certificates on personal tokens.
2. Ask your security officers for your initial token password and the activation code.
3. Make sure that your security officers have assigned to you and approved the **admin** RBAC role in the SwiftNet Online Operations Manager (O2M) for the live or test environment (or both). RBAC means "Role-Based Access Control" and determines what a certificate is allowed to access.
4. Activate your token on the [Swift Certificate Centre](#). See [Activate Token](#) on page 53.
5. Insert your activated token into an appropriate USB port of your PC. Make sure that you have the password that you created during the activation process.
6. Log in to Alliance Cloud:
Live environment: <https://swift-alliancecloud.browse.swiftnet.sipn.swift.com>
Test environment: <https://swift-alliancecloud-test.browse.swiftnet.sipn.swift.com>
7. Go to the Admin centre module.

Alliance Cloud administrator tasks

If you have questions when doing the following tasks, then help is available after you log in. Just click the [?](#).

1. Set up the roles and the related permissions for users.
When you first log in, you will automatically receive the **Administrator** role in Alliance Cloud. This is a read-only role and cannot be modified.
Alliance Cloud provides a set of default roles (which contain a set of permissions) that are already available for you to use. The existing [default roles](#) cannot be modified and apply to all of the BICs belonging to the [business entity](#). You can copy them and modify the copied roles to make them more specific to your institution.
Create additional roles, as needed, and assign permissions to the roles or use parameters to further restrict what users can do. For example, you can create a new role based on the Message management operator default role. You can then limit the access to messages based on criteria such as BICS, amount, and currency. See "Create Customised Roles" in the [Alliance Cloud Operations Guide](#).

Important If for some reason the **first** Alliance Cloud administrator to log in to Alliance Cloud is deleted from Alliance Cloud and then subsequently created with the same user name in O2M, then this administrator must be created manually in the Admin centre by the other (second) Alliance Cloud administrator.

2. Create new users and assign them roles.

Tip *Alternatively, you can ask Alliance Cloud users to log in to the Admin centre to automatically create their user name and then log out. You can then assign the role or roles to users to allow them to work in Alliance Cloud. For more information, see [Initial Login by Alliance Cloud Users](#) on page 60.*

When creating users, for each user make sure that you have the exact name as defined in O2M by your security officers (the 8-character BIC and username). Ask your security officers to provide you with this information before you start to create the users.

Create the two users who will be the Message management administrators. Assign the role **Message management configurator** to these users. This role will give them the permissions to create, manage, and approve application channels, units, and workflows. Create a user or multiple users who will be the Event log administrators. Assign the role **Auditor** to these users. This role will give them permissions to view the Event log. Create the other users in the Admin centre and assign roles to each user.

Important After creating users, you cannot edit the BIC or the user name. If a name change is needed, then one of your security officers must change the name of the user in the SwiftNet Online Operations Manager (O2M). O2M will synchronise with Alliance Cloud between sessions to update the name

3. The second Alliance Cloud administrator must log in to approve any newly created users.

Default roles in Alliance Cloud

Type of user	Default role in Alliance Cloud Admin centre	Description
Alliance Cloud administrators	Administrator	Create, modify, and delete users and roles, and assign roles to users in the Admin centre. An institution must have at least two of these administrators. When the Alliance Cloud administrators log in to Alliance Cloud for the first time, they automatically receive the Administrator role in Alliance Cloud.
Event log administrators	Event log viewer	View and investigate events that occurred in the Admin centre and Message management modules.
Message management administrators	Back-office operator	When messages have not been successfully distributed to the back-office (through SIL or direct APIs), the back-office operator has the permission to restart and relaunch the distribution of these messages to an application channel.
Message management administrators	Message management business operator	Access to all permissions of the message management module except the permission to redistribute the messages to an application channel.
Message management administrators	Message management business operator (incl. verify own)	Access to all permissions of the message management module except the permission to redistribute the messages to an application channel. Verify own messages.
Message management administrators	Message management authoriser	Verify, approve, cancel and close (single or multiple) messages. Note <i>Cannot create messages.</i>
Message management administrators	Message management creator	Create and repair messages. Create and manage message templates.

Type of user	Default role in Alliance Cloud Admin centre	Description
Message management administrators	Message management configurator	Create the application channels and units in the Admin centre. Design and configure the workflow in the Admin centre. Design and configure the archive messages feature.
Message management administrators	Message management viewer	View messages.
Message management operators	Message management operator	Create messages, view and search for messages, verify messages, repair messages, and approve messages based on the specific conditions and criteria configured in the workflow. Redistribute messages manually to the back office.

Roles provisioned for delegation purposes

These roles are provisioned for delegation purposes and can be shared with another institution for a certain amount of time. These roles are locked. The provider and the customer cannot modify them.

Default role	Description
External message management configurator	Create, manage, and approve application channels and units, and configure workflows on behalf of a delegating customer
Support	The Support role is assigned by customers to Swift.

Token renewal

Your token certificate is valid for two years.

Make sure that you renew your token certificate in the Swift Certificate Centre before its expiry date. If you do not renew the certificate in time, then your security officer must reset the token. See "Renew Token Certificate" in the [Alliance Cloud Operations Guide](#).

See also Knowledge Base article [5020138](#) **How to verify the expiration date of a certificate on a token.**

Related information

[Alliance Cloud Operations Guide](#)

10.1 Initial Login by Alliance Cloud Users

There are two ways to create users in Alliance Cloud.

1. Recommended option

Each user can log in to Alliance Cloud before an Alliance Cloud administrator creates the users in the Admin centre. The user profile will be created automatically in the Admin centre based on the name defined in SwiftNet Online Operations Manager (O2M) by a security officer. Users must then log off and let the Alliance Cloud administrator assign the appropriate role or roles to them before they can begin working in Alliance Cloud. This option ensures that the correct user name is created in the Admin centre. This option also saves time as the Alliance Cloud administrator does not have to manually create each user.

2. An Alliance Cloud administrator manually creates each user in the Admin centre. The administrator must use the **exact name** as defined in O2M by a security officer (the

8-character BIC and username). The administrator must ask the security officers for this information before starting to create the users. The administrator then assigns the appropriate role or roles to the users. Users can then log in to Alliance Cloud and perform tasks based on their roles.

11 Message Management Administrator Tasks

Message management administrators create, manage, and approve application channels and units, and configure workflows. They may also activate and configure the archive copy distribution (archive messages) and import message templates, to facilitate the migration to Alliance Cloud from another Swift interface.

The Message management administrator must liaise with the security officers, the Alliance Cloud administrator, and the Alliance Cloud connectivity option administrator to complete some of the tasks described in this section.

☑ Click [here](#) to go to the Getting Started checklist.

Prerequisites

Before you can log in to Alliance Cloud, make sure that the following tasks are completed:

1. To access the Swift Certificate Centre, make sure that one of your colleagues, such as your system administrator, has installed the Swift Personal Token Software (available on the [Download Centre](#)) **and** SConnect on the PC where you will use the Swift personal token. These are one-off tasks that must be completed to have the necessary software to connect, configure, and to read the certificates on personal tokens.
2. Ask your security officers for your initial token password and the activation code.
3. Make sure that your security officers have assigned the **user** RBAC role to you (and approved it) in the SwiftNet Online Operations Manager (O2M). RBAC means "Role-Based Access Control" and determines what a certificate is allowed to access.
4. Activate your token on the [Swift Certificate Centre](#). See [Activate Token](#) on page 53.
5. Make sure that an Alliance Cloud administrator has created you as a user and has assigned the **Message management configurator** role to you. This role gives you the permissions to create, manage, and approve application channels, units, and workflows.
6. Insert your activated token into an appropriate USB port of your PC.
Make sure that you have the password that you created during the activation process.
7. Log in to Alliance Cloud:

Live environment: <https://swift-alliancecloud.browse.swiftnet.sipn.swift.com>

Test environment: <https://swift-alliancecloud-test.browse.swiftnet.sipn.swift.com>

Message management administrator tasks

1. Design the connection to the back office with the Alliance Cloud connectivity option administrator.
The Swift [Professional Services](#) team is available to help customers with this task if needed.
2. Create the application channel in the Admin centre.
An application channel allows Message management to receive from any Alliance Cloud connectivity option messages and files to be sent to Swift and to receive messages from Alliance Cloud. An application channel is also needed to send a copy of your messages and files with their history to a long-term storage engine. The same Distinguished Name (DN) must be used in SwiftNet Online Operations Manager (O2M), in the Admin centre, and in the SIL or Alliance Cloud Connectors GUI. Before creating the application channel in the Admin centre, you must check with your security officer and your Alliance Cloud connectivity option administrator. See [Add an Application Channel in Alliance Cloud](#) on page 64.

Important If your institution plans to use the active/standby feature for any Alliance Cloud connectivity option instances, then you must create the application channels **using the Common DN used in O2M (ignoring the numbered common name segment, such as %1)**. Contact your institution's Alliance Cloud connectivity option administrator for more information.

3. *Optional*: create units in the Admin centre to separate traffic between departments or teams.
Liaise with the Alliance Cloud administrator, who will link roles to units.
4. Design and configure the workflows in the Admin centre.
You must have one active workflow for each direction (incoming and outgoing).
If your institution has multiple business entities, then each business entity must have one active workflow for each direction.
 - Configure workflow steps and actions
 - *Optional*. Add a rule to distribute a copy (for an incoming workflow only) or a PDF copy (for both outgoing and incoming workflows) of a message with a distribution tag. When you assign a distribution tag in the workflow, SIL will download the message and store the message in a sub-folder in the reception directory. SIL automatically creates the sub-folder with the name of the distribution tag.
For more information about workflows, see [Alliance Cloud Operations Guide](#).
5. *Optional*: activate or configure the messages archive feature, which will automatically trigger a specific *archive copy* distribution at regular intervals
6. If your operators will test messages for the upcoming Standards release, then a Test and Training BIC for future mode must be configured in the **Parameters** screen of the Admin centre. See [Future mode](#) on page 118.
7. Import message template files into Alliance Cloud using the Admin centre module.
 - For Alliance Access and Alliance Entry customers
See [How to import message templates](#) in the [Alliance Cloud Operations Guide](#).
 - For Alliance Lite2 customers
 - a. Request an extract of the message templates in Alliance Lite2. To do so, contact Swift Customer Support using the [Case Manager](#). See also [000011107 - Alliance Lite2 - Customisation Request](#).
 - b. Provide complete information on what is required. You can order the specific configuration changes, one by one, as payable changes:
 - Export FIN message templates created in an Alliance Lite2 test environment.
 - Export MX message templates created in an Alliance Lite2 test environment
 - c. Swift will ask for a confirmation of the requested changes.
 - d. After you receive the templates from Swift, see [How to import message templates](#) in the [Alliance Cloud Operations Guide](#).

Token renewal

Your token certificate is valid for two years.

Make sure that you renew your token certificate in the Swift Certificate Centre before its expiry date. If you do not renew the certificate in time, then your security officer must reset the token. See "Renew Token Certificate" in the [Alliance Cloud Operations Guide](#).

See also Knowledge Base article [5020138](#) **How to verify the expiration date of a certificate on a token**.

11.1 Add an Application Channel in Alliance Cloud

The Message management administrator must create an application channel in the Alliance Cloud Admin centre module that will correspond to each channel configured in a Swift Integration Layer (SIL) instance.

1. In the SwiftNet Online Operations Manager (O2M), your institution's security officers create a DN for each application channel.
2. The Message management administrator creates the application channel or channels in Alliance Cloud Admin centre.

Each application channel is composed of a name and an optional description. It is identified by a Distinguished Name (DN) created by your security officers in O2M.

If your institution plans to use the active/standby feature for any Alliance Cloud connectivity option instances, then you must create the application channels **using the Common DN used in O2M (ignoring the numbered common name segment, such as %1)**. For more information, contact the administrator for your Alliance Cloud connectivity option.

3. The Alliance Cloud connectivity option administrator imports the channel (disk) or token certificate into the Alliance Cloud connectivity option using the SIL GUI, the Alliance Cloud Connectors GUI, or the API clients' features.

It is identified by the same Distinguished Name (DN) mentioned in the previous step.

When you create an application channel, you can define the distribution format for MTs, the XMLv2 revision, define how incoming multi-format messages will be distributed, and decide if the channel is bi-directional (default) or if it should only accept messages incoming from Swift.

Instructions about how to add an application channel in the Alliance Cloud Admin centre module are available online after you log in to the Admin centre.

The screenshot shows the 'Create new application channel' form in the Alliance Cloud Admin Centre. The form is titled '+ Create new application channel' and includes a sub-note: 'Create a new application channel for a particular business need. Activation of an application channel requires approval from another administrator.' At the top right, there are buttons for 'Cancel', 'Create as inactive', and 'Create & activate'. The form fields include: 'Distinguished name (DN)' (required), 'Application channel name', 'Description (optional)', and 'Business entity' (a dropdown menu). Below these fields is a 'Direction' section with a note: 'The direction in which this application channel is allowed to exchange.' It has two radio button options: 'Both directions allowed' (selected) and 'Not allowed to send outgoing messages'.

Related information

[Alliance Cloud Operations Guide](#)

11.2 Application Channel Limitations

Alliance Cloud architecture was designed to simplify the processing of messages. A configuration that includes less than 10 application channels should cater for the majority of complex scenarios.

If you need to create more than 10 application channels, then contact [Swift Professional Services](#) or the Swift Product team to request assistance in finding the optimal configuration.

Note

Each application channel connects to Alliance Cloud separately. Therefore, it consumes network bandwidth between the customer premises and Alliance Cloud and increases the risk of reaching the spike arrest limits. For more information, see the [Swift Messaging API Getting Started](#).

12 Swift Integration Layer (SIL) Installation and Configuration Tasks

The system administrator installs Swift Integration Layer. The SIL administrator (also known as the SIL_Owner) is a different person who will use the SIL GUI to configure SIL after installation, download the channel certificate (if applicable), and test and start application channels. The application channels are needed to exchange messages with Alliance Cloud.

Application channels require a certificate. This certificate is used to secure the connection to Alliance Cloud. This certificate can be stored on a token (Internet and Windows only) or on a channel certificate (MV-SIPN).

The SIL administrator must not be a part of the Windows administrator group.

The SIL administrator must liaise with the security officers and the Message management administrator to complete some of the tasks described in this section.

☒ Click [here](#) to go to the Getting Started checklist.

SIL installation tasks

The system administrator performs the following tasks:

1. Download Swift Integration Layer from the [Download Centre](#).
You can do so only after receiving an e-mail from Swift that confirms that Alliance Cloud has been provisioned for your institution.
2. Install Swift Integration Layer 2.4.0 on your premises. See the [Swift Integration Layer 2.4.0 Release Letter](#).
Give the SIL administrator password (that is initialised during installation) to the SIL administrator. Ideally, the SIL administrator will be with you during the installation. The SIL administrator needs this password to log in to the SIL GUI and to run certain command line tools.

Prerequisites for the SIL administrator

Make sure that the following tasks are completed before you configure the SIL GUI:

1. Your security officers must create and authorise a Distinguished Name (DN) in SwiftNet Online Operations Manager (O2M) for each application channel in SIL.
When security officers create the DN for the application channel, they must select the **Certificate Class** for the DN: **Personal token** or **Channel** (for a channel certificate).

Important If your institution plans to use the active/standby feature for SIL instances, then the application channels must be created using equivalent DNs. Make sure that your institution's security officers know about the decision to use this feature before they create the DNs in O2M. See [Use Active/Standby for SIL Instances](#) on page 78.

2. The Message management administrator must create the application channels in the Alliance Cloud Admin centre.

Important If you are using multiple application channels, then the Message management administrator must configure the application channels **using the Common DN (ignoring the numbered common name segment (for example, %1))**.

3. If you are using a **channel certificate**, then your security officers must give you the pair of activation secrets generated by O2M during the DN creation process. The SIL administrator needs these secrets to download the channel certificate into SIL.
4. In O2M, your security officers must assign the **access_to_service** RBAC role to the application channel DNs and approve the role.
5. Activate the token.
If you are using tokens (and not channel certificates), then your security officer must give you the token for the application channel, the activation secrets, and the initial token password. See [Activate Token](#) on page 53.
6. For more information about the emission and reception flows, file examples, message formats, and API endpoints, see "File and REST Application Channels" in the [Alliance Cloud Operations Guide](#).

Note *The security officer and administrator tasks mentioned previously are described in the appropriate sections of this document.*

SIL configuration tasks

The SIL administrator performs the following tasks:

- Configure SIL for Alliance Cloud using the SIL GUI. You need the SIL administrator password to log in to the GUI.
- Start SIL using the command `sil start`, then run the command `sil status`.
- [Log in to the SIL GUI](#) on page 71.
- Do the configuration tasks in the SIL GUI. These tasks include importing token certificates or disk (channel) certificates, assigning a certificate to a channel, and creating and configuring application channels.
See "Managing Application Channels in the SIL GUI" in the [Alliance Cloud Operations Guide](#).
- In the SIL GUI on the Alliance Cloud **application channels** page, start the application channel.
- [Test SIL Connectivity with Alliance Cloud](#) on page 80.
- If you have a problem and need to send configuration and logging information to Swift Support, then use the `sil support collectinfo` command. See [SIL Support Commands](#) on page 77

Note *Alliance Cloud command line tools in SIL are available only to start, stop, and retrieve the status of the Alliance Cloud component and application channels. See [Alliance Cloud Commands](#) on page 74.*

Alliance Cloud API Connector

Swift Integration Layer (SIL) offers an API Connector, providing connectivity with Alliance Cloud by exposing RESTful APIs.

The API Connector Software Developer Kit (SDK) provides a quick and easy way to integrate any back-office application (using Java or potentially any JVM language) with the RESTful APIs.

For more information about the Alliance Cloud API Connector and the SDK, see the [Knowledge Centre](#).

Token renewal

Your token certificate is valid for two years.

Make sure that you renew your token certificate in the Swift Certificate Centre before its expiry date. If you do not renew the certificate in time, then your security officer must reset the token. See "Renew Token Certificate" in the [Alliance Cloud Operations Guide](#).

See also Knowledge Base article [5020138](#) **How to verify the expiration date of a certificate on a token.**

Channel certificates

A channel certificate is valid for two years.

It is not possible to renew a channel certificate. When the certificate expires, your channel certificate can no longer connect to Alliance Cloud.

To continue using Alliance Cloud with a channel certificate, your security officer must recover the certificate. Then the Alliance Cloud connectivity option administrator must import the new certificate into the appropriate software: Swift Integration Layer, the Alliance Cloud Connectors, or the Swift Messaging API-related API client.

12.1 Swift Integration Layer End of Support in 2026

Swift's strategy foresees a zero-footprint future for its customers, whereby core applications are directly connected to our services using APIs.

Swift will therefore end support of Swift Integration Layer (SIL) by 30 June 2026.

For more information, see Knowledge Base article [6000466](#) - **Managing the SIL Sunset.**

The Alliance Cloud File Connector functionality will be supported beyond the end of support date of SIL.

However, you must migrate to the new Alliance Cloud File connector on the Swift Microgateway before 30 June 2026 to continue to use the file connectivity functionality.

The API Connector (or REST Connector) will go out of support at the same time as SIL. Customers who use the API Connector should use the Swift Messaging API after the end of support for SIL.

12.2 Alliance Cloud Connector

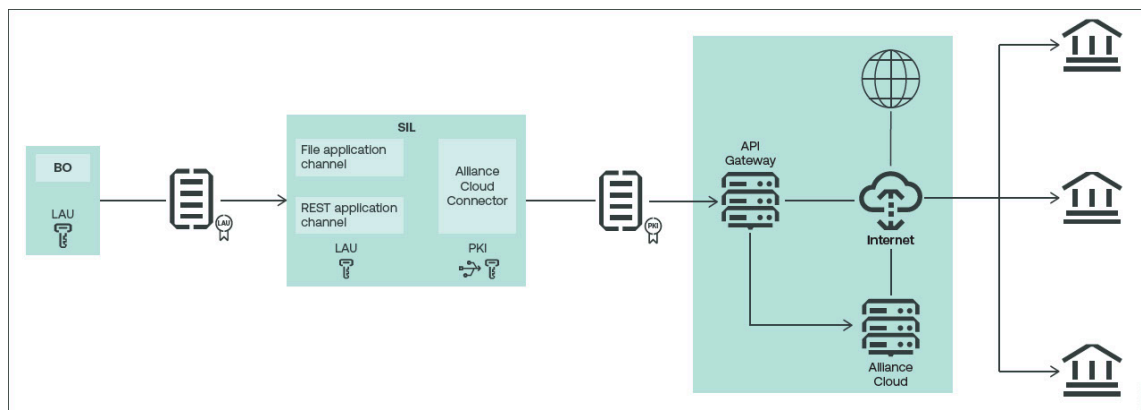
The Alliance Cloud Connector enables Swift messages and files to be exchanged between back-office applications and the Alliance Cloud server over the internet or through the multi-vendor secure IP network (MV-SIPN).

Alliance Cloud can connect to the back office in different ways, including the following:

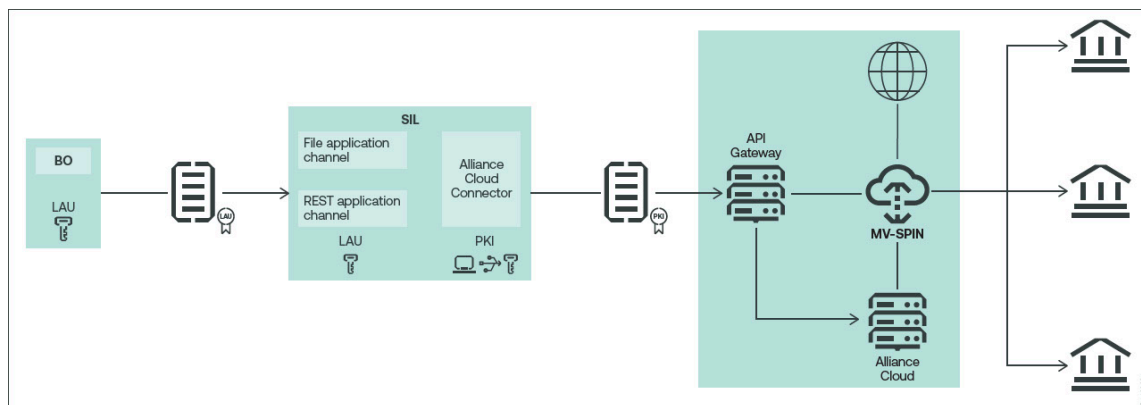
- File channel
- REST channel (RESTful APIs)

For more information, see [Configure and Use Swift Integration Layer](#) on page 69.

Connection over the Internet with a Swift personal token



Connection over MV-SIPN with a Swift personal token or a channel certificate



Related information

[File and REST Application Channels in the Alliance Cloud Operations Guide](#)

12.3 Configure and Use Swift Integration Layer

12.3.1 SIL Command Line Tools

SIL can be configured using command line tools.

Alliance Cloud customers must perform a number of configuration tasks using a GUI. See [SIL GUI for Alliance Cloud Configuration](#) on page 70.

You can execute SIL commands by typing the full command from within a shell or Windows command prompt (for example, `sil setup changepassword`) or by using the SIL interactive console.

For more information about SIL commands, see the [Swift Integration Layer User Guide](#).

Prerequisites

The operating system (OS) user who owns, and runs the Swift Integration Layer commands is referred to as the **<SIL_OWNER>** (or the SIL administrator).

Most commands do not require providing an explicit user name or password in the command line.

However, some sensitive commands require a password, referred to as the SIL administrator password.

During installation, the person who installs SIL (such as the system administrator) initialises interactively the SIL administrator password that will be used by the **<SIL_OWNER>**.

Only the **<SIL_OWNER>** and the OS administrator group have full file access permissions to the SIL directory. OS administrator group permissions to execute command line tools are restricted.

The **<SIL_OWNER>** can execute all commands **except** for the following, which require root or administrator privileges:

- `sil setup service create`
- `sil setup service remove`

The SIL interactive console maintains the SIL administrator password for a 12 hour session. This avoids having to type the administrator password each time a command that requires it is run. The inactivity timeout is set to 15 minutes.

How to use the SIL interactive console

You can execute commands in two different ways:

1. Type the command as follows:
`$SIL_HOME\bin\sil <command>`
2. Open a session in the SIL interactive console:
`$SIL_HOME\bin\sil`
`>sil`
`<type your command>`

Note *The `sil` command does not start `sil`.*

The console provides auto-completion for SIL commands. Auto-completion is context-sensitive. It can only auto-complete words that are available in the next level of the command. For example, in the highest level of the interactive console, the letter “s” can be auto-completed to the start, stop, and status commands in the default category, as well as setup, support, and signservice, which are the categories in the next level.

Help function

You can request help by typing `help` or `-help`.

The console displays the following information:

- syntax of the command, including mandatory and optional options
- categories/sub-categories
- actions, options, and argument (if required)
- help text with a description of the category and the command along with the options

The help information is context-sensitive. For example, `setup service -help` displays the actions for the sub-category of service such as create, remove, start, and stop.

Another example is `setup service create -help`, which displays only the option `-instance`.

12.3.2 SIL GUI for Alliance Cloud Configuration

SIL offers a graphical user interface (GUI) for Alliance Cloud.

The SIL administrator (also known as the SIL_Owner) must use the GUI to perform a number of configuration tasks needed to use Alliance Cloud.

Your system administrator must first install SIL with an easy to use installation wizard (see the [Swift Integration Layer 2.4.0 Release Letter](#)). The SIL administrator can then access the SIL GUI to perform the tasks described in this topic (see [Log in to the SIL GUI](#) on page 71).

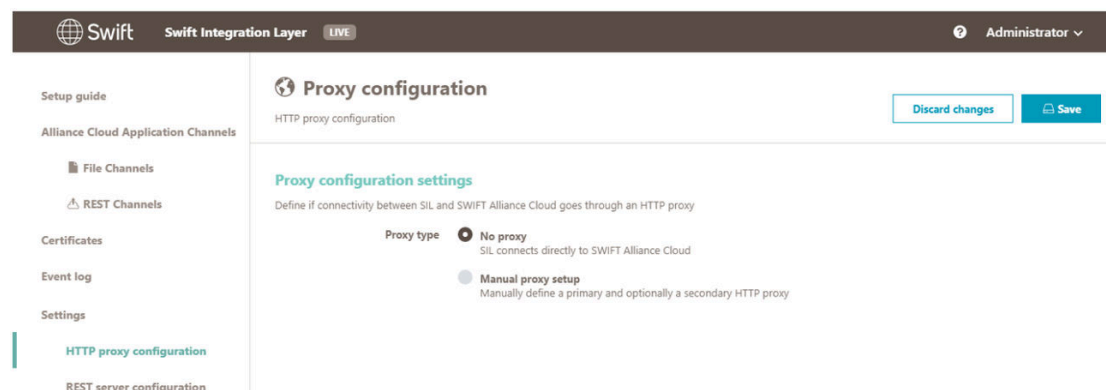
SIL GUI

The GUI is designed to be intuitive and easy to use. Online help is available to guide you through the interface.

The following tasks can be performed in the GUI by the SIL administrator:

- Change the SIL administrator password
- Import token certificates and disk (channel) certificates
- Assign a certificate to a channel
- Renew and delete certificates
- Create and configure File and REST channels
- Configure Local Authentication (LAU), with a choice of a AES-GCM variable or fixed length initialization vector (IV)
The Fixed IV option is compatible with the Alliance Access implementation of AES-GCM LAU.
- Test connectivity and start and stop application channels
- Configure an HTTP proxy (optional)
- View the event log

Example of a GUI screen



12.3.3 Log in to the SIL GUI

SIL offers a graphical user interface (GUI) for Alliance Cloud customers.

Before you begin

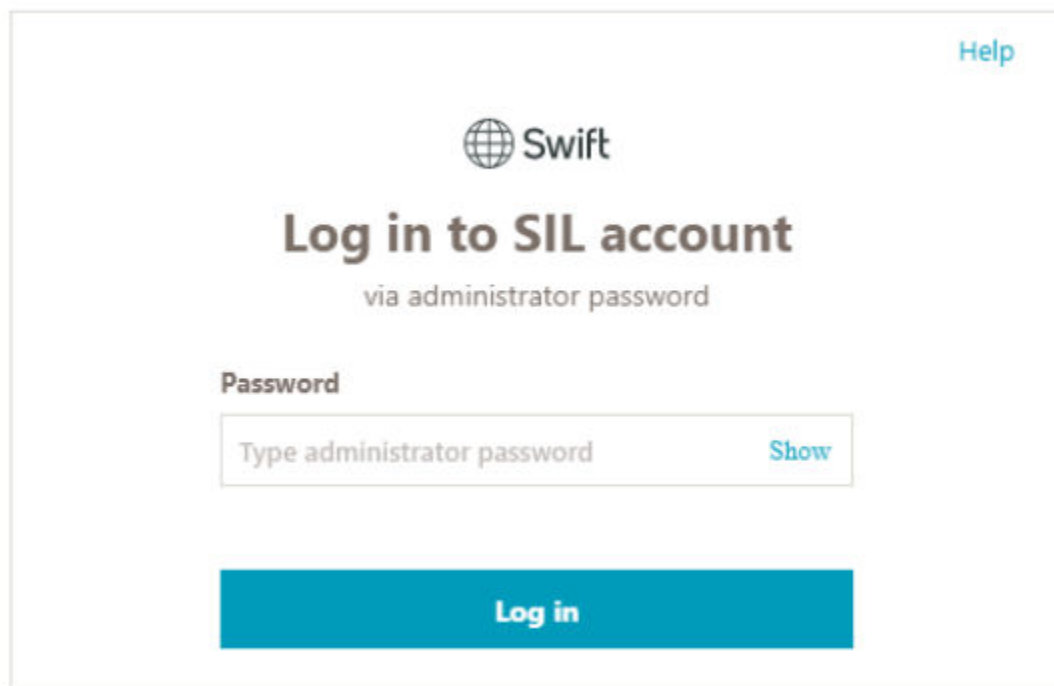
Swift Integration Layer must be installed and started.

You need the SIL administrator password to log in to the SIL GUI.

Procedure

1. There are two ways to log in to the SIL GUI:
 - Type in the URL in your browser.
You can find the URL by using `sil status` command.
 - Use the command `sil startui` to launch the SIL GUI in your browser.

2. Type the administrator password.

A screenshot of the Swift Log in to SIL account interface. The page has a white background with a blue 'Help' link in the top right corner. The Swift logo is centered at the top. Below it, the text 'Log in to SIL account' is displayed in a large, bold, dark blue font, followed by 'via administrator password' in a smaller, lighter blue font. A 'Password' label is positioned above a text input field. The input field contains the placeholder text 'Type administrator password' and a blue 'Show' link on the right. Below the input field is a large blue button with the text 'Log in' in white.

3. You should now be logged in to the GUI.

12.3.4 SIL Base Commands

The SIL base (or root) commands let you start, stop, and retrieve the status of SIL installed components and packages.

Related information

[SIL Command Line Tools](#) on page 69

12.3.4.1 Start SIL

Start SIL with the `sil start` command. If a SIL service was created, then the command starts SIL as a service.

Procedure

1. Execute the command using the SIL interactive console or by typing the full command. See [How to use the SIL interactive console](#) on page 70.
2. Run the following command:

```
sil start
```

SIL checks if the operating system on which SIL is trying to start corresponds to one of the values in the licence file.

SIL contains a default licence for Alliance Cloud customers.

The state of each package and component is preserved each time SIL is started. Starting SIL causes all packages and components that were in the STARTED state to be automatically started.

This also means that SIL can be in the STARTED state while a package is FAILED.

12.3.4.2 Stop SIL

Stop SIL with the `sil stop` command. If a SIL was started as a service, then the command stops the SIL service.

Procedure

1. Execute the command using the SIL interactive console or by typing the full command. See [How to use the SIL interactive console](#) on page 70.
2. Run the following command:

```
sil stop
```

If SIL is in the process of being stopped, then all components and packages are automatically stopped. The state of each component and package before the platform stop is preserved when the platform is restarted.

12.3.4.3 SIL Status

Display the status of SIL, installed packages, SIL components, trace log activation state, e-mail notifications activation state, and event log format and levels with the `sil status` command.

Procedure

1. Execute the command using the SIL interactive console or by typing the full command. See [How to use the SIL interactive console](#) on page 70.
2. Run the following command:

```
sil status
```

If SIL is stopped, then the status command returns the status of SIL only. The status of packages and components are only returned if SIL is started.

SIL statuses

Status	Description
STARTED	SIL is started. SIL is considered as STARTED when the SIL framework is loaded. The components and packages then start and have their own life cycle. For example, this means that SIL can be STARTED while a package is in state FAILED . If SIL is started as a service, then the service name also appears.
PARTIALLY STARTED	SIL is started but some packages or components failed to start.
STOPPED	SIL is not started.
FAILED	SIL, or a SIL component or package has failed.
STARTING	SIL is starting.
STOPPING	SIL is stopping.

Components statuses

Status	Description
NOT CONFIGURED	A component is installed but is not configured.
STARTED	A component is started.

Status	Description
PARTIALLY_STARTED	SIL is started but some components failed to start.
STOPPED	A component is configured, but it is not started.
FAILED	A component has failed.
STARTING	The component is starting.
STOPPING	The component is stopping.

Packages statuses

Status	Description
STARTED	The package is started.
STOPPED	The package is installed but is not started.
FAILED	The package could not be started.
STARTING	The package is starting.
STOPPING	The package is stopping.
INSTALL_FAILED	The package installation failed.
NOT_LICENSED	The package is not associated to a runtime licence. You must uninstall and install the package.
FRAGMENT_RESOLVED	When a bundle of type FRAGMENT (a type of bundle that makes its contents available to another bundle) is being installed, it stays in the FRAGMENT_RESOLVED state of an OSGi lifecycle. Therefore, it cannot be started or stopped.
WAITING_DEPENDENCIES	The package has been successfully installed but depends on other packages that have not been installed yet.

Monitoring statuses

Name	Status
Trace log	ON OFF
E-mail notification	ON OFF threshold value
Event log	ON OFF threshold value

12.3.5 Alliance Cloud Commands

The commands in the Alliance Cloud category let you start and stop the application channels and display the status.

All configuration tasks for Alliance Cloud must be done using the GUI. See [SIL GUI for Alliance Cloud Configuration](#) on page 70.

12.3.5.1 Sample Files to Implement LAU Signature for Alliance Cloud

SIL supports the use of the AES-GCM cryptographic standard as a Local Authentication (LAU) mechanism. LAU offers integrity and authenticity for traffic that is exchanged between two entities (for example between SIL and the back office).

To help customers implement the LAU signature when using SIL in Alliance Cloud, a zipped LAU verification tool and two sample code files are available.

After you have installed SIL, these two files will be available in the `$SIL_HOME/samples/sil-alliancecloud-lau-sample/` directory:

- **LauUtils.java**
Provides various functions to help implementation of SIL Alliance Cloud LAU (signature and encryption).
- **SampleApplication.java**
Sample class that shows full LAU usage (encryption and decryption, for files and in-memory payloads), using functions from LauUtils.

The LAU tool contains the following:

- executable scripts for encryption and decryption
Windows: `lau-cli-encrypt.cmd` and `lau-cli-decrypt.cmd`
Linux: `lau-cli-encrypt` and `lau-cli-decrypt`
- a java archive to be launched by the scripts
- a readme document to explain how the tool functions

Copyright of source code

Swift owns the copyright on the source code samples provided with SIL, and grants the customer a right to copy, use, and adapt them for the purpose of implementing integration flow using SIL.

You may use, copy, adapt this source code sample for the purpose of implementing the LAU signature between your back-office application and SIL.

Swift provides these source code samples for the customer's convenience, and does not guarantee completeness, fitness for a particular purpose, frequency of updates, ease of maintenance, or absence of errors.

12.3.5.2 Application Channels in SIL

Each SIL instance can have multiple application channels.

Your institution's security officers must first create and authorise a DN in SwiftNet Online Operations Manager for each application channel. The Message management administrator must then create the application channels in the Alliance Cloud.

The BIC component of the DN must be in the list of BICs of the Alliance Cloud business entity.

As an application channel is identified by a Distinguished Name, the DNs created by the security officers are used as the identifiers of the application channels. Each application channel configured in SIL corresponds to an application channel defined in the Alliance Cloud Admin centre module by the Message management administrator. They must both have the same DN.

12.3.5.2.1 Start an Application Channel

Start one or all application channels of the Alliance Cloud component with the `sil alliancecloud start` command.

You can also start an application channel in the SIL GUI. See [Log in to the SIL GUI](#) on page 71.

Before you begin

- You must be the SIL administrator (SIL_Owner) to run this command.
- The Alliance Cloud component must be running.

Procedure

1. Execute the command using the SIL interactive console or by typing the full command. See [How to use the SIL interactive console](#) on page 70.
2. Run one of the following commands:

Command	Description
<code>sil alliancecloud start [-channel <distinct name> <index>]</code>	To start one specific application channel
<code>sil alliancecloud start -channel all</code>	To start all application channels

Certain directories are automatically created:

Emission flow

- archive: messages that were successfully sent
- emission: messages that must be sent
- error: messages that failed to be sent
- in_progress: messages being sent

Reception flow

- reception: messages, delivery reports, and transmission reports that were received
- temp: messages, delivery reports, and transmission reports that are being received

12.3.5.2.2 Stop an Application Channel

Stop one or all application channels of the Alliance Cloud component with the `sil alliancecloud stop` command.

You can also stop an application channel in the SIL GUI. See [Log in to the SIL GUI](#) on page 71.

Before you begin

- You must be the SIL administrator (SIL_Owner) to run this command.
- The Alliance Cloud component must be running.

Procedure

1. Execute the command using the SIL interactive console or by typing the full command. See [How to use the SIL interactive console](#) on page 70.
2. Run one of the following commands:

Command	Description
<code>sil alliancecloud stop [-channel <<i>distinguished name</i>> <<i>index</i>>]</code>	To stop one specific application channel
<code>sil alliancecloud stop -channel all</code>	To stop all application channels

12.3.5.2.3 Display the Alliance Cloud Component and Application Channel Status

Display the status of the Alliance Cloud component and of the application channels with the `sil alliancecloud status` command.

You can also view the status of an application channel in the SIL GUI. See [Log in to the SIL GUI](#) on page 71.

Procedure

1. Execute the command using the SIL interactive console or by typing the full command. See [How to use the SIL interactive console](#) on page 70.
2. Run the following command:

```
sil alliancecloud status
```

The status of an application channel displays the following elements:

- an index
- application channel name
- status of the emission and reception flow

12.3.6 SIL Support Commands

The commands in the SIL Support category let you retrieve the SIL release version, collect configuration and logging information, and split the Support Info File.

Related information

[SIL Command Line Tools](#) on page 69

12.3.6.1 Collect Support Info

Use the `sil support collectinfo` command to collect configuration and logging information on the SIL host, in the form of a zip file. This operation is usually run when you need to send the .zip file to Swift Support to investigate a problem.

Procedure

1. Execute the command using the SIL interactive console or by typing the full command. See [How to use the SIL interactive console](#) on page 70.
2. Run the following command:

```
sil support collectinfo -file <file name> | -dir <directory> [-from  
<yyyymmdd'T'HHmmss>] [-includepackages]
```

Parameter	Description
-file <file name>	The file name and the directory in which the .zip file is to be created. If the .zip extension is not specified manually in the file name, then it is automatically added to the file.
-dir <directory>	The directory in which the support info zip file is to be created The filename of the zip file is in the following format sil_supportinfo_<yyyymmdd-hhmm>.zip where <yyyymmdd-hhmm> is the time the command runs.
-from <yyyymmdd'T'HHmmss>	Optional Use this option to filter out log files that have been modified before the date in the parameter, thereby removing old data from the support information archive. If you do not use this option, then logs of the current day and previous days are taken into account.
-includepackages	Optional Use this option to gather information about installed packages (OSGi bundles and resources), and related configuration details. Components and configuration details, such as the Sign Service and Lite2 are automatically included in the support info archive with or without the -includepackages option. If you do not use this option, then client-related information, such as installed OSGi bundles / resources and related specific configuration, is not added to the support info archive.

The zip file include all logs and configuration files with the encrypted sensitive information. It also includes the SIL Instance ID, the SIL licence file, and the runtime licence associations (provided the -includepackages option is used). Keystores are not embedded.

12.4 Use Active/Standby for SIL Instances

This topic describes how to fail over to a standby instance.

This feature is only available for Alliance Cloud customers.

When two or more SIL instances are installed in an active/standby set-up and an active instance becomes unavailable, you can fail over to a standby instance.

Before you begin

Decide on the number of SIL instances that you need to install. Only one instance can be active, but you can configure multiple standby instances. In the following example, there is only one standby instance. Simply repeat these steps if you need additional standby instances.

At least two SIL instances must be installed and correctly configured:

- Only one SIL instance must be active.
An *active-active* set-up is not supported at this time.
- When the need arises to fail over to the standby SIL instance, the failed active SIL must be stopped before starting the standby instance. See below for details.
- The SIL instances must share the same common DN.

Important If you are using multiple application channels, then you must use certificates with the same common DN for the same type of application channel.

- The application channels in the SIL GUI must be configured using equivalent DNs. Equivalent DNs use a naming scheme that makes the differences between the two DNs transparent to the application. Equivalent certificates must have the same Role-Based Access Control (RBAC) roles.
- In the Alliance Cloud Admin centre module, the Message management administrator must configure the application channels **using the Common DN (ignoring the numbered common name segment)**.

To use DN equivalence, type a % followed by one or two digits in the **Name** field. For example, %01.

Example of DN equivalence

If you want to set up two application channels, then the following DNs can be used to set up the application channels on two SIL instances:

DN application channel 1	cn=%01,cn=appch1,cn=<server-x>,o=bankbebb,o=swift cn=%02,cn=appch1,cn=<server-x>,o=bankbebb,o=swift
DN application channel 2	cn=%01,cn=appch2,cn=<server-x>,o=bankbebb,o=swift cn=%02,cn=appch2,cn=<server-x>,o=bankbebb,o=swift

Procedure

1. **The following steps describe how to install the active and standby SIL instances:**

1. Install and configure the first SIL instance that will be the standby instance. See the appropriate [Swift Integration Layer Release Letter](#).
2. Test the connectivity between the first instance (standby) and Alliance Cloud using the SIL GUI. See [Log in to the SIL GUI](#) on page 71.
3. Stop the standby instance using the command `sil stop`.
4. Install and configure the second SIL instance that will be the active instance. See the appropriate [Swift Integration Layer Release Letter](#).
5. Test the connectivity between the second (active) instance and Alliance Cloud using the SIL GUI. See [Log in to the SIL GUI](#) on page 71.

2. **The following steps describe how to fail over to a standby instance:**

6. Stop the active SIL instance using the command `sil stop`.
7. Start the standby SIL instance, which becomes the new active instance using the command `sil start`.

For File channels, go to step [8](#) on page 80. For REST channels, go to step [10](#) on page 80.

3. **Specific steps to be taken for File application channels:**

8. For the **emission** flow (outgoing messages), the back office must do the following:
 - a. Re-send all messages that have not been ACKed by the failed active SIL instance to the new active instance.
 - b. From this point on, the back office must send all new messages to the emission directories of the new active SIL.
9. For the **reception** flow (incoming messages), the back office must do the following:
 - a. Process all remaining messages in the reception directory of the failed SIL instance.
 - b. From this point on, use the application channel reception directories of the standby SIL, which becomes the active instance.

Messages in the **temp** directory will be downloaded again with .pdr by the standby SIL. The extension .pdr indicates that retries occurred during the message download.

4. **Specific steps to be taken for REST application channels:**

10. For the **emission** flow (outgoing messages), the back office must do the following:
 - a. Send a post API call for messages for which an HTTP response was not received to the HTTP endpoint of the standby SIL. See "REST Channel Reception Flow" in the [Alliance Cloud Operations Guide](#).
 - b. Provide new messages to the HTTP endpoint of the standby SIL only.
11. For the **reception** flow (incoming messages), the back office must do the following:
 - a. Download messages again, for which an HTTP response was not received, from the HTTP endpoint of the standby SIL.
 - b. Use only the HTTP endpoint of the standby SIL.
 - c. For messages that were downloaded but not confirmed or rejected by the back-office application:
 - The back-office application can retry to confirm or reject the messages.
 - If not, then the back office will automatically download these messages again. See "REST Channel Reception Flow" in the [Alliance Cloud Operations Guide](#).

12.5 Test SIL Connectivity with Alliance Cloud

After you create an application channel in the Swift Integration Layer (SIL) GUI, click Test Connectivity to test the connectivity from SIL to Alliance Cloud.

If SIL cannot successfully connect to Alliance Cloud, then follow the instructions in this topic.

Before you begin

Read [Swift Integration Layer \(SIL\) Installation and Configuration Tasks](#) on page 66.

Procedure

1. Verify authentication with the Swift API Gateway and connectivity between SIL and Alliance Cloud.
 - a. Check the allowable downtime window (ADW) for Alliance Cloud. See [Operational Status](#).
 - b. *For MV-SIPN connectivity only:* make sure that the DNS server is correctly installed and configured. See the appropriate Knowledge Base article:
For Windows: [5018095](#)

For Red Hat Enterprise Linux: [5016788#unixdns](#)

Several options are available including:

- c. Make sure that SIL can reach Swift services over the MV-SIPN connection. To do so, execute the `nslookup` command. For more information, see the **Resolution** section in the case manager article [SIL unable to connect to Alliance Cloud](#).
 - d. Make sure firewall settings are correctly configured. See the entry for the **API Gateway** in [SIL and Alliance Cloud Connectors to Swift Connectivity](#) on page 97.
2. Make sure that the application channel exists in Alliance Cloud.
 - a. Make sure that the correct Distinguished Name (DN) is assigned to the application channel.

The Message management administrator creates the application channel or channels in Alliance Cloud Admin centre.

Each application channel is composed of a name and an optional description. It is identified by a Distinguished Name (DN) created by your security officers in O2M. See [Add an Application Channel in Alliance Cloud](#) on page 64.
 - b. If your institution plans to use the active/standby feature for SIL instances, then you must create the application channels **using the Common DN used in O2M (ignoring the numbered common name segment, such as %1)**.
 - c. Read the article [Alliance Cloud - Unable to start Application Channel \(File/Rest channel\)](#).
 3. Make sure that the application channel is active in Alliance Cloud.
 - a. When you have configured the application channel in Alliance Cloud, you can decide to create it with an **Inactive** status (click [Create as inactive](#)) or to create it and activate it immediately (click [Create & activate](#)). Activation of an application channel always requires approval from another user.
 - b. An application channel with an **Active** status allows SIL to connect to the Alliance Cloud platform to start exchanging traffic.

For more information, see the [Alliance Cloud Operations Guide](#).

13 Alliance Cloud MQ Connector Installation and Configuration Tasks

The Alliance Cloud MQ Connector enables customers to set up IBM MQ queues to exchange FIN and InterAct messages with Alliance Cloud.

The system administrator installs the MQ Connector alongside the lightweight footprint (Swift Microgateway).

The MQ Connector administrator is a different person who performs the Alliance Cloud MQ Connector configuration-related tasks.

Application channels are needed to exchange messages with Alliance Cloud. Application channels require a certificate. This certificate is used to secure the connection to Alliance Cloud.

For the MQ Connector, this certificate must be stored as a channel certificate (multi-vendor secure IP network (MV-SIPN)).

The MQ Connector administrator must not be a part of the Windows administrator group.

The MQ Connector administrator must liaise with the security officers, the Swift Microgateway administrator, and the Message management administrator to complete some of the tasks described in this section.

☒ Click [here](#) to go to the Getting Started checklist.

Note *Currently PDFs and message archives are not supported by the Alliance Cloud MQ Connector.*

Alliance Cloud MQ Connector Installation Tasks

The system administrator performs the following tasks:

- Download the latest version of the Alliance Cloud MQ Connector and the Swift Microgateway from the [Download Centre](#).
You can do so only after receiving an e-mail from Swift that confirms that Alliance Cloud has been provisioned for your institution.
- Ensure critical tasks have been completed, such as Java Keystore, including the required Java version or API Gateway certificate on the Swift Microgateway UI).
- Install the Alliance Cloud MQ Connector and the Swift Microgateway on your premises. See the MQ Connector [Release Letter](#) and the Swift Microgateway [Installation Guide](#).
- Provide the MQ Connector administrator with the MQ Connector administrator password (initialised during installation). Ideally, the MQ Connector administrator will be with you during the installation. The MQ Connector administrator needs this password to log in to the MQ Connector GUI.
For more information about the Swift Microgateway, see the [Developer Portal](#).

Prerequisites for the MQ Connector administrator

Make sure that the following tasks are completed before you configure the Alliance Cloud MQ Connector GUI:

- Your security officers must create and authorise a Distinguished Name (DN) in SwiftNet Online Operations Manager (O2M) for each application channel in the MQ Connector.
For the MQ Connector, when security officers create the DN for the application channel, they must select the Certificate Class for the DN: Channel (for a channel certificate).

Important If your institution plans to use the active/standby feature for MQ Connector instances, then the application channels must be created using equivalent DNs. Make sure that your institution's security officers know about the decision to use this feature before they create the DNs in O2M. See [Use Active/Standby for MQ Connector Instances](#) on page 83.

- The Message management administrator must create the application channels in the Alliance Cloud Admin centre.
-

Important If you are using multiple application channels, then the Message management administrator must configure the application channels using the Common DN (ignoring the numbered common name segment (for example, cn=%01).

- Your security officers must provide you with the pair of activation secrets generated by O2M during the DN creation process. The Swift Microgateway administrator needs these secrets to download the channel certificate into the lightweight footprint.
- In O2M, your security officers must assign to the application channel DNs the **access_to_service** RBAC role, which is under the **swift.alliancecloud.sil** service for Live.
- Your MQ Administrator must provide the keystore where certificates used to configure the TLS are stored. This keystore must be in or converted into PKCS12 format. The password of this keystore must be provided as well.

Alliance Cloud MQ Connector configuration tasks

The Alliance Cloud Cloud MQ Connector administrator performs the following tasks:

- Access the Alliance Cloud MQ Connector using the GUI. The MQ Connector administrator password is needed to log in to the GUI.
- Set up the connectivity to the MQ server manually or using CCDT files.
- Assign valid certificates to MQ application channels during its creation.
- Manage (create, edit, delete) MQ application channels and the subsequent emission and reception destinations.
- Start and stop the fully configured MQ application channels to enable the flow of messages between back-office applications and Alliance Cloud.

For more information about how to perform these tasks, see "Configuring the MQ Connector GUI" in the [Alliance Cloud Operations Guide](#).

13.1 Use Active/Standby for MQ Connector Instances

This topic describes how to fail over to a standby instance.

This feature is only available for Alliance Cloud customers.

When two or more MQ Connector instances are installed in an active/standby set-up and an active instance becomes unavailable, you can fail over to a standby instance.

Only one instance can be active, but you can configure multiple standby instances. In the following example, there is only one standby instance. Simply repeat these steps if you need additional standby instances.

- Only one MQ Connector instance must be active at each moment in time: An active-active set-up is not supported at this time.
- When the need arises to fail over to the standby MQ Connector instance, the failed active MQ Connector must be stopped before starting the standby instance.

- The MQ Connector instances must share the same common DN.

Important If you are using multiple application channels, then you must use certificates with the same common DN for the same type of application channel.

- The MQ application channels in the MQ Connector GUI must be configured using equivalent DNs. Equivalent DNs use a naming scheme that makes the differences between the two DNs transparent to the application. Equivalent certificates must have the same Role-Based Access Control (RBAC) roles.
- In the Alliance Cloud Admin centre module, the Message management administrator must configure the application channels **using the Common DN (ignoring the numbered common name segment)**. To use DN equivalence, type a % followed by one or two digits in the Name field. For example, %01.

Example of DN equivalence

If you want to set up two application channels, then the following DNs can be used to set up the application channels on two MQ Connector instances:

DN application channel 1	cn=%01,cn=appch1,cn=<server-x>,o=bankbebb,o=swift cn=%02,cn=appch1,cn=<server-x>,o=bankbebb,o=swift
DN application channel 2	cn=%01,cn=appch2,cn=<server-x>,o=bankbebb,o=swift cn=%02,cn=appch2,cn=<server-x>,o=bankbebb,o=swift

14 Swift Messaging API Tasks

Alliance Cloud offers a REST API, which serves as a bidirectional connector for API clients to exchange messages with Alliance Cloud, using REST endpoints.

Upload and download endpoints are available per Swift service.

For more information, see the [Swift Messaging API Getting Started](#).

15 Message Management Operator Tasks

Message management operators perform specific tasks in Message management based on the role assigned to them. These tasks can include manually creating messages and message templates, viewing and searching for messages, redistributing message manually to the back office, repairing messages, and approving messages before they are sent to Swift.

☑ Click [here](#) to go to the Getting Started checklist.

Prerequisites

Before you can log in to Alliance Cloud, make sure that the following tasks are completed:

1. To access the Swift Certificate Centre, make sure that one of your colleagues, such as your system administrator, has installed the Swift Personal Token Software (available on the [Download Centre](#)) **and** SConnect on the PC where you will use the Swift personal token. These are one-off tasks that must be completed to have the necessary software to connect, configure, and to read the certificates on personal tokens.
2. Ask your security officers for your initial token password and the activation code.
3. Make sure that your security officers have assigned the **user** RBAC role to you (and approved it) in the SwiftNet Online Operations Manager (O2M). RBAC means "Role-Based Access Control" and determines what a certificate is allowed to access.
4. Activate your token on the [Swift Certificate Centre](#). See [Activate Token](#) on page 53.
5. Make sure that an Alliance Cloud administrator has created you as a user and has assigned the **Message management operator** role to you.
6. Insert your activated token into an appropriate USB port of your PC. Make sure that you have the password that you created during the activation process.
7. Log in to Alliance Cloud:
Live environment: <https://swift-alliancecloud.browse.swiftnet.sipn.swift.com>
Test environment: <https://swift-alliancecloud-test.browse.swiftnet.sipn.swift.com>

Message management operator tasks

If you have questions when doing the following tasks, then help is available after you log in. Just click the [?](#).

In Message management, you will be able to do the following tasks.

- manually create messages
- repair messages
- verify messages
- view messages
- search for messages
- create and use message templates
- export messages
- build your searches and save them in your favourites
- configure your preferences
- change the status of a message
- redistribute message manually to the back-office
- final approve a message before it is sent to Swift
- test messages for the upcoming Standards Release (see [Future mode](#) on page 118)

Token renewal

Your token certificate is valid for two years.

Make sure that you renew your token certificate in the Swift Certificate Centre before its expiry date. If you do not renew the certificate in time, then your security officer must reset the token. See "Renew Token Certificate" in the [Alliance Cloud Operations Guide](#).

See also Knowledge Base article [5020138](#) **How to verify the expiration date of a certificate on a token.**

Related information

[Message Creation, Verification, Repair, and Approval](#) on page 116

[Message management User Guide](#)

16 Event Log Administrator Tasks

The Event log is used to view and investigate events that occurred in the Admin centre and Message management modules.

The Event log administrator must liaise with the security officers and the User and Role administrator to complete some of the tasks described in this section.

☒ Click [here](#) to go to the Getting Started checklist.

Prerequisites

Before you can log in to Alliance Cloud, make sure that the following tasks are completed:

1. To access the Swift Certificate Centre, make sure that one of your colleagues, such as your system administrator, has installed the Swift Personal Token Software (available on the [Download Centre](#)) **and** SConnect on the PC where you will use the Swift personal token. These are one-off tasks that must be completed to have the necessary software to connect, configure, and to read the certificates on personal tokens.
2. Ask your security officers for your initial token password and the activation code.
3. Make sure that your security officers have assigned the **user** RBAC role to you (and approved it) in the SwiftNet Online Operations Manager (O2M). RBAC means "Role-Based Access Control" and determines what a certificate is allowed to access.
4. Activate your token on the [Swift Certificate Centre](#). See [Activate Token](#) on page 53.
5. Make sure that an Alliance Cloud administrator has created you as a user and has assigned the **Event log viewer** role to you, which gives you the permissions to view the Event log.
6. Insert your activated token into an appropriate USB port of your PC.
Make sure that you have the password that you created during the activation process.
7. Log in to Alliance Cloud:

Live environment: <https://swift-alliancecloud.browse.swiftnet.sipn.swift.com>

Test environment: <https://swift-alliancecloud-test.browse.swiftnet.sipn.swift.com>

Event log administrator tasks

If you have questions when doing the following tasks, then help is available after you log in. Just click the [?](#).

1. Click on the Event log module.
2. Verify that audit logs have been created for previous actions.

Token renewal

Your token certificate is valid for two years.

Make sure that you renew your token certificate in the Swift Certificate Centre before its expiry date. If you do not renew the certificate in time, then your security officer must reset the token. See "Renew Token Certificate" in the [Alliance Cloud Operations Guide](#).

See also Knowledge Base article [5020138](#) **How to verify the expiration date of a certificate on a token.**

17 Relationship Management Portal Tasks

The Relationship Management Portal is a central application managed by Swift, which centrally records and enforces pre-agreed relationships between correspondents.

It enables institutions to view, create, store, and manage pre-agreed relationships with their correspondents.

Users can access the portal through a direct link or from the Alliance Cloud GUI.

Your institution's security officers must assign and approve the appropriate [RMA RBAC roles](#) to users in your institution in the SwiftNet Online Operations Manager (O2M).

Important Local RMA management applications can be used only to create *local authorisations*. For more information, see [RMA Evolution Frequently Asked Questions](#).

Related information

[Assign RBAC Roles](#) on page 46

[Relationship Management Portal Getting Started](#)

[Relationship Management Portal User Guide](#)

17.1 Relationship Management (RMA) Administrator Tasks

Users who are assigned the RMA *admin* RBAC role in the SwiftNet Online Operations Manager can run reports about authorisations and set up and manage RMA distribution files subscriptions in the Relationship Management Portal (RMA Portal).

The RMA administrator must liaise with the security officers to complete some of the tasks described in this section.

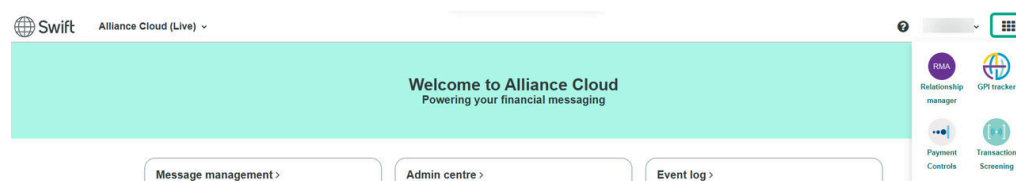
Prerequisites

1. To access the Swift Certificate Centre, make sure that one of your colleagues, such as your system administrator, has installed the Swift Personal Token Software (available on the [Download Centre](#)) **and** SConnect on the PC where you will use the Swift personal token. These are one-off tasks that must be completed to have the necessary software to connect, configure, and to read the certificates on personal tokens.
2. Ask your security officers for your initial token password and the activation code.
3. Make sure that your security officers have assigned and approved the following RBAC roles to you in the SwiftNet Online Operations Manager (O2M). RBAC means "Role-Based Access Control" and determines what a certificate is allowed to access.
 - **user** (only if you need to access Alliance Cloud)
 - the **admin** RBAC role for the RMA Portal (see [Role-Based Access Control Requirements](#) in the [Relationship Management Portal Getting Started](#))
4. Activate your token on the [Swift Certificate Centre](#). See [Activate Token](#) on page 53.
5. Insert your activated token into an appropriate USB port of your PC. Make sure that you have the password that you created during the activation process.
6. Access the Relationship Management Portal directly or through Alliance Cloud:
 - **Relationship Management Portal**
Live environment: <https://rma-portal.browse.swiftnet.sipn.swift.com>
Pilot environment: <https://rma-portal-pilot.browse.swiftnet.sipn.swift.com>

- **Alliance Cloud**

Live environment: <https://swift-alliancecloud.browse.swiftnet.sipn.swift.com>

Test environment: <https://swift-alliancecloud-test.browse.swiftnet.sipn.swift.com>



RMA administrator tasks

For more information about how to run reports and set up and manage RMA distribution files subscriptions, see the [Relationship Management Portal Getting Started](#) and the [Relationship Management Portal User Guide](#).

Token renewal

Your token certificate is valid for two years.

Make sure that you renew your token certificate in the Swift Certificate Centre before its expiry date. If you do not renew the certificate in time, then your security officer must reset the token. See "Renew Token Certificate" in the [Alliance Cloud Operations Guide](#).

See also Knowledge Base article [5020138](#) **How to verify the expiration date of a certificate on a token.**

17.2 Relationship Management (RMA) Operator Tasks

Users who are assigned the RMA *operator* RBAC role in the SwiftNet Online Operations Manager can create, modify, activate, reject, delete, and revoke authorisations in the Relationship Management Portal (RMA Portal). They can also create and manage communications.

Prerequisites

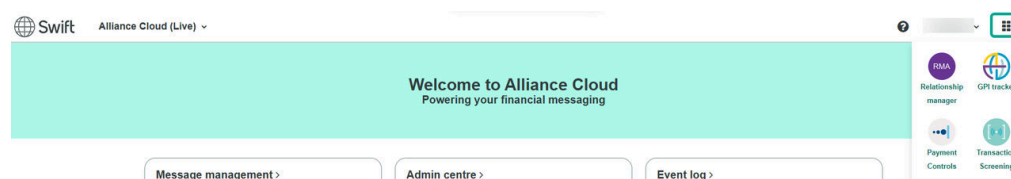
1. To access the Swift Certificate Centre, make sure that one of your colleagues, such as your system administrator, has installed the Swift Personal Token Software (available on the [Download Centre](#)) **and** SConnect on the PC where you will use the Swift personal token. These are one-off tasks that must be completed to have the necessary software to connect, configure, and to read the certificates on personal tokens.
2. Ask your security officers for your initial token password and the activation code.
3. Make sure that your security officers have assigned and approved the following RBAC roles to you in the SwiftNet Online Operations Manager (O2M). RBAC means "Role-Based Access Control" and determines what a certificate is allowed to access.
 - **user** (only if you need to access Alliance Cloud)
 - the **operator** RBAC role for the RMA Portal (see [Role-Based Access Control Requirements](#) in the [Relationship Management Portal Getting Started](#))
4. Activate your token on the [Swift Certificate Centre](#). See [Activate Token](#) on page 53.
5. Insert your activated token into an appropriate USB port of your PC. Make sure that you have the password that you created during the activation process.
6. Access the Relationship Management Portal directly or through Alliance Cloud:
 - **Relationship Management Portal**
Live environment: <https://rma-portal.browse.swiftnet.sipn.swift.com>

Pilot environment: <https://rma-portal-pilot.browse.swiftnet.sipn.swift.com>

- **Alliance Cloud**

Live environment: <https://swift-alliancecloud.browse.swiftnet.sipn.swift.com>

Test environment: <https://swift-alliancecloud-test.browse.swiftnet.sipn.swift.com>



RMA operator tasks

In the Relationship Management Portal, you can do the following tasks.

- create authorisations to receive traffic from your correspondents
- modify authorisations
- activate and reject authorisations to send from your correspondents
- revoke authorisations, meaning that you withdraw from your correspondent the permission to send you messages
- create and manage communications between your institution and correspondents

For more information, see the [Relationship Management Portal User Guide](#).

Token renewal

Your token certificate is valid for two years.

Make sure that you renew your token certificate in the Swift Certificate Centre before its expiry date. If you do not renew the certificate in time, then your security officer must reset the token. See "Renew Token Certificate" in the [Alliance Cloud Operations Guide](#).

See also Knowledge Base article [5020138](#) **How to verify the expiration date of a certificate on a token.**

18 Set up the Environment for Alliance Cloud

Your system administrator or staff responsible for the Swift installation must perform the following tasks, as appropriate.

☒ Click [here](#) to go to the Getting Started checklist.

1. Review the appropriate operating system requirements:
 - Swift Integration Layer
See the [Swift Integration Layer 2.4.0 Release Letter](#)
 - Swift Microgateway
See the Swift Microgateway *Getting Started Guide*, available on the [Swift Developer Portal](#) > Additional information section.
2. Check with your network administrator which ports can be used by Swift Integration Layer for automatic flows. See [Port Availability](#) in the *Swift Integration Layer 2.4.0 Release Letter*. For the Alliance Cloud Connectors, see "Port Availability" in the appropriate release letter under [Alliance Cloud Connectors](#).
3. Review the qualified web browsers for Alliance Cloud. See [Web Browser Configuration](#) on page 92.
4. Read about [TLS Security](#) on page 93.
5. *Optional*: order MV-SIPN (multi-vendor secure IP network).
Alliance Connect products are network connectivity products that offer a permanent connection to SwiftNet through the public Internet or the managed backbone of a Swift Network Partner.
For more information, visit [swift.com](#). To order, go to [swift.com](#) > [Ordering](#).
6. *For MV-SIPN connectivity only*: Install and configure the DNS server. See the appropriate Knowledge Base article:
For Windows: [5018095](#)
For Red Hat Enterprise Linux: [5016788#unixdns](#)
Several options are available including:
 - install a DNS server on each workstation
 - install a DNS server on one workstation and point other workstations to this workstation
 - deploy a central DNS serverSwift recommends that you discuss the DNS flow deployment with your internal IT department.
7. Configure the firewalls to allow the appropriate IP addresses and ports. See [Configure Firewall Settings](#) on page 93.
8. Install the Personal Token Software on all PCs on which a Swift personal token will be used for Alliance Cloud. See [Install Token Software](#) on page 98.
This is a one-off procedure that you must complete to have the necessary software to configure and to read the certificates on Swift personal tokens.
9. Install SConnect on all PCs on which a Swift personal token will be used for Alliance Cloud. SConnect is a browser extension that enables applications and websites to communicate with tokens. To connect to an application with a token, installation is required.
For installation instructions, see [SConnect Installation Methods](#) in the *SConnect Installation Guide*.

18.1 Web Browser Configuration

Alliance Cloud has been qualified using the English language version of the following browsers:

- Google Chrome

- Microsoft Edge
- Mozilla Firefox

Swift no longer recommends the use of Internet Explorer.

Browser	Recommended browser version	Network connectivity	
		MV-SIPN	Internet
Google Chrome	Latest "stable" version	x	✓
Microsoft Edge (Chromium)	For more information, see the website for the browser.	x	✓
Microsoft Edge (IE mode)		✓	✓
Mozilla Firefox	Latest "stable" version • <i>Firefox for Desktop</i> is automatically updated to the latest version. • <i>Firefox for Enterprise</i> follows the release calendar and the Extended Support Release (ESR) cycle.	✓	✓

SConnect must be installed on all PCs on which a Swift personal token will be used. To view the qualified operating systems, see the [Swift Certificate Centre - SConnect Installation Guide](#).

For Firefox, see [Install SConnect for Mozilla Firefox](#) in the *SConnect Installation Guide*.

See also "Web Browser Configuration" in the [Swift Integration Layer 2.4.0 Release Letter](#).

✓ Click [here](#) to go to the Getting Started checklist.

18.2 TLS Security

Transport Layer Security (TLS)-intercepting security solutions may prevent connection to some Swift services, especially the services that rely on personal tokens for mutual authentication. These solutions must not interrupt the TLS flow for Swift services.

18.3 Configure Firewall Settings

Alliance Cloud customers must configure the firewall settings between the Alliance Cloud users' computer and the Internet or the multi-vendor secure IP network (MV-SIPN) and between the server on which Swift Integration Layer is installed to connect to Alliance Cloud and the Internet or the multi-vendor secure IP network (MV-SIPN).

✓ Click [here](#) to go to the Getting Started checklist.

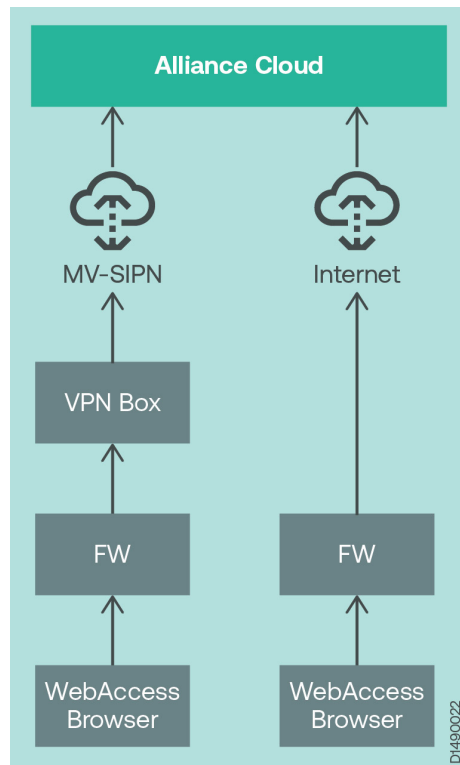
Firewall security

For services to function correctly, the firewall must allow outgoing TCP connections to the URLs or IP addresses listed in this section. Systems using channel or token-based certificates require these connections.

Note *No incoming connections are required. Swift recommends that users block all incoming connections from the internet.*

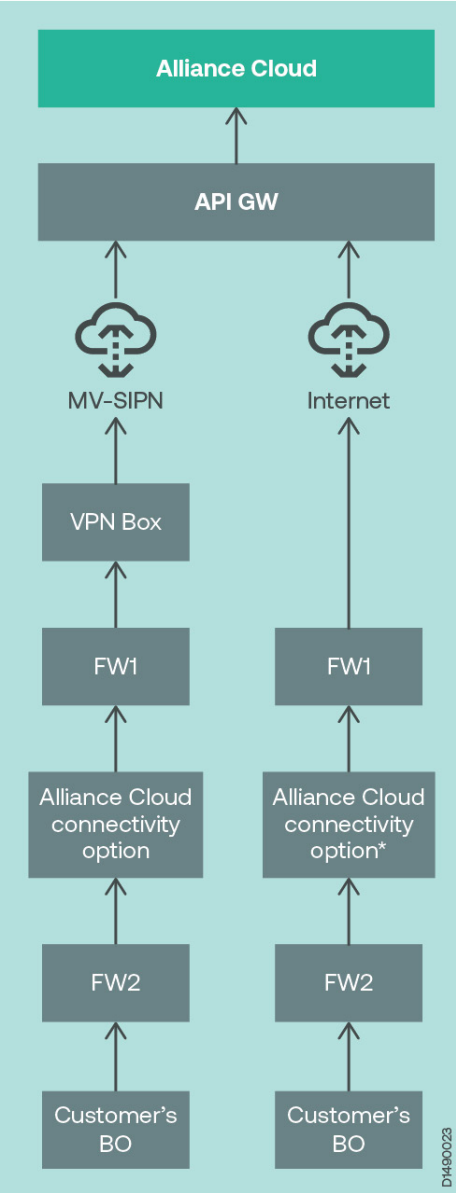
The Alliance Cloud GUI is a Swift Web Access client. Swift Web Access enables secure, browser-based access from an end-user client who uses a standard browser, to a service provider's web server over Swift, in this case the Alliance Cloud GUI.

For more information about how to configure Swift Web Access, see the [Network Configuration Tables Guide](#).



Customer footprint for the pilot environment

If you use an Alliance Cloud connectivity option (Swift Integration Layer, Alliance Cloud Connectors, or an API client) with MV-SIPN connectivity in combination with a channel certificate, then connectivity to the **Entrust Authority Enrollment Server for Web** is required.



* Not all Alliance Cloud connectivity options are supported over the Internet. For more information, see [Alliance Cloud Connectivity Options](#) on page 129.

18.3.1 User-to-Application: Alliance Cloud GUI

Alliance Cloud GUI is based on the standard configuration of Swift Web Access for browsers.

For more information, see [Swift Web Access](#) in the [Network Configuration Tables Guide](#).

	Live	Test	Comment
Alliance Cloud GUI	URL: https://swift-alliancecloud.browse.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.1.244 IP on the Internet: 149.134.170.157	URL: https://swift-alliancecloud-test.browse.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.1.208 IP on the Internet: 149.134.170.126	Port 443/tcp (HTTPS). Same URL for Internet and MV-SIPN.

	Live	Test	Comment
IdP	URL: https://idp.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.2 IP on the Internet: 149.134.170.40	URL https://idp.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.2 IP on the Internet: 149.134.170.40	
Swift Certificate Centre	MV-SIPN https://scc.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.252 Internet https://certificates.swift.com IP on the Internet: 149.134.170.6	MV-SIPN https://scc.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.252 Internet https://certificates.swift.com IP on the Internet: 149.134.170.6	

18.3.2 Application-to-Application: Swift Messaging API

The Swift Messaging API is only available on MV-SIPN and not over the Internet.

	Live	Test	Comment
API Gateway	URL: https://api.swiftnet.sipn.swift.com/alliancecloud IP in MV-SIPN: 149.134.1241	URL: https://api-test.swiftnet.sipn.swift.com/alliancecloud IP in MV-SIPN: 149.134.63.27	Port 443/tcp (HTTPS)
Swift Certificate Centre	https://scc.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.252	https://scc.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.252	Port 443/tcp (HTTPS)
Entrust Authority Enrolment Server for Web - Server #1 (WebConn #1)	URL: https://wbcl01.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.252.8	URL: https://wbcl01.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.252.8	Port 49171/tcp (HTTPS) connectivity to Entrust Authority Enrollment Server for Web is required.
Entrust Authority Enrolment Server for Web - Server #2 (WebConn #2)	URL: https://wbcl02.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.244.134	URL: https://wbcl02.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.244.134	
Swift CA Certificates Download Service	URL: https://cacertificates.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.63.242	URL: https://cacertificates.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.63.242	Port 443/tcp (HTTPS)
S3 storage used in signed URL for FileAct exchange over Swift Messaging API	URL: https://s3-eu.swiftnet.sipn.swift.com/alliancecloud-external-fileact-live IP in MV-SIPN: 149.134.2.69	URL: https://s3-eu.swiftnet.sipn.swift.com/alliancecloud-external-fileact-pilot IP in MV-SIPN: 149.134.2.69	Port 443/tcp (HTTPS)

18.3.3 Application-to-Application: Swift Integration Layer and Alliance Cloud Connectors

For customers that use the Swift Integration Layer (SIL) customer footprint or the Alliance Cloud Connectors component on the Swift Microgateway.

For the application-to-application (A2A) flow, customers install SIL or Alliance Cloud Connectors on their premises. They play the role of an intermediate node between customers' back-offices and Alliance Cloud systems. SIL and the Alliance Cloud Connectors perform REST calls to the API Gateway, which forwards them to Alliance Cloud.

18.3.3.1 SIL and Alliance Cloud Connectors to Swift Connectivity

	Live	Test	Comment
API Gateway	URL: https://api.swiftnet.sipn.swift.com/swift-alliancecloud-sil IP in MV-SIPN: 149.134.1.241 IP on the Internet: 149.134.170.100	URL: https://api-test.swiftnet.sipn.swift.com/swift-alliancecloud-sil-pilot IP in MV-SIPN: 149.134.63.27 IP on the Internet: 149.134.170.99	Port 443/tcp (HTTPS). SIL and the Alliance Cloud Connectors connect to Alliance Cloud through API Gateway. There is a live API Gateway and a test API Gateway.
Swift Certificate Centre	MV-SIPN https://scc.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.252 Internet https://certificates.swift.com IP on the Internet: 149.134.170.6	MV-SIPN https://scc.swiftnet.sipn.swift.com IP on MV-SIPN: 149.134.63.252 Internet https://certificates.swift.com IP on the Internet: 149.134.170.6	Port 443/tcp (HTTPS). The URL for Internet and MV-SIPN is the same.
Entrust Authority Enrolment Server for Web - Server #1 (WebConn #1)	URL: https://wbcl01.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.252.8 IP on the Internet: n/a	URL: https://wbcl01.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.252.8 IP on the Internet: n/a	Port 49171/tcp (HTTPS). If the customer operates SIL or the Alliance Cloud Connectors with MV-SIPN connectivity in combination with a channel certificate, then connectivity to Entrust Authority Enrollment Server for Web is required.
Entrust Authority Enrolment Server for Web - Server #2 (WebConn #2)	URL: https://wbcl02.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.244.134 IP on the Internet: n/a	URL: https://wbcl02.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.244.134 IP on the Internet: n/a	
Swift CA Certificates Download Service	URL: https://cacertificates.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.63.242 IP on the Internet: n/a	URL: https://cacertificates.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.63.242 IP on the Internet: n/a	Port 443/tcp (HTTPS).
Alliance Cloud FileAct Service	URL: https://swift-alliancecloud-sil-file.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.0.170 IP on the Internet: 149.134.171.13	URL: https://swift-alliancecloud-sil-file-pilot.swiftnet.sipn.swift.com IP in MV-SIPN: 149.134.0.143 IP on the Internet: 149.134.171.12	Port 443/tcp (HTTPS). SIL or the Alliance Cloud Connectors connect to the Alliance Cloud FileAct Service for uploading/downloading FileAct messages. There is a different URL for Live and Test.

Firewall Rules

Source host	Source port	Destination host	Destination port
SIL and Alliance Cloud Connectors	> 1023/tcp	Pilot API Gateway	443/tcp (HTTPS)
	> 1023/tcp	Live API Gateway	443/tcp (HTTPS)
	> 1023/tcp	Swift Certificate Centre	443/tcp (HTTPS)
	> 1023/tcp	Entrust Authority Enrolment Server for Web - Server #1 (WebConn #1)	49171/tcp (HTTPS)
	> 1023/tcp	Entrust Authority Enrolment Server for Web - Server #2 (WebConn #2)	49171/tcp (HTTPS)
	> 1023/tcp	Swift CA Certificates Download Service	443/tcp (HTTPS)
	> 1023/tcp	Pilot Alliance Cloud FileAct Service	443/tcp (HTTPS)

Source host	Source port	Destination host	Destination port
	> 1023/tcp	Live Alliance Cloud FileAct Service	443/tcp (HTTPS)

18.3.3.2 Configuration for SIL and Alliance Cloud Connectors Web Application

Source host	Source port	Destination host	Destination port
Web browser	> 1023/tcp	SIL and Alliance Cloud Connectors	8443/tcp (HTTPS) or user-defined

18.3.3.3 Back Office to SIL and Alliance Cloud Connectors Connectivity

SIL offers the following connection types:

- Files
- WS

Alliance Cloud Connectors offer the following connection type:

MQ – for firewall rules for MQ connectivity, proper connectivity must be provided between the MQ server host and the Alliance Cloud Connectors host, which depends on the MQ setup.

Firewall Rules for Web Services (REST channel)

Source host	Source port	Destination host	Destination port
Back office hosts	> 1023/tcp	SIL	50443/tcp or user-defined

18.4 Install Token Software

Before you can activate and use your personal token on Swift portals, you must install the personal token software and SConnect on each computer on which you intend to use the token.

For more information about the installation prerequisites and how to install the token software, see the [Swift Certificate Centre Personal Token Software Installation Guide](#).

18.5 Internet Access Inclusion/Exclusion (Optional)

This topic describes how to disable internet access to Alliance Cloud.

If you disable internet access, then this means that the only option to connect to Alliance Cloud is through the multi-vendor secure IP network (MV-SIPN) connectivity (VPN box). You can only disable internet access if your institution is subscribed to MV-SIPN. If you need to subscribe to Alliance Connect, then please contact your Swift Account Manager.

How to request the exclusion

1. An Alliance Cloud security officer must create a case using the [Case Manager](#) on swift.com in which they request to include/exclude their Distinguished Name (DN) address. For more information, see Knowledge Base article [5026197](#).
2. After creation of the case, your case will be followed up by Swift Support or Professional Services if you are being onboarded by them.

Important If the request is urgent, then you must also call your local Swift Support Centre to make them immediately aware of the creation of the request. Please enter the related case reference when you call.

3. After the inclusion/exclusion procedure has been executed by Swift, you will be informed by your Customer Support Centre or Professional Services.

19 Test your Message Flows

After completing all tasks in the [Alliance Cloud Getting Started Checklist](#) on page 15, you can begin testing your message flows.

If you are migrating from another infrastructure to Alliance Cloud, then you must request the migration of your Test and Training (T&T) flows from your existing solution to Alliance Cloud before testing.

Request migration of your Test and Training flows

You can manage the migration of your flows on the [Alliance Cloud ordering page](#): [Migrate Services to Alliance Cloud](#).

Requests that are placed before the end of each Tuesday will take effect during the following weekend. Requests that are placed on Wednesdays will take place the weekend after the following weekend.

Contact your Swift consultant if you need help with this task.

Important Log out of your T&T Logical Terminal (used to exchange FIN traffic) on your current infrastructure. Do not acquire any T&T store-and-forward queues **before** the confirmed maintenance window during which Swift will activate your T&T flow on Alliance Cloud.

Direct your test message flow from your back-office application to Alliance Cloud.

20 Plan Volume and Throughput Tests for Alliance Cloud

For more information, see Knowledge Base articles [2008531](#) and [600376](#).

21 Delivery Subset Sharing Mode and Throughput Tasks

This topic describes how customers can request activation of high throughput, change the delivery subset sharing mode, and remove custom delivery subsets along with the deadlines before migration or activation. Some of these tasks are only for migrating customers.

Alliance Cloud supports a daily volume of 100,000 messages, sent and received, per day per BIC with a throughput of maximum 50,000 MT or MX messages per hour.

Depending in your throughput, you must adapt your delivery subset sharing mode and increase your windows size.

Your throughput is less than 5000 messages/hour

Task	Description	Type of customer	Reference	Deadline
Make sure your delivery subset sharing mode is set to "N"	N - None - Not Sharing	Migrating customers	FIN Delivery Subset Details Window in the <i>Alliance Access Configuration Guide</i>	At least five days before the migration date

Throughput is higher than 5000 messages/hour or 11,000 messages/day

Task	Description	Type of customer	Reference	Deadline
Request activation of high throughput	Remind your Swift consultant to request the activation of high throughput in Alliance Cloud.	New and migrating customers	n/a	At least one week before the migration date
Change your delivery subset sharing mode to "L"	L - Load balance - if multiple LTs share the same subset(s), then distribution of messages is done more evenly across LTs so that no single LT is overwhelmed.	Migrating customers	See Knowledge Base article 6000375 .	Must be one week before the migration date.

Throughput is higher than 22,000 messages/hour or 43,000 messages/day

Task	Description	Type of customer	Reference	Deadline
Request activation of high throughput	Remind your Swift consultant to request the activation of high throughput in Alliance Cloud.	New and migrating customers	n/a	At least one week before the migration date
Request an increase in window size of your LTs	Request an increase in window size.	New and migrating customers	<i>Change your FIN window size e-order</i>	At least three weeks before the migration date
Change your delivery subset sharing mode to "L"	L - Load balance - if multiple LTs share the same subset(s), then distribution of messages is done more evenly across LTs so that no single LT is overwhelmed.	Migrating customers	See Knowledge Base article 6000375 .	Must be one week before the migration date.

Reset user-defined delivery subsets

For migrating customers

Reset the delivery subset from your legacy interface by sending a system message (MT 047).

For Alliance Access, see the [Alliance Access Configuration Guide](#).

For Alliance Entry, see the [Alliance Entry Configuration Guide](#).

22 Request Activation on the Live Environment

After completing all tasks in the [Alliance Cloud Getting Started Checklist](#) on page 15, you can request activation on the live environment.

Migrating customers

You must request the migration of your live flows from your existing solution to Alliance Cloud. You can do so on the Alliance Cloud ordering [page](#) > **Migrate Services**. See [Migrate your SwiftNet Services to Alliance Cloud](#) on page 32 and [Migrate your FIN Services to Alliance Cloud](#) on page 33.

Requests that are made before the end of Tuesday take effect during the following weekend. Requests that are made on Wednesday take place the weekend after the following weekend. Contact your Swift consultant if you need help with this task.

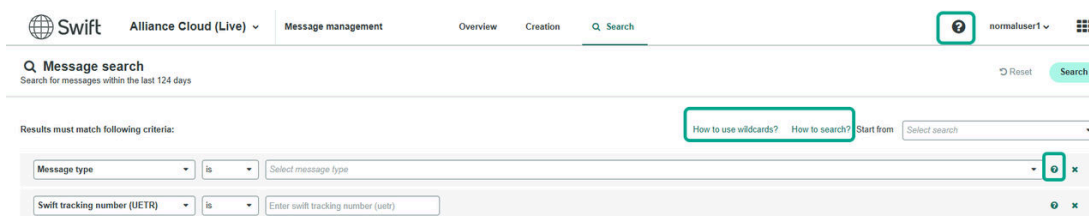
Important If FIN is currently hosted on an interface that is not controlled by Swift, then you must ensure that the Logical Terminal is properly logged out before the migration date, and remains so.

New Swift customers

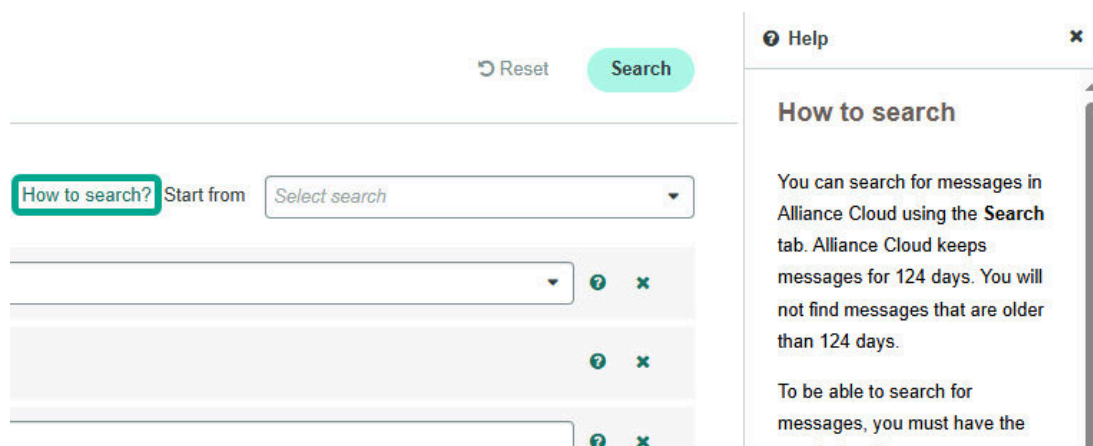
- **Swift Professional services is helping you with the implementation**
Your project manager must send an e-mail to your Swift consultant to request activation on the live environment.
- **You did not request Swift Professional Services to help you with the implementation**
[Central Activation of FIN for New BICs](#) on page 31

23 Online Help

Alliance Cloud is an intuitive and easy to use application. If you have questions, then help is available after you log in. Just click the appropriate **Help** link or the  icon.



Information will appear in a right-hand pane. If there is additional information about the topic, then the [See more help](#) link appears at the bottom of the right-hand pane. Click this link to open the full Alliance Cloud help.



24 Swift Training

Swift provides training about standards, products, and services to suit different needs. From tailored training to self-paced e-learning modules on [Swift Smart](#), a range of training options are available for all Swift end users.

Swift Smart

[Swift Smart](#) is an interactive, cloud-based training service that offers a large variety of courses for different levels of knowledge. The courses contain exercises and quizzes and are available in multiple languages. The [Swift Smart catalogue](#) provides a list of courses that are organised into these learning tracks:

- General knowledge
- Work with messages
- Deploy and manage Swift software solutions
- Security and audit
- Compliance and shared services

[Swift Smart](#) is accessible from the desktop or a mobile device. No installation is required.

Swift Smart is available to all connected Swift end users and registered Swift partners with a swift.com account. For more information, see [How to become a swift.com user](#).

Tailored training

A full range of tailored programmes is available to meet specific training needs. For more information, visit the [Training](#) web page.

24.1 Swift Smart Modules for Alliance Cloud

Swift Smart modules are [available](#) to help you familiarise yourself with Alliance Cloud:

- discover how Alliance Cloud is fully managed by Swift and minimises the use of internal infrastructure and resources
- learn the basics of Alliance Cloud for a messaging operator, security officer, SIL administrator, and Alliance Cloud administrator.

Related information

[Swift Training](#) on page 106

25 Terminology

Term	Definition
Alliance Cloud connectivity options	The following options are available, which enable customers to set up automated message exchange between back-office applications and Alliance Cloud: - Alliance Cloud API Connector connecting through Swift Integration Layer - Alliance Cloud Connectors: - File Connector - MQ Connector - Swift Messaging API For more information, see the documentation on the Knowledge Centre.
Alliance Cloud <connectivity option> administrator	The Alliance Cloud connectivity option administrator is the user that configures the Alliance Cloud connectivity option: - SIL administrator - MQ Connector administrator - API client administrator for the Swift Messaging API
Alliance Cloud API Connector	Alliance Cloud API Connector allows you to connect your back office to the REST channel. The REST channel is configured in the SIL GUI and connects to the application channel configured in Alliance Cloud. The API Connector will go out of support at the same time as the Swift Integration Layer in June 2026.
Alliance Cloud Connectors	This connectivity option uses the Swift Microgateway to exchange messages and files with Alliance Cloud. There are two types of Alliance Cloud Connectors: the File Connector and the MQ Connector.
Alliance Cloud File Connector	The Alliance Cloud File Connector enables FIN and InterAct messages to be exchanged between Alliance Cloud and your back-office applications using a file-based connectivity method.
Alliance Cloud MQ Connector	The Alliance Cloud MQ Connector enables customers to set up IBM MQ queues to exchange FIN and InterAct messages with Alliance Cloud.
Alliance Connect	Alliance Connect products deliver secure and reliable connectivity to Swift. Alliance Connect has three tiers: Bronze, Silver/Silver Plus, and Gold. For a multi-vendor secure IP network (MV-SIPN), customers must order Alliance Connect. For more information, visit swift.com.
Application channel	An application channel is a connection between Alliance Cloud and any Alliance Cloud connectivity option to send and receive messages. The application channel must be configured by customers in both places. Alliance Cloud currently offers different types of application channels: - File channel - API channel - REST channel - MQ channel Application channels require a certificate. This certificate is used to secure the connection to Alliance Cloud. This certificate can be hosted on a personal token or on a disk (channel certificate).
Business entity	A business entity is a group of BICs. An institution can define multiple business entities to separate the messages and their processing. If multiple business entities are defined, then they can be used in the role definition to limit the access of the user. If your institution does not use multiple business entities, then the term "business entity" and its related options do not appear in the Alliance Cloud interface.

Term	Definition
	An institution can currently order only one business entity.
Channel certificate	Channel (disk) certificates require access through multi-vendor secure IP network (MV-SIPN). For MV-SIPN, customers must order Alliance Connect. For more information, visit swift.com .
Distinguished Name (DN)	The identification of an entity following the X.500 notation. SwiftNet identifiers have the format of a DN. An example is <code>cn=xyz, ou=abc, o=bankbebb, o=swift</code> , in which <code>bankbebb</code> is the 8-character BIC, and the other elements at the left form the optional extension. This extension enables detailed identification by department, geographical location, application, or individual.
Distinguished Name (DN) equivalence	A specific naming scheme that standardises the naming format for multiple DNs that identify the same entity (application or human). If your institution plans to use the active/standby feature for the Alliance Cloud connectivity options connections, then the application channels must be created using equivalent DNs. In these connections, the following DNs are considered as equivalent: <code>cn=<server-x>, o=bankbebb, o=swift</code> <code>cn=%1, cn=<server-x>, o=bankbebb, o=swift</code> <code>cn=%2, cn=<server-x>, o=bankbebb, o=swift</code>
Entry condition(s)	In a workflow, an entry condition is a step that uses a combination of criteria to define the messages to which the criteria apply.
File channel	The File application channel uses a directory structure on the local host to provide an interface to your back-office application. The File channel is configured in the SIL GUI and connects to the application channel configured in Alliance Cloud.
FIN service	The messaging service that enables the secure and reliable exchange of Swift MT messages in store-and-forward mode.
Incoming	In a workflow, incoming is the direction from the correspondent and the network towards the customer. The term defines the direction of a message or a message workflow.
InterAct	InterAct is the messaging service for exchanging XML-based financial messages and data between users, including Swift MX and ISO 20022-based payments, settlement instructions, FX confirmations, statements and reports. InterAct enables the interactive (real-time) and store-and-forward exchange of messages between parties. InterAct is particularly suited for mission-critical and time-critical application.
Multi-vendor secure IP network (MV-SIPN)	The Swift architecture based on a network model that uses state-of-the-art security (secure IP network). The multi-vendor secure IP network also improves resilience and capacity, while avoiding dependency on a single network supplier.
Offline security officer	An offline security officer has access to offline tools only, such as Secure Channel and the swift.com user administration tool: Identity Management.
Online security officer	An online security officer has access to offline tools only, such as the Swift Certificate Centre and SwiftNet Online Operations Manager.
Outgoing	In a workflow, outgoing is the direction from the customer towards the network and the correspondent. The term defines the direction of a message or a message workflow.
Permissions	Each role in Alliance Cloud has one or more related permissions. Some permissions can be customised. For example, for the Approve

Term	Definition
	message permission, you can define the currencies and amounts, destinations, and message types that the user can approve.
Personal Token Software	Customers can download the Personal Token Software from the Swift Certificate Centre or the Download Centre . All Swift services and products that use a token require this software.
Relationship Management Portal	The Relationship Management Portal is a central application managed by Swift, which centrally records and enforces pre-agreed relationships between correspondents. It enables institutions to view, create, store, and manage pre-agreed relationships with their correspondents.
REST channel	With the REST channel, users upload and download messages or files using API calls. Data is sent in JSON format. A REST channel is configured in the SIL GUI and connects to the application channel configured in Alliance Cloud.
Role	A role defines an action or set of actions that a user can perform for a specific Alliance Cloud module, such as Message management. A role can be linked to multiple business entities, but a role can only be linked to one Alliance Cloud module. Each role has one or more related permissions. Some permissions can be customised. For example, for the Approve message permission, you can define the currencies and amounts, destinations, and message types that the user can approve.
Role-Based Access Control (RBAC)	An optional SwiftNet facility that enables customers to control the access of end-users and applications to service functions. For Alliance Cloud, Swift defines the available user access profiles (roles) for use with RBAC. After provisioning, the security officer within an institution can grant roles to end users and applications.
SConnect	A browser extension that enables applications and websites to communicate with tokens. To connect to an application with a token, installation is required.
Secure Channel	Swift's central application for the management of security officers.
Swift Certificate Centre (SCC)	A portal to the SwiftNet PKI Certification Authority that enables end users to manage PKI certificates. For example, an end user may access the portal to activate a token or renew a PKI certificate.
SIL administrator password	The SIL administrator password is initialised during installation of Swift Integration Layer by the user (system administrator) who installs SIL. The SIL administrator (SIL_Owner) needs this password to log in to the SIL GUI and run certain command-line tools.
SIL GUI	The Swift Integration Layer graphical user interface (GUI) lets the SIL administrator perform a number of configuration tasks needed to use Alliance Cloud.
SIL administrator (SIL_Owner)	The user that configures and runs SIL after SIL has been installed by a system administrator.
Swift Integration Layer (SIL)	An integration framework, based on open technologies, that provides means of integrating customers formats and business flows with Swift messaging services. SIL enables messages to be exchanged between your back office and Alliance Cloud.
Swift Messaging API	A REST API, which serves as a bidirectional connector for API clients to exchange messages with Alliance Cloud using REST endpoints. For more information, see the Swift Messaging API Getting Started.

Term	Definition
SwiftNet Online Operations Manager (O2M)	An application that enables security officers to manage their SwiftNet PKI certificates and delegate Role-Based Access Control roles through a Swift-managed Swift Web Access service.
User	A user is a person linked to an institution. A user must have a DN and the appropriate RBAC roles assigned by their security officers. Each user that needs to log in to Alliance Cloud must have a user account on the Admin centre, which is created by the Alliance Cloud administrator. Each user account is assigned one or more roles, which define the actions that they can do on the Alliance Cloud platform and which data that they can see.
Workflow	A workflow is a sequence of steps that define how a message should be processed in Alliance Cloud. All messages in Alliance Cloud go through either an incoming workflow or an outgoing workflow. An incoming workflow defines what happens to messages that your institution receives. An outgoing workflow defines the steps that messages must go through before your institution sends them to Swift.
Workflow step	When a workflow is created in the Admin centre, the workflow step defines what should happen to a message. The step can be an automatic check or an action that requires human intervention. Message validation and approving a message are both possible steps in a workflow.

Appendix A About Alliance Cloud

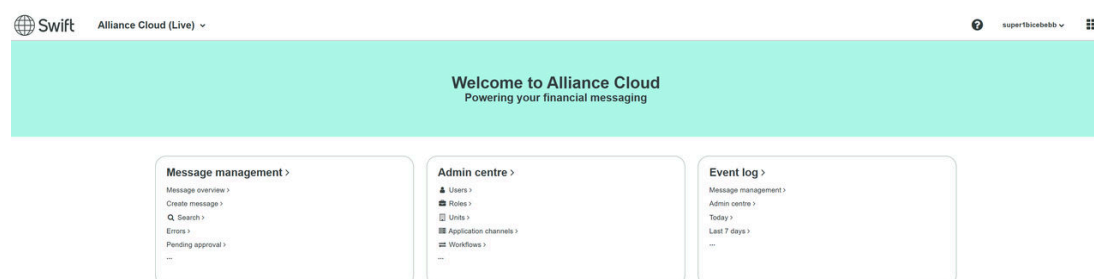
A.1 Alliance Cloud Modules

Alliance Cloud consists of the following modules. Each module enables users to perform specific tasks. When users log in, they will see only the modules assigned to their specific roles.

- **Admin centre**
 - Manage the users and roles for your institution.
 - Configure the different modules such as Message management :
 - Manage and configure the message processing workflow
 - Manage and configure the archive messages feature
 - Manage and configure application channels for connectivity to back-office applications
 - Manage the units
 - Configure a Test and Training BIC for future mode
 - Import message templates
- **Message management**
 - Create messages manually for MT (FIN) business messages (such as a fin.103) and FIN system messages. For information about MX formats for manual message creation, see Knowledge Base article [5025814: Alliance Cloud message management functionalities](#).
 - View, verify, and approve messages coming from the back office
 - Search for messages, configure and save searches
 - Repair messages in error state coming from the back office and manually created
 - In the Test and Training (T&T) environment, create messages for the current Standards release and create messages for the upcoming FIN Standards release as of activation of the **future** mode until the Standards cutover date in November.
- **Event log**

View and investigate events that occurred in the Admin centre and Message management modules

Relationship Management authorisations are managed in the Relationship Management Portal, not in Alliance Cloud. See [Relationship Management Portal Tasks](#) on page 89.



A.2 Types of Alliance Cloud Users, Roles, and Related Functions

There are several types of Alliance Cloud users. There are also other functions that are needed to do the initial set-up of Alliance Cloud and to set up the end-to-end flow to connect to Alliance Cloud.

Alliance Cloud provides a set of default roles in the Admin centre that are already available for you to assign to users. Each role contains a set of permissions. The existing roles cannot be

modified, but you can copy them and modify the copied roles to make them more specific to your institution.

Note *If you are a Business Connect Provider or an End Customer of a Business Connect Provider, then you will have fewer default roles.*

Alliance Cloud users and roles

Type of user	Default role in Alliance Cloud Admin centre	Description
Alliance Cloud administrators	Administrator	Create, modify, and delete users and roles, and assign roles to users in the Admin centre. An institution must have at least two of these administrators. When the Alliance Cloud administrators log in to Alliance Cloud for the first time, they automatically receive the Administrator role in Alliance Cloud.
Event log administrators	Event log viewer	View and investigate events that occurred in the Admin centre and Message management modules.
Message management administrators	Back-office operator	When messages have not been successfully distributed to the back-office (through SIL or direct APIs), the back-office operator has the permission to restart and relaunch the distribution of these messages to an application channel.
Message management administrators	Message management business operator	Access to all permissions of the message management module except the permission to redistribute the messages to an application channel.
Message management administrators	Message management business operator (incl. verify own)	Access to all permissions of the message management module except the permission to redistribute the messages to an application channel. Verify own messages.
Message management administrators	Message management authoriser	Verify, approve, cancel and close (single or multiple) messages. Note <i>Cannot create messages.</i>
Message management administrators	Message management creator	Create and repair messages. Create and manage message templates.
Message management administrators	Message management configurator	Create the application channels and units in the Admin centre. Design and configure the workflow in the Admin centre. Design and configure the archive messages feature.
Message management administrators	Message management viewer	View messages.
Message management operators	Message management operator	Create messages, view and search for messages, verify messages, repair messages, and approve messages based on the specific conditions and criteria configured in the workflow. Redistribute messages manually to the back office.

For Business Connect Providers, the default roles are:

- Administrator
- Event log viewer
- Back-office operator

- Message management viewer
- Message management configurator

For End Customers of Business Connector Providers, the default roles are:

- Administrator
- Event log viewer

Roles provisioned for delegation purposes

These roles are provisioned for delegation purposes and can be shared with another institution for a certain amount of time. These roles are locked. The provider and the customer cannot modify them.

Default role	Description
External message management configurator	Create, manage, and approve application channels and units, and configure workflows on behalf of a delegating customer
Support	The Support role is assigned by customers to Swift.

Other related functions

Type of user	Description
Security officers	Security officers are responsible for the management of the PKI tree in SwiftNet Online Operations Manager (O2M), the channel certificates, and the tokens given to the users. An institution must have at least two security officers. An administrator can also have the role of the security officer. The institution can decide whether the same person has both the security officer role and an administrator role.
System administrator	The system administrator downloads Swift Integration Layer from the Download Centre and installs it.
Alliance Cloud <connectivity option> administrator	The Alliance Cloud connectivity option administrator is the user that configures the Alliance Cloud connectivity option: • SIL administrator • MQ Connector administrator • API client administrator for the Swift Messaging API

Example default role in Alliance Cloud Admin centre

Back to roles overview

Role

Message management operator

(Locked role) - Active

Export

Add users

Role parameters

Assigned users (0)

Read only - You cannot edit the role parameters because this is a locked role. You can assign users to the role.

General information

Role name

Message management operator

Description

Status

Active

Module

Message management

Access to business entities (1)

Users with this user role have access to the following business entities:

BICEBEBB_MESSAGING_US

BICEBEBB

Permissions

Users with this role have the permission to do the following actions:

Access to messages

Manual creation and repair

The workflow defines whether a manually created or repaired message must be either verified, pre-approved, or final approved.

Create & repair message

Verification and approval

The workflow defines whether a message must be either verified, pre-approved, or final approved. Users cannot final approve a message that they have manually created or repaired.

Verify message

Final approve message

Distribute to application channel

Distribute to application channel

Close and cancel

Close a message

Cancel a message

Create and manage templates

A.3 Roles, Users, Units, and Business Entities

Roles

A role defines an action or set of actions that a user can perform for a specific Alliance Cloud module, such as Message management. A role can be linked to multiple business entities, but a role can only be linked to one Alliance Cloud module. By default, a role applies to all of the BICs that belong to the business entity.

Each role has one or more related permissions. Some permissions can be customised. For example, for the **Approve message** permission, you can define the currencies and amounts, destinations, and message types that the user can approve.

Users

A user is a person linked to an institution.

Each user that needs to log in to Alliance Cloud must have a user account on the Admin centre, which is created by the Alliance Cloud administrator.

Each user account is assigned one or more roles, which define the actions that they can do on the Alliance Cloud platform and which data that they can see.

User Reports and Role Reports

As an administrator of Alliance Cloud you can export user reports and role reports for reporting and auditing requirements. For more information, see the Alliance Cloud Operations Guide.

Units

A unit is an attribute you can add to messages to separate your message flows and limit the access to messages.

A unit is assigned to a message and a message can only belong to one unit (or to none). If a unit is assigned to a message that already has a unit, it replaces the old unit.

The appropriate role is then assigned to each user by the Alliance Cloud administrator using the Admin centre module.

Scenario	Description
A unit is not specified in the permissions for the role.	Users can do the actions specified in the role on all messages (messages with a unit and messages without a unit).
A unit or units is specified in the permissions for the role.	Users can do only the actions specified in the role on messages tagged with those specific units.
The unit is null in the permissions for the role.	Users can do only the actions specified in the role on messages which have no unit.
The unit is not null in the permissions for the role.	Users can only do the actions specified in the role on messages which have a unit (that is, any unit), but not those without a unit.

Business entities

A business entity is a group of BICs.

A unit can only belong to one business entity. Also, a business entity can contain one or more BICs. Every message sent to a BIC goes to the business entity to which the BIC belongs. By default, the roles assigned to a User allow the same permissions for all BICs belonging to the business entity.

If multiple business entities are defined, then they can be used in the role definition to limit the access of the user.

If your institution does not use multiple business entities, then the term "business entity" and its related options do not appear in the Alliance Cloud interface.

A.4 Workflows

A workflow is a sequence of steps that define how a message should be processed in Alliance Cloud.

All messages in Alliance Cloud go through either an incoming workflow or an outgoing workflow. An incoming workflow defines what happens to messages that your institution receives. An outgoing workflow defines the steps that messages must go through before your institution sends them to Swift. There is always one active workflow for each direction (incoming and outgoing) and for each business entity. When an inactive workflow becomes active, the current active workflow becomes automatically inactive.

Note *Archiving a copy of a message or file and its history is not a workflow step. Archiving a copy is done through a specific type of distribution managed outside the workflows configuration.*

For detailed information about workflows, see the [Alliance Cloud Operations Guide](#).

A.5 Message Creation, Verification, Repair, and Approval

In the Message management module, you can manually create MT (FIN) business messages (such as a fin.103) and FIN system messages. For information about MX formats for manual message creation, see Knowledge Base article [5025814: Alliance Cloud message management functionalities](#).

You can choose the type of message that you want to create from the **New** tab or the **Favourites** tab if you have added messages to favourites. You will see only the messages that you have the permission to create.

For more information, see the [Alliance Cloud Message Management User Guide](#).

Raw and structured view

You can create messages in raw and structured view in Alliance Cloud.

In raw view, Alliance Cloud displays in text format the fields in the body of the message. No additional information is provided about what to enter in each field. You must type the content or copy and paste the body from another source.

In structured view, Alliance Cloud displays structured information about the fields to help you select and enter values in the message.

The header fields always appear in structured view. For header fields, you can click the field name and information about that field will appear in a right-hand pane. Mandatory fields are marked with an asterisk (*).

Message templates

You can save time by using message templates to create messages that you send on a regular basis.

A message template contains values that do not change often, such as the sender and the receiver of the message. If you create a message from a template, then you only need to enter values for fields that are variable, such as dates and amounts.

You can use one template to create any number of new messages.

After you create a template, you can also edit or delete the template.

When a user creates, modifies (including the template name), or deletes a message template, Alliance Cloud creates an event in the Event log. Alliance Cloud also creates an event when a message is created from a template. Only users with the **Event log viewer** role can view the Event log.

See also [Upgrading a template to a new message standard](#) in the *Message Management User Guide*.

Message repair

Provided the message content allows Alliance Cloud to identify the message type, an outgoing message that ends in one of the following error states may be repaired by users who have the permission to create and repair messages:

- Validation failed
- Verification rejected

- Final approval rejected
- Send failed
- NACKed
- Delayed NACK
- Delivery failed

Users can repair messages created manually or sent by the back office. You cannot repair a message in AnyXML format.

Message verification

You can configure the workflow so that messages created manually, repaired, and messages coming from the back office need verification by another user.

Note *If you have been granted the appropriate permission, you may verify messages that you created or repaired yourself.*

After an MT (FIN) or MX message has been created, another user with the **Verify message** permission can verify certain fields in messages with the status **Pending verification**. Only some fields in the message body can be verified, such as **Date**, **Currency**, or **Amount**. When verifying a message, verifiable fields are empty in the message.

If you are not able to correctly verify a message, then you can reject the message.

Message verification is a functionality used to prevent input errors by having a second person re-enter important fields in a message. It is not an additional authorisation step.

Message approval

You can configure the workflow so that manually created messages, repaired messages, and messages coming from the back office need approval by another user with the appropriate permission.

Swift message standards and future mode

In the Test and Training (T&T) environment, you can create messages for the current Standards release. You can also create messages for the upcoming FIN Standards release as of activation of the **future** mode until the Standards cutover date in November. This mode is generally activated each year by the end of September. See [Future mode](#) on page 118.

For FIN message creation, online help is available by clicking the  next to the message name. The help provides detailed information about the fields and format specifications to help you create the body of the message.

See also [Standards releases](#) on page 120.

Related information

[Workflows in the Alliance Cloud Operations Guide](#)

A.6 Swift Standards

A.6.1 Future mode

In future mode, Test and Training (T&T) users can exchange messages with themselves or with any other T&T user with the future message syntax for the new FIN Standards release.

Important You can only activate future mode during the future mode testing period. For more information, including when this period starts for Alliance Cloud, see the following:

- [Alliance Cloud Operations Guide](#)
- Knowledge Base article [5026256: Alliance Cloud - When to activate the Future Mode](#)
- [Alliance Cloud - Future Mode](#)

When switching between current and future mode, Alliance Cloud sends a fin.072 system message (Test Mode Selection) to FIN on behalf of the customer BIC. This is a billable system message.

There are two different modes:

- **Full function**
A T&T BIC can exchange messages with another T&T BIC using the new syntax release. Both BICs must be logged in to the full function mode. FIN validates the messages and returns a positive acknowledgement (ACK) or a negative acknowledgement (NACK) and also delivers the message to the recipient.
- **Local test**
The T&T BIC can send messages only to themselves. FIN validates the messages based on the new syntax release and returns an ACK or a (NACK), but does not deliver the message to the recipient.

There is no concept of current or future formats in system messages.

To use the future mode, an operator who has been granted the **Manage parameters** permission must configure a Test and Training BIC for future mode in the **Parameters** screen of the Admin centre. The permission is activated by one of your Alliance Cloud administrators. The Admin centre online help explains how to configure Alliance Cloud for the future mode.

A.6.2 Swift Standards

Financial messaging standards are agreements on how to define and organise the data in order to exchange financial transactions in a structured manner. The standards use a common language which increases the automation of the business processing chain, also known as straight-through processing (STP).

Swift supports two types of messages:

- Standards MT (FIN)
- Standards MX

Most of the Swift MX messages are registered ISO 20022 messages.

Changes between current and new release

In November of each year, Swift can activate a maintenance release for MT (FIN) and MX in order to bring standards in line with business changes and to correct technical issues. MX releases can also be activated at any time of the year. You can view the changes for MTs in the *Standards Release Guide*. For more information, see [Changes between current and new release](#) on page 121.

You can also view the changes on the MyStandards platform. See [MyStandards](#) on page 124.

A.6.2.1 MT (FIN) messages

Message text standards for individual messages within each category are contained in the category volumes:

- Category 1 - Customer Payments and Cheques
- Category 2 - Financial Institution Transfers
- Category 3 - Treasury Markets - Foreign Exchange, Money Markets, and Derivatives
- Category 4 - Collection and Cash Letters
- Category 5 - Securities Markets
- Category 6 - Treasury Markets - Commodities
- Category 6 - Reference Data
- Category 7 - Documentary Credits and Guarantees/Standby Letters of Credit
- Category 8 - Travellers Cheques
- Category 9 - Cash Management and Customer Status
- Category n - Common Group Messages

Swift message types

Each message category consists of different message types (MT). For example, MT 101 (Request for Transfer) and MT 103 (Single Customer Credit Transfer) are part of Category 1. For a complete list of message types, see the [Standards MT General Information](#).

Note *In Alliance Cloud, an MT is called fin.xxx, such as fin.101 or fin.103.*

A.6.2.2 MX messages

ISO 20022 benefits

ISO 20022 is an emerging global and open standard for payments messaging. Most of the Swift MX messages are registered ISO 20022 messages.

ISO 20022 offers many benefits including the following:

- creates a common language and model for payments data across the globe
- provides higher quality data than other standards, which means higher quality payments
- can adapt to new needs and new approaches
- is not controlled by a single interest
- can be used by anyone in the industry and implemented on any network

MX overview

An MX is an XML message definition for use on the SwiftNet service. An MX can be one of the following:

- a base message
 - an ISO 20022 message
 - an ISO 20022 candidate message (that is, a message that has not yet been approved)
 - a proprietary message (Swift message or from an organisation that develops or uses messages in XML syntax)
- a usage guideline of a base message

MX message classification and naming

Each MX has a message name and a message identifier. The message name is human-readable. The message identifier is a unique structured computer-readable identifier for use by systems and applications.

A message name and its identifier must be considered in the context of its business area. Examples of business areas are `camt` (Cash Management) and `pain` (Payments Initiation).

The following table describes the different components of the message `pacs.008.001.08`.

Component	Name	Function
<code>pacs</code>	Business Area	Mandatory 4-character code that identifies the business. <code>pacs</code> stands for Payments Clearing and Settlement.
<code>008</code>	Message function	Identification (3 characters) for the functionality covered by the message
<code>001</code>	Variant	3-digit number that indicates if it is a base message (001) or an official registered restriction with a specific number for easier routing, validation, and processing of the instances.
<code>08</code>	Version number	Indicates how many maintenances the original message has undergone. When a reference to the message in general is made (which refers to all existing versions), <code>XX</code> is often used.

Related information

ISO 20022 for dummies on www.swift.com

A.6.2.3 Standards releases

In November of each year, Swift can activate maintenance releases for MT (FIN) and for MX to bring standards in line with business changes and to correct technical issues. MX releases can also be activated at any time of the year. For more information, go to swift.com.

Once the new releases are activated, you will typically be able to see messages previously created with the former Standards version and messages created with the new Standards version in Alliance Cloud. In the live environment, you will be able to create messages using only the new Standards version.

Messages from two different Standards releases can appear in Alliance Cloud because messages from the previous Standards release are kept for 124 days. In Message management, you can see the version of the message when you create the message. You can also see the version in the **Header & info** tab > **Format** section.

Actions to be taken before the switch-over

Before Swift switches to the new annual Standards release in Alliance Cloud, we recommend that you do the following:

- Send your business messages as soon as possible before the switch-over in November
- At the end of your business week, make sure that all of your pending messages are transmitted.

A.6.2.3.1 Release cycle

For more information and to view the upcoming release schedule for MT and MX, go to www.swift.com.

MT Standards release cycle

Timeline	Description
Fifteen months prior to implementation (SR-15)	Swift publishes a high-level document (for budget and resource allocation). It highlights the potential scope and size of the subject maintenance release, based on the change requests received. These changes must still be validated by a Working Group and some of them may be reworded, redefined or even removed.
Eleven months prior to implementation (SR-11)	Swift publishes a revised, high-level document (for budget and resource allocation), which shows only those change requests that were approved by the working groups and accepted by a country vote.
Ten months prior to implementation (SR-10)	The Standards Release Guide (SRG) provides details of the changes published in the revised, high-level document.
Exceptional fast-track maintenance process (SR-10)	An exceptional fast-track maintenance process can be announced in December (SR-10) and can result in additional changes to the Standards Release Guide which will then be published at the latest seven months prior to implementation (SR-7).
Three months prior to implementation (SR-3)	The Standards MT User Handbook is available on www.swift.com . At that time, the Test and Training system is available.
Standards release (SR-0) date	The changes are implemented on the Swift network.

Related information

[MTs and MX/ISO Usage Guidelines Development and Maintenance Processes](#)
[Version and Release Management for ISO 20022 Messages - Best Practices](#)

A.6.2.3.2 Changes between current and new release

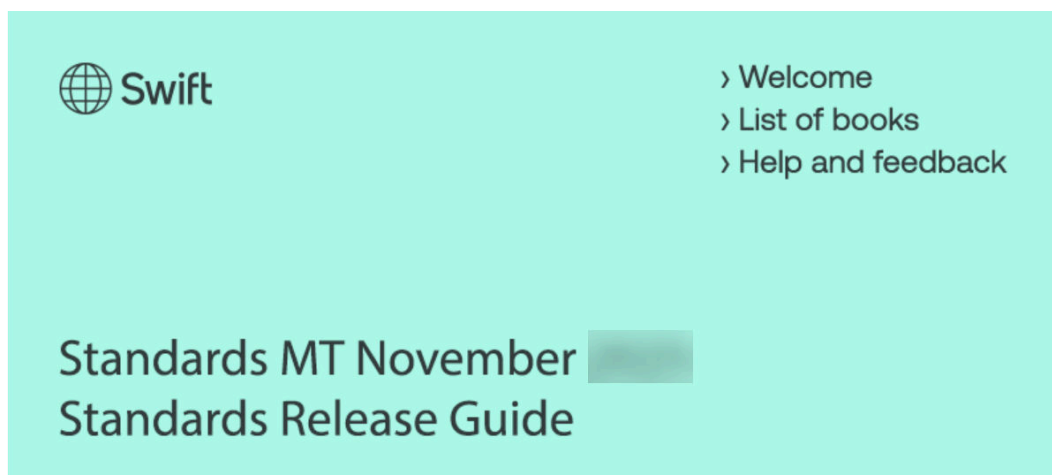
There are different ways to view the changes between the current Swift Standards release and the new release.

- The [Standards Release Guide](#) describes the changes for the next version of the Standards MT messages. It also provides information about format specifications, rules, guidelines, and field specifications.

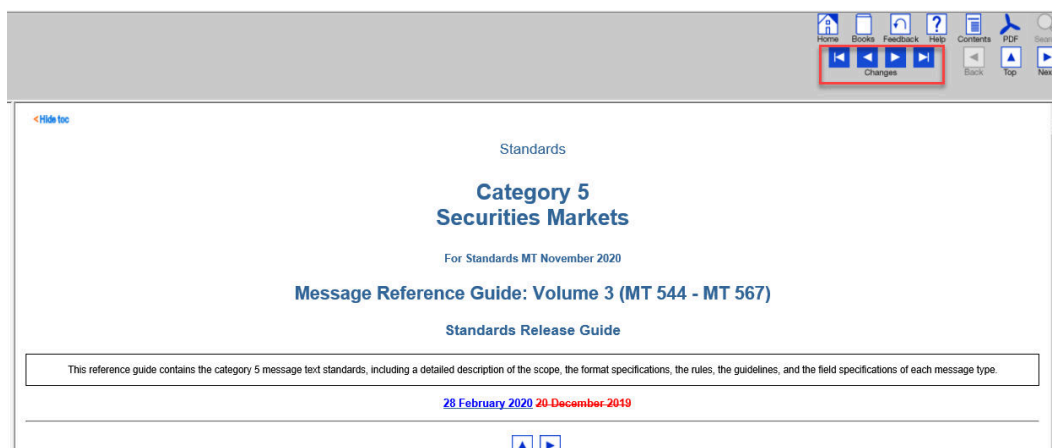
- The *SR <year> - Business Highlights* provides summarised, high level, business information related to the changes made to MTs as part of the annual Standards release. For more information, visit [Standards Releases](#) on [www.swift.com](#).
- The *Standards MT Updated High-Level Information* provides a summary of approved change requests for the release. For more information, visit [Standards Releases](#) on [www.swift.com](#).
- The [MyStandards](#) platform provides an overview of the changes between the current and the new MT and MX releases. A swift.com account is required to access the platform. At a minimum, customers need a MyStandards **Lite** payable licence to view the comparison for a message from one Standards release to the next. For more information, see [MyStandards](#) on page 124.

How to view changes in the Standards Release Guide

1. Go to the Standards MT [page](#) on the [Knowledge Centre \(User Handbook\)](#).
2. Click the link for the *Standards Release Guide*.
3. On the **Standards Release Guide** page, click the link to save the zip file locally.
4. Unzip the file and click `index.htm`.
The Standards Release Guide window opens.



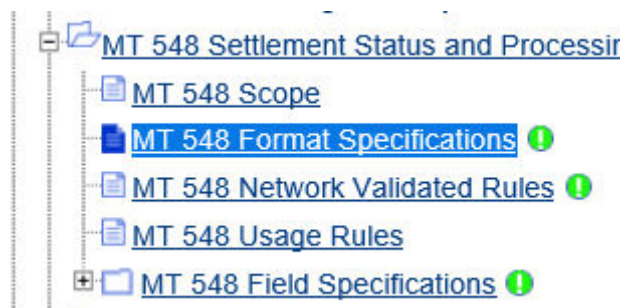
5. Click **Welcome** to view a summary of the changes per category.
Click **Help and feedback** for more information about how to use the guide.
6. Click **List of books** and select the message category and volume (if appropriate) that you want to view. Changes are highlighted in both html and pdf versions. In the html version, you can move from one change to the next using the arrow buttons. You can also click the **Home** icon to return to the main page.



7. Specific changes are clearly marked.

Optional Sequence C Penalties				
M	16R			Start of Block
O	69a	STAT	Period	Statement Period
M	22F	CODE	Indicator	► Penalty List Type Complete/Updates Indicator

8. Icons also appear in the left-hand navigation pane to highlight changes:
- A green icon indicates updated information.
 - A blue icon indicates new information.
 - A red icon indicates deleted information.



9. You can also view the changes in the pdf version. They are summarised in the *Summary of Changes* topic, with links to the changed messages. Changes are also identified in the bookmarks: [Updated], [Inserted], or [Deleted].

Related information

[Standards documentation](#) on page 123

A.6.2.4 Standards documentation

Swift provides comprehensive documentation about Standards on the [Knowledge Centre](#). These documents are public. A swift.com account is not required, except for the *Message Format Validation Rules*.

Standards MT documentation

The Standards MT documentation on the [Knowledge Centre](#) includes the following:

- **General Field Definitions Plus**
This online reference provides an index of messages, fields, qualifiers, codes, definitions, and error codes for messages, including the ISO 15022 messages. Each index entry links to additional information that is specific to that entry. For example, each indexed message links to detailed information about the specific message type, including the scope, the format, and the related fields.
This information is also available in the Standards MT Online Help that is available in Alliance Cloud Message management.
- **General Information**
This document provides information about all Standards MT (message type) categories, and explains the general rules, conventions, and principles for the Standards MTs.
- **Message Format Validation Rules**
The Message Format Validation Rules (MFVR) describes the FIN messages text validation rules to be implemented with the Standards release.
- **Message Reference Guide**
Message Reference Guides are available per message category. Each guide contains the message text standards, including a detailed description of the scope, the format specifications, the rules, the guidelines, and the field specifications of each message type.

- **Standards Release Guide**

The Standards Release Guide (SRG) for Standards MT describes the changes for the next version of the Standards messages. This document provides information about format specifications, rules, guidelines, and field specifications.

- **Usage Guidelines**

The usage guidelines explain how to use message standards. In addition, the document identifies specific issues that relate to message standards, and provides clarification (and examples) of message standards.

Standards MX documentation

The Standards MX documentation on the [Knowledge Centre](#) includes the following.

These documents describe base messages only. Usage Guidelines are not currently included.

- **General Information**

This document describes the Swift Standards MX messages (MXs) and explains the concept of XML for MX messages and the structure and function of these messages.

- **Message Definition Reports and Schemas**

These documents provide information about the use of the messages per category (such as Cash Management or Payments Initiation) and includes, for example, business scenarios and message flow. They also provide details about the messages.

A.6.2.5 MyStandards

[MyStandards](#) is a collaborative web platform that is used to manage standards definitions and industry usage in an efficient way.

The MyStandards service also includes the MyStandards Usage Guideline Editor, an offline application that makes it possible for users to define and maintain their own usage guidelines. MyStandards also lets users view the Standards releases and change requests.

A swift.com account is required to access the platform. At a minimum, customers need a MyStandards **Lite** payable licence to view the comparison for a message from one Standards release to the next. MyStandards also offers other additional features that require a payable licence. See the [MyStandards Service Description](#).

The [MyStandards User Guide](#) explains how to use the platform, including how to get started and how to manage the base standards.

MyStandards Readiness Portal

This portal is a web application built on top of MyStandards that simplifies customer onboarding and migration by providing customer-facing standards testing capabilities. It provides a tailor-made experience to customers, including an advanced message validation service and direct links to relevant documentation in MyStandards.

For more information, see [MyStandards Readiness Portal User Guide](#).

A.7 Unsupported Messages and Exceptions in Alliance Cloud

This topic lists the FIN and MX messages that are currently not supported in Alliance Cloud. It also describes the messages that can be used only under certain conditions.

In the following tables, *Incoming* system messages are messages that your institution receives from Swift through Alliance Cloud. *Outgoing* system messages are message that your institution sends to Swift using Alliance Cloud.

FIN system messages not supported in Alliance Cloud

Message type	Message name	Direction
fin.008	System Request to Quit	Incoming
fin.009	System Request to Logout	Incoming
fin.020	Retrieval Request (Text and History)	Outgoing
fin.024	Bulk Retrieval Request	Outgoing
fin.026	FINCopy Bulk Retrieval Request (For Central Institutions only)	Outgoing
fin.027	FINCopy Bulk Retrieval Response (For Central Institutions only)	Incoming
fin.028	FINCopy Message Status Request (For Central Institutions only)	Outgoing
fin.029	FINCopy Message Status Report (For Central Institutions only)	Outgoing
fin.041	Select Status Request for FIN	Outgoing
fin.047	Delivery Instructions Redefinition Request	Outgoing
fin.077	Additional Selection Criteria for FIN	Outgoing
fin.096	FINCopy to Server Destination Message	Incoming
fin.097	FINCopy Message Authorisation/Refusal Notification	Outgoing

Note *The fin.072 message (Test Mode Selection) is not supported for manual creation in the Alliance Cloud GUI. This message is sent automatically by Alliance Cloud in the context of future mode. It is used to specify the mode of the next FIN test session. This message is a billable system message. For more information, see [Future mode](#) on page 118.*

FIN system messages sent from the back office

Only the following system messages can be sent from the back office (using an application channel). Other system messages sent by the back office that are not in this table will be rejected by Alliance Cloud.

Message type	Name
fin.022	Retrieval Request (History)
fin.031	Session History Request
fin.032	Delivery Subset Status Request
fin.035	Delivery Instruction Request
fin.037	Time Zone Status Request
fin.044	Undelivered Report Rules Redefinition
fin.045	Daily Check Time Change Request
fin.046	Undelivered Message Report Request
fin.048	Undelivered Report Rules Request
fin.049	Daily Check Report Time Query
fin.070	Undelivered SSI Update Notification Report Request

Message type	Name
fin.073	Message sample request
fin.074	Broadcast Request
fin.090	User-to-Swift Message

MX system messages not supported in Alliance Cloud

Message type	Name	Direction
xsys.001.001	Y-Copy Authorisation or Refusal	Outgoing
xsys.006.001	Input Channel List Report Request	Outgoing
xsys.007.001	Input Channel List Report	Incoming
xsys.008.001	Queue Status Report Request	Outgoing
xsys.008.001	Queue Status Report Request	Outgoing
xsys.009.001	Queue Status Report	Incoming
xsys.009.001	Queue Status Report	Incoming
xsys.009.001	Queue Status Report	Incoming
xsys.013.001	Bulk Retrieval Request	Outgoing
xsys.014.001	Bulk Retrieval Report	Incoming
xsys.015.001	Retrieval Request	Outgoing
xsys.015.001	Retrieval Request	Outgoing
xsys.016.001	Retrieval Report	Incoming
xsys.016.001	Retrieval Report	Incoming
xsys.018.001	Session History Report Request	Outgoing
xsys.019.001	Session History Report	Incoming
xsys.024.001	Y-Copy Status Request	Outgoing
xsys.025.001	Y-Copy Status Response	Incoming
xsys.026.001	Output Channel List Report Request	Outgoing
xsys.027.001	Output Channel List Report	Incoming
xsys.028.001	Update Queue Sharing Mode Request	Outgoing

MX system messages with exceptions

Users can send the xsys.004.001.01 (Undelivered Traffic Report Request) system message, but the RqstrPttrn field is mandatory. This field is used to restrict the report of undelivered messages or files to the DNs (Distinguished Names) sent by Requestor that matches the RqstrPttrn.

This field contains the requestor DN. This can be a full DN or a pattern. The pattern is a wildcard that matches all Requestors below a certain node. It can have the wildcard character "*" only as the last character in the last node.

An example of a full wildcard RqstrPttrn is as follows:

`*, o=bankbebb, o=swift`

An example without wildcards is as follows:

o=bankbebb, o=swift

Limitation for ESMIG bulked messages

You cannot manually create messages with a Business File Header (BFH). Although the request type head.002 is visible in the GUI, you can only send messages with a BFH using automated flows. These messages must use the format AnyXML. The MX format is not supported for these messages.

This limitation applies to both ESMIG services:

- esmig.t2.iast (store-and-forward mode (SnF))
- esmig.t2.ia (real-time mode)

A.8 Token-Based Certificates and Channel Certificates

When connecting over the Internet and for users connecting to Alliance Cloud, a personal token must be used. For application-to-application flows, when connecting over Swift's multi-vendor secure IP network (MV-SIPN), a personal token or channel certificate can be used. The use of a channel certificate is optional.

Personal tokens are only supported on Windows. Channel certificates are supported on Windows and Red Hat Linux.

Token-based certificates

A **token-based certificate** is a certificate that resides on a personal token. A personal token, also called USB token or physical token, is a piece of hardware that provides a means for Swift to authenticate the identity of a user or an application. The token includes PKI credentials that the owner of the token has generated. The PKI credentials are used to create digital signatures that allow the owner of the token or the application itself to be identified. The token is personal and must not be shared with another user. It is protected by a password that the owner of the token must keep private.

How to renew personal token certificates

There is no automatic renewal process for personal token certificates and keys. Manual renewal must occur at least once every 24 months. The token is ready for renewal as of 90 days before its expiry date.

When the certificate expiry date is less than 3 months (90 days) away, a warning message is displayed during login.

The personal token user uses the Swift Certificate Centre to renew the token. If the token is not renewed in time, then the token expires.

If a token has expired, then the token can only be reset, see the [Swift Certificate Centre Portal User Guide](#). However, its certificate can be recovered by using the SwiftNet Online Operations Manager, see the [SwiftNet Online Operations Manager User Guide](#). See also article [5018261](#).

Channel certificates

A **channel certificate** is an encrypted, disk-based profile file that provides a means for Swift to authenticate the identity of an application. Alliance Cloud supports channel certificates as an alternative means to physical tokens.

The channel certificate only secures the connection from Alliance Cloud application channel(s) to the Alliance Cloud server in Swift's central infrastructure. In addition, Swift uses channel certificates to generate non-repudiation evidence of the emission of a business message from an Alliance Cloud customer to the Alliance Cloud server at Swift.

See also [Channel Certificate Recovery](#) on page 55.

A.9 Application Channels

Application channels exist both in the Alliance Cloud connectivity option that a customer uses and in Alliance Cloud. Customers must configure application channels in both places. They are not needed by customers that do not connect their back-office engines to Alliance Cloud. The channel definitions in the Alliance Cloud connectivity option and Alliance Cloud must have the same Distinguished Name (DN) for the connection to work. SIL, the , or the API client is installed and configured on the customer's premises. The application channel configuration is done in the Admin centre by the Message management administrator.

Application channels require a certificate. This certificate is used to secure the connection to Alliance Cloud. This certificate can be hosted on a token or on a disk. Disk certificates (also called channel certificates) require access through multi-vendor secure IP network (MV-SIPN). For MV-SIPN, customers must order Alliance Connect. See "Set up the Environment for Alliance Cloud" in [Alliance Cloud Getting Started](#).

An application channel allows Alliance Cloud to receive messages and files to be sent to correspondents from the Alliance Cloud connectivity option. Application channels are also used to send messages and documents (such as reports and archive copies) to the Alliance Cloud connectivity option. Customers can configure these actions in the message workflows and archive messages in the Admin centre.

An application channel has the following characteristics:

- It is owned by an institution.
- It is for one business entity.
- It can be linked to one unit or to no unit.
- it can be either bi-directional or only to send messages and documents to the Alliance Cloud connectivity option.

An application channel does not have a role or permissions.

Each application channel is composed of a name and an optional description. It is identified by a Distinguished Name (DN), which corresponds to the DN configured for that Alliance Cloud connectivity option instance.

An institution's security officers must first create and authorise a DN in SwiftNet Online Operations Manager for each application channel. The application channel is created in the Alliance Cloud Admin centre module, using this same DN to identify it. This DN is then added to the Alliance Cloud connectivity option.

Important If your institution plans to use the active/standby feature for the Alliance Cloud connectivity option instances, then you must create the application channels in Alliance Cloud using the Common DN used in O2M (ignoring the numbered common name segment, such as %1). For more information, contact your institution's administrator for your Alliance Cloud connectivity option.

Important If your institution plans to use the archive feature of Alliance Cloud, then you must use an application channel that does not allow outgoing messages in your archiving configuration.

Managing application channels in Alliance Cloud

A Message management administrator can add, modify, and delete an application channel.

An application channel with the status **Active** can connect to the Alliance Cloud platform. An inactive application channel can still be used in the message workflow. As a result, new messages will still be assigned to that application channel and will be waiting for distribution in the Alliance Cloud platform.

An application channel with the status **Inactive** cannot connect to the Alliance Cloud platform.

An application channel cannot be deleted if it is used in any message workflow (active or inactive) or in the archive messages configuration.

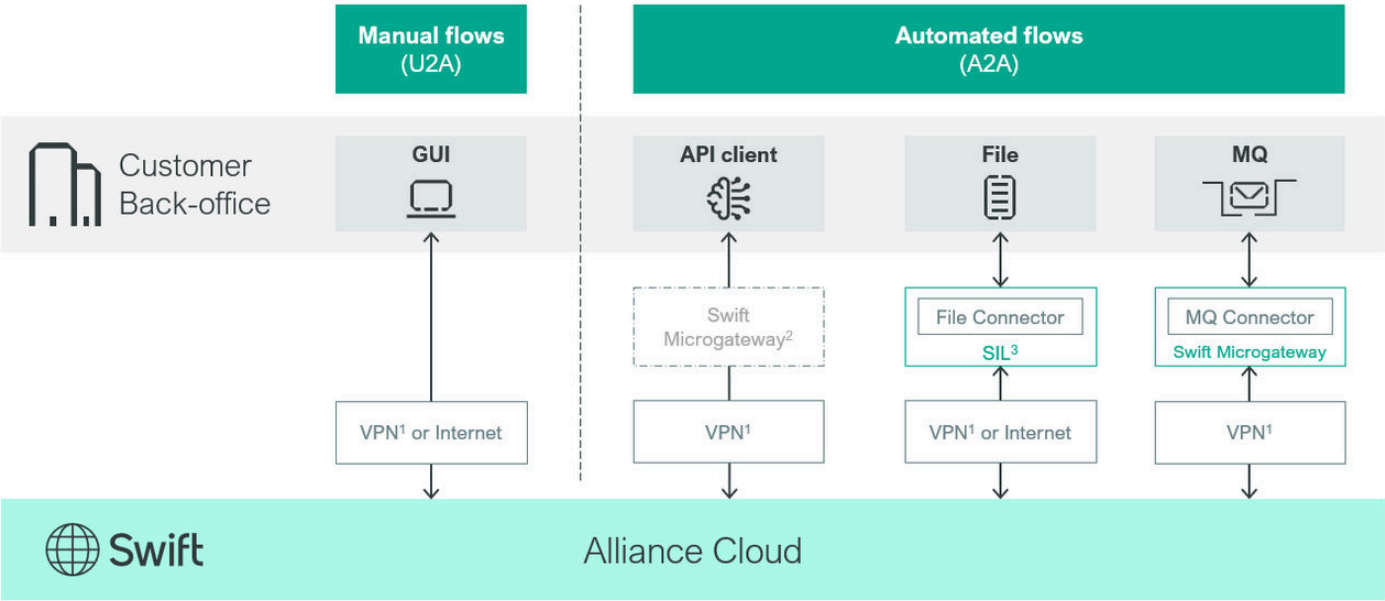
Related information

[Add an Application Channel in Alliance Cloud](#)

A.10 Alliance Cloud Connectivity Options

The following options are available, which enable customers to set up automated message exchange between back-office applications and Alliance Cloud:

Option	Description	Connectivity	More information
API Connector connecting through Swift Integration Layer	The API Connector will go out of support at the same time as the Swift Integration Layer in June 2026. You can replace it with the Swift Messaging API.	- Internet - VPN	API Connector documentation on the Knowledge Centre Knowledge Base article 6000466 - Managing the SIL Sunset
Alliance Cloud Connectors:	File Connector - available during the third quarter of 2025 File-based back-office integration	- Internet - VPN	Available mid-2025
	MQ Connector IBM MQ back-office integration	VPN	MQ Connector Release Letter Alliance Cloud MQ Connector Installation and Configuration Tasks on page 82
Swift Messaging API	A REST API, which serves as a bidirectional connector for API clients to exchange messages with Alliance Cloud using REST endpoints.	VPN	Swift Messaging API Getting Started



1	Alliance Connect (on premise VPN devices) or Alliance Connect Virtual (VPNs hosted in a Public Cloud)
2	Optional
3	Swift Integration Layer (SIL) will be end of support by 30 June 2026.

Legal Notices

Copyright

Swift © 2025. All rights reserved.

Restricted Distribution

Do not distribute this publication outside your organisation unless your subscription or order expressly grants you that right, in which case ensure you comply with any other applicable conditions.

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

Translations

The English version of Swift documentation is the only official and binding version.

Trademarks

Swift is the trade name of S.W.I.F.T. SC. The following are registered trademarks of Swift: 3SKey, Innotribe, MyStandards, Sibos, Swift, SwiftNet, Swift Institute, the Standards Forum logo, the Swift logo, Swift GPI with logo, the Swift GPI logo, and UETR. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.