



Service

Support

Secure Channel User Guide

This guide describes how to use the Secure Channel application. It provides procedures for how to register as a security officer, manage your secure code cards, manage SWIFTNet offline interventions, manage security officers, and view SWIFT interface licence keys.

09 February 2010

Table of Contents

Preface	3
1 Overview	4
1.1 About Secure Channel	4
1.2 Secure Channel Functionality	4
1.3 Secure Channel Profiles	5
2 For SWIFTNet Security Officers	7
2.1 Required Browser Configuration	7
2.2 How to Manage Secure Code Cards	7
2.3 How to Submit SWIFTNet Offline Interventions	14
2.4 How to Manage Security Officers	23
3 For Alliance Security Officers	32
3.1 How to Register as an Alliance Security Officer	32
3.2 How to View Your Alliance Licence Keys	33
Legal Notices	35

Preface

About this document

This guide describes how to use the Secure Channel application. It provides procedures for how to register as a security officer, manage your secure code cards, manage SWIFTNet offline interventions, manage security officers, and view SWIFT interface licence keys.

Customers can find the latest available version of this document at www.swift.com > Support > Secure channel.

Audience

This document is for the following SWIFT audiences:

- SWIFTNet security officers, who use Secure Channel to manage secure code cards, register and manage security officers, and manage SWIFTNet offline interventions
- Alliance security officers, who use Secure Channel to view SWIFT interface licence keys

Terminology

This document contains terms that are consistent with SWIFT terminology as defined in the SWIFT Glossary.

Significant changes

The following tables list all significant changes to the content of the *Secure Channel User Guide* since the February 2008 edition. These tables do not include editorial changes that SWIFT makes to improve the usability and comprehension of the document.

New information	Location
<p>The new Manage security officers tab allows you to do the following tasks:</p> <ul style="list-style-type: none"> • view all security officers within a PKI hierarchy • register, terminate (deregister), and update a SWIFTNet security officer 	<p>2.4, "How to Manage Security Officers" on page 23</p>

Related documentation

- Knowledge Base FAQ, [tip 2119358](#), Secure Channel
- *Swift.com Registration and Administration User Guide* at www.swift.com > Support > Secure channel, Useful links

The latest version of Knowledge Base documentation is available at www.swift.com > Support > Knowledge base.

1 Overview

Introduction to the application

Secure Channel is a SWIFT application for security officers. Secure Channel allows registered security officers to manage secure code cards, and manage SWIFTNet offline interventions. Secure Channel allows Alliance security officers to view SWIFT interface licence keys.

1.1 About Secure Channel

Secure Channel access

Secure Channel is accessible from www.swift.com > Support > Secure channel. You must be registered for swift.com online services to access Secure Channel.

Secure Channel benefits

Secure Channel:

- replaces the SWIFTNet Offline Intervention Form (SOIF), and provides a more efficient and automated means to process offline interventions. Requests are made online through the Secure Channel, and you can download the re-issued activation secrets to your SWIFTNet operational environment.
- gives SWIFTNet security officers an overview of all the security officers in their institution and allows them to make appropriate registration changes online instead of through e-forms
- improves the way Alliance interface software licence keys are distributed. With Secure Channel, licence keys are no longer distributed on paper. The Alliance security officers can see the interface licence keys online.

1.2 Secure Channel Functionality

Description

Secure Channel provides SWIFTNet functionality and Alliance functionality.

SWIFTNet PKI functionality

SWIFTNet PKI security officers with a secure code card can use the SWIFTNet PKI functionality to submit the following types of SWIFTNet Offline Intervention requests:

- revoke certificate
- recover certificate
- cancel recovery of certificate
- reissue of PKI activation secrets
- reissue SWIFTNet Link Import file
- reissue SWIFTNet Link Import file with SWIFTNet Link certificate recovery
- unlock SWIFTNet Link Import file
- revocation and deactivation of a distinguished name

Requests for the generation of new secrets (PKI activation secrets, or SWIFTNet Link installation secrets) are sent to the customer's operational environment through SWIFTNet. A standard internet browser is required to collect these secrets.

Security officers can also submit a Non-Repudiation Verification Request . SWIFT sends the response by courier or by fax.

Alliance functionality

Users defined as left security officer (LSO) or right security officer (RSO) in their profile can access the Alliance passwords section. The section displays the master and initialisation licence keys for the following SWIFT interfaces:

- CASmf
- Alliance Access
- Alliance Entry
- Alliance Gateway
- PC Connect
- MQSA
- Alliance RMA
- Alliance Starter Set
- Alliance Messenger stand-alone

Security officer registration functionality

SWIFTNet PKI security officers with a secure code card can use this functionality to do the following tasks:

- register new security officers
- update their own contact details
- remove existing security officer

1.3 Secure Channel Profiles

Description

The Secure Channel interface that is displayed to you depends on your user profile, as set up in the two "How to Register" sections in this guide:

- If you are registered as SWIFTNet security officer for both the Live and the ITB network, and also have the role of Alliance security officer (LSO, or RSO, or both) selected in your user profile, then you see the full functionality of the application as shown in the following figure. The first two tabs are for SWIFTNet offline intervention requests, and the third tab is for viewing SWIFT interface licence keys.
- If you are registered as SWIFTNet security officer for the Live network, then you see the **SWIFTNet Production** tab.
- If you are registered as SWIFTNet security officer for the ITB network, then you see the **SWIFTNet ITB** tab.

- If you have the role of Alliance security officer (LSO, or RSO, or both) selected in your user profile, then you see only the **Alliance Passwords** tab.



2 For SWIFTNet Security Officers

Introduction

SWIFTNet security officers can use Secure Channel to:

- manage secure code cards
- submit SWIFTNet offline interventions
- maintain security officers

During the undertaking process when you join SWIFT, either you register two initial security officers or you define PKI delegation and the security officers of another institution (the administering institution) manage your PKI.

2.1 Required Browser Configuration

Prerequisites

In order for the online application to work correctly, especially when working with secure code cards, the following setup of your internet browser is required:

- Java Runtime must be installed with version 1.4 or higher. For information about how to download Java, see tip [2128633](#).
- The browser pop-up blocker must be disabled.
- The browser must accept cookies.

Tip Before accessing the Secure Channel application, it is good practice to delete your temporary internet files and close all browser windows.

2.2 How to Manage Secure Code Cards

Description

The SWIFTNet (PKI) security officers must have the secure code card to submit SWIFTNet Offline Interventions through the Secure Channel application.

Note Only SWIFTNet security officers need to receive this card.

Every SWIFTNet security officer receives a secure code card for each SWIFTNet environment for which they are registered (for example, LIVE, ITB or both). The card contains highly confidential information and is strictly for personal use only. You cannot use the secure code card of another security officer.

How to read the card

The secure code card columns are labelled "A" to "H", from left to right. The rows are labelled "1" to "8", from top to bottom. A cell is uniquely referenced by its column and row labels. In the following example of a secure code card, the cell "E3" contains the value "2FC":

	A	B	C	D	E	F	G	H	
1	PF5	U8T	3JQ	K6F	F2V	4Y9	68L	5TB	1
2	BCZ	NSD	DHN	5QX	2EN	ZD6	J6M	39D	2
3	V4A	MED	NFY	5VB	2FC	L7X	QAL	FN7	3
4	GCG	NLQ	DXC	VL9	Y2T	XDS	C9Y	UVG	4
5	962	NRY	ST2	QX7	V7J	XBA	UGN	SRS	5
6	KJV	VTG	SVC	A37	BBH	EUL	YCD	2XF	6
7	K5Y	8G4	RYC	T59	KHC	DMS	2CJ	9QU	7
8	P53	AJ4	HPJ	HVY	5S9	EMR	GEB	RH6	8
	A	B	C	D	E	F	G	H	

TAN Table id: 1.13803

Overview of Secure Channel procedures

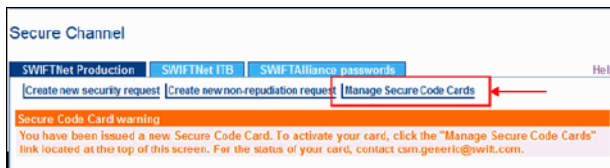
Security officers can activate, lock, unlock, and revoke a card.

2.2.1 Activating a Card

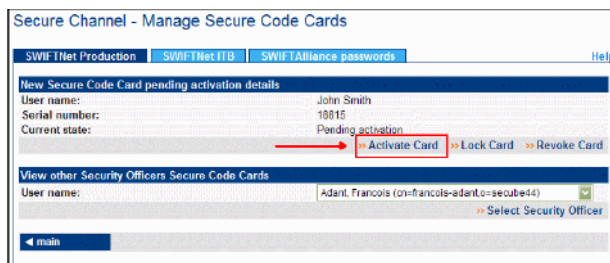
To activate your card

Activate your secure code card as soon as you receive it:

1. In Secure Channel (www.swift.com > Support > Secure channel), click **Manage Secure Code Cards**.



2. Click **Activate Card** under the heading **New Secure Code Card pending activation details**.



The **Secure Channel - Activate Card** screen appears.

- In the Enter cell values row, type your password values in the three columns. To do this, compare the values listed in the Requested cells field (C1, B3, C3) against your Serial Number table, as illustrated in the following diagram. The values are not case sensitive.

Secure Channel - Activate Card

SWIFTNet Production | SWIFTNet ITB | SWIFTAlliance passwords | Help

Secure Code Card details

Environment: Production (Pilot or Live services)
 Requesting Security Officer: John Smith
 Institution BICB: SECUBE44
 User name: John Smith
 Serial number: 18815
 Current state: Pending activation

Request signature

Sign your request by entering the requested cell values from your Secure Code Card.

Serial number: 18815

Requested cells: C1 - B3 - C3

Enter cell values: 3jq - med - nfy

Operation confirmation

The logged user declares to have full capacity and authority to make this request on behalf of the above mentioned institution. Activating the Secure Code Card will allow me to submit security requests (SWIFTNet Offline Interventions).

I agree with the request terms described above

cancel | reset | submit

	A	B	C	D	E	F	G	H	
1	PF5	U8T	3JQ	K6F	F2V	4Y9	68L	5TB	1
2	BCZ	NSD	DHN	5QX	2EN	ZD6	J6M	39D	2
3	V4A	MED	NFY	5VB	2FC	L7X	QAL	FN7	3
4	GCG	NLQ	DXC	VL9	Y2T	XDS	C9Y	UVG	4
5	962	NRV	ST2	QX7	V7J	XBA	UGN	SRS	5
6	KJV	VTG	5VC	A37	BBH	EUL	YCD	2XF	6
7	K5Y	8G4	RYC	T59	KHC	DMS	2CJ	9QU	7
8	P53	AJ4	HPJ	HVY	5S9	EMR	GEB	RH6	8
	A	B	C	D	E	F	G	H	

- Read the Operation confirmation text, then click the **I agree with the request terms described above** box.

The following screen appears, confirming that you have activated your card successfully.

Secure Channel - Activate Card

SWIFTNet Production | SWIFTNet ITB | SWIFTAlliance passwords | Help

The following Secure Code Card operation has been successfully performed.

Secure Code Card details

Environment: Production (Pilot or Live services)
 Requesting Security Officer: John Smith
 Institution BICB: SECUBE44
 User name: John Smith
 Serial number: 18815
 Current state: Active

continue

- Click **submit**.
- Click **continue** if you want to perform another Secure Channel operation.

2.2.2 Locking a Card

Introduction

If you suspect that your secure code card security is compromised, then you must lock the card. A locked card is in a temporary state until you either unlock or revoke it.

You can lock your own card or the card of another security officer in your institution. You can lock cards that show their Current state as Active or Pending activation.

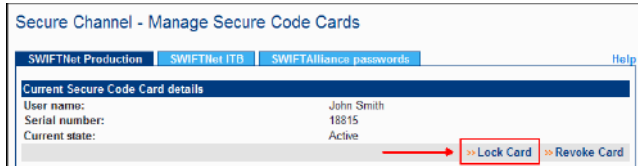
To lock a card

To lock a secure code card, do the steps that follow:

1. In Secure Channel, click **Manage Secure Code Cards**.

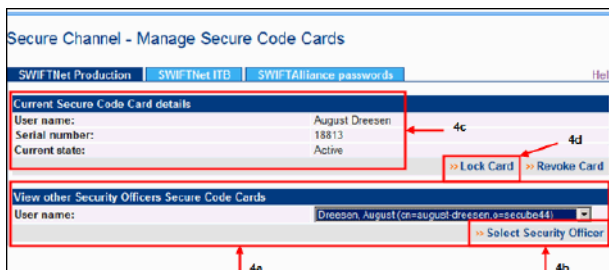


2. To lock your own card, click **Lock Card**.



3. To lock the card of other security officers:
 - a. Select the security officer from the User name drop-down list, under the section **View other Security Officers Secure Code Cards**.
 - b. Click **Select Security Officer**.
 - c. The top half of the screen changes and shows the secure code card details of the security officer to lock. Check the details to make sure that you lock the correct secure code card.
 - d. Click **Lock Card**.

The **Secure Channel - Lock Card** page appears:



4. In the Enter cell values row, type your password values in the three columns. To do this, compare the values listed in the Requested cells field (F5, A6, A5) against your Serial Number table. The values are not case sensitive.

	A	B	C	D	E	F	G	H	
1	PF5	U8T	3JQ	K6F	F2V	4Y9	68L	5TB	1
2	BCZ	NSD	DHN	5QX	2EN	ZD6	J6M	39D	2
3	V4A	MED	NFY	5VB	2FC	L7X	QAL	FN7	3
4	GCG	NLQ	DXC	VL9	Y2T	XDS	C9Y	UVG	4
5	962	NRV	ST2	QX7	V7J	XBA	UGN	SRS	5
6	KJV	VTG	5VC	A37	BBH	EUL	YCD	2XF	6
7	K5Y	8G4	RYC	T59	KHC	DMS	2CJ	9QU	7
8	P53	AJ4	HPJ	HVY	5S9	EMR	GEB	RH6	8
	A	B	C	D	E	F	G	H	

- Read the Operation confirmation text, then click the **I agree with the request terms described above** box.

- Click **submit**.

The following screen appears, confirming that you have locked the card successfully:

- Click **continue** to do another Secure Channel operation.

2.2.3 Unlocking a Card

Introduction

To unlock a card, your Current state must show Active. You can unlock a secure code card that shows its Current state as Locked or Locked at activation.

You cannot unlock your own card. You must ask a security officer in your institution to unlock your card.

To unlock a secure card

To unlock a secure code card:

- In Secure Channel, click **Manage Secure Code Cards**.

- Select the security officer from the **User name** drop-down list, under the section **View other Security Officers Secure Code Cards**.

- Click **Select Security Officer**.
- Click **Unlock Card**.

The **Secure Channel - Unlock Card** page appears

Request signature
Sign your request by entering the requested cell values from your Secure Code Card.

Serial number: 18815

Requested cells: B5 - F6 - A3
Enter cell values: nry - eu1 - v4a

Operation confirmation
The logged user declares to have full capacity and authority to make this request on behalf of above mentioned institution. By unlocking the card the owner will be able again to submit new security requests.

I agree with the request terms described above.

5. this, compare the values listed in the Requested cells field (B5, F6, A3) against your Serial Number table. The values are not case sensitive.

	A	B	C	D	E	F	G	H	
1	PF5	U8T	3JQ	K6F	F2V	4Y9	68L	5TB	1
2	BCZ	NSD	DHN	5QX	2EN	ZD6	J6M	39D	2
3	V4A	MED	NFY	5VB	2FC	L7X	QAL	FN7	3
4	GCG	NLQ	DXC	VL9	Y2T	XDS	C9Y	UVG	4
5	962	NRV	ST2	QX7	V7J	XBA	UGN	SRS	5
6	KJV	VTG	5VC	A37	BBH	EUL	YCD	2XF	6
7	K5Y	8G4	RYC	T59	KHC	DMS	2CJ	9QU	7
8	P53	AJ4	HPJ	HVY	5S9	EMR	GEB	RH6	8
	A	B	C	D	E	F	G	H	

6. Read the **Operation confirmation** text, then click the **I agree with the request terms described above** box.

Request signature
Sign your request by entering the requested cell values from your Secure Code Card.

Serial number: 18815

Requested cells: B5 - F6 - A3
Enter cell values: nry - eu1 - v4a

Operation confirmation
The logged user declares to have full capacity and authority to make this request on behalf of above mentioned institution. By unlocking the card the owner will be able again to submit new security requests.

I agree with the request terms described above.

7. Click **submit**

The following screen appears, confirming that you have unlocked the card successfully:

SWIFTNet Production | SWIFTNet ITB | SWIFT Alliance passwords | Help

The following Secure Code Card operation has been successfully performed.

Secure Code Card details

Environment: Production (Pilot or Live services)

Requesting Security Officer: John Smith

Institution BIC: SECUBE44

User name: August Dreessen

Serial number: 18813

Current state: Active

Additional comments:

8. Click **continue** to do another Secure Channel operation.

2.2.4 Revoking a Card

Introduction

If you suspect that your secure code card security is compromised, then you must either lock the card, or revoke it. The Revoke Card option lets you cancel your secure code card and request a new one. You must activate the new card upon receipt.

You can revoke your own card, or the card of another security officer in the institution.

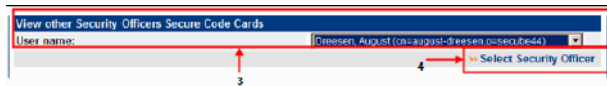
To revoke a secure card

To revoke a secure code card:

1. In Secure Channel, click **Manage Secure Code Cards**.



2. Select the security officer from the **User name** drop-down list, under the section **View other Security Officers Secure Code Cards**.



3. Click **Select Security Officer**.
4. The top half of the screen changes and shows the secure code card details of the security officer to revoke. Check the details to make sure that you revoke the correct secure code card. Also, make sure that the Current state shows either Active, Locked, or Pending Activation.
5. Click **Revoke Card**.

The **Secure Channel - Revoke Card** page appears.

The screenshot shows the 'Secure Channel - Revoke Card' page. It has a header with tabs for 'SWIFTNet Production', 'SWIFTNet ITB', and 'SWIFT Alliance passwords'. The main content area is divided into several sections:

- Secure Code Card details:** Environment: Production (Pilot or Live services); Requesting Security Officer: John Smith; Institution BIC: SECUBE44; User name: August Dreesen; Serial number: 18813; Current state: Active.
- A new Secure Code Card must be generated by SWIFT and delivered to me:** Radio buttons for 'Yes' and 'No'. The 'No' option is selected. A red box highlights this section, with a red arrow pointing to it and the number '7'.
- Additional comments:** A text input field.
- Request signature:** Sign your request by entering the requested cell values from your Secure Code Card. Serial number: 18815. Requested cells: A7 - B4 - A8. Enter cell values: [input: 15y] - [input: n1q] - [input: p53]. A red box highlights this section, with a red arrow pointing to it and the number '8'.
- Operation confirmation:** The logged user declares to have full capacity and authority to make this request on behalf of above mentioned institution. Revoking a Secure Code Card will prevent the owner to submit security requests (SWIFTNet Offline Interventions). The owner will require a new card in order to submit new security requests. A checkbox 'I agree with the request terms described above' is checked.

 At the bottom, there are buttons for 'cancel', 'reset', and 'submit'. A red box highlights the 'submit' button, with a red arrow pointing to it and the number '9'.

6. If you would like a new secure code card issued, then select **Yes to A new Secure Code Card must be generated by SWIFT and delivered to me**.
7. In the Enter cell values row, type your password values in the three columns. To do this, compare the values listed in the Requested cells field (A7, B4, A8) against your Serial Number table. The values are not case sensitive.

	A	B	C	D	E	F	G	H	
1	PF5	U8T	3JQ	K6F	F2V	4Y9	68L	5TB	1
2	BCZ	NSD	DHN	5QX	2EN	ZD6	J6M	39D	2
3	V4A	MED	NFY	5VB	2FC	L7X	QAL	FN7	3
4	GCG	NLQ	DXC	VL9	Y2T	XDS	C9Y	UVG	4
5	962	NRV	ST2	QX7	V7J	XBA	UGN	SRS	5
6	KJV	VTG	SVC	A37	BBH	EUL	YCD	2XF	6
7	KSY	8G4	RYC	T59	KHC	DMS	2CJ	9QU	7
8	P53	AJ4	HPJ	HVY	5S9	EMR	GEB	RH6	8
	A	B	C	D	E	F	G	H	

8. Read the **Operation confirmation** text, then click the **I agree with the request terms described above** box.
9. Click **submit**

The following screen appears, confirming that you have revoked the card successfully:

10. Click **continue** to do another Secure Channel operation.

2.3 How to Submit SWIFTNet Offline Interventions

Description

The SWIFTNet (PKI) functionality of Secure Channel replaces the standard SWIFTNet Offline Intervention Form that a SWIFTNet security officer must submit to request interventions. Examples of interventions include a recovery or a revocation of a PKI certificate or a reissue of SWIFTNet Link activation secrets.

With Secure Channel, requests are done online, and you can download the re-issued activation secrets right into your SWIFTNet operational environment. Secure Channel does not replace Local Registration Application functionality which remains.

What are SWIFTNet Offline Interventions?

SWIFTNet Offline Interventions allow security officers to manage certificates offline in case the online Local Registration Application cannot be used. For example, in the case of lost licence keys, or when activation secrets expire before they have been used.

Two types of SWIFTNet Offline Interventions

We can distinguish between the following two types of intervention requests:

- Security requests that do not require the delivery of new secrets. Requests that do not require new secrets are the following:
 - revoke PKI certificate
 - revoke and deactivate PKI certificate

- cancel recovery of certificate
- unlock SWIFTNet Link Import file
- Security requests which require the delivery of new secrets. There are two types of secrets that can be delivered:
 - New PKI activation secrets (= reference number and authorisation code). In this category, we have the following requests:
 - Recover PKI certificate
 - Re-issue PKI activation secrets
 - New SWIFTNet Link installation secrets (= leftmost and rightmost authentication string). In this category, we have the following requests:
 - Re-issue of SWIFTNet Link import file
 - Re-issue of SWIFTNet Link import file w/ certificate recovery

2.3.1 Creating and Monitoring Security Requests (Without Delivery of New Secrets)

2.3.1.1 Creating New Security Requests

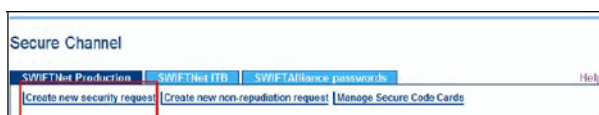
Creating the request

In Secure Channel, select the tab for your environment:

1. • **SWIFTNet Production** if your request is linked with a Live or Pilot service on the production network
- **SWIFTNet ITB** if your request is linked with the integration testbed network

Note You must be registered as a SWIFTNet security officer for the selected network.

2. Click **Create new security request**.



Enter information

1. If you have a case open with the SWIFT Support Centre that is associated with your request, then enter the 8-digit number in the **Case Number** field (optional).

SWIFTNet Production | SWIFTNet ITB | SWIFT Alliance passwords

Create new security request

Step 1 enter information | Step 2 verify and accept | Step 3 view confirmation

Request general information

Environment: Production (Pilot or Live services)

Institution BIC: SECURE44

Request authorization: Single

Case Number: 1

Request details

Request type: Revoke PKI certificate 2 & 3

SNJ or SNL Domain ID, or Distinguished Name: --Select SNJ or SNL Domain ID, or Distinguished Name--

Additional comments

cancel reset 4 5 next

2. Select your Request type from the drop-down list. For example, **Revoke PKI certificate**.
3. Your provisioned SWIFTNet Link and SNJ IDs are provided in the list for selection. Select the SNJ or SWIFTNet Link domain ID, or Distinguished Name that are specific to the request. If you select **Other DN**, then type in a specific Distinguished Name yourself (for example, the DN of a security officer). For example, to revoke the PKI certificate of a security officer, enter the Distinguished Name of that security officer.
4. Enter your comments related to the request in the **Additional comments** box (optional).
5. Click **next**.

Verify and accept

1. Verify that you have the correct information under **Request details**.
2. Verify that the **Serial number** on screen matches the number printed on your personal secure code card.

g19779.gif @ 100% (Background)

SWIFTNet Production | SWIFTNet ITB | SWIFT Alliance passwords

Create new security request

Step 1 enter information | Step 2 verify and accept | Step 3 view confirmation

Request details

Request Number: 20445

Environment: Production (Pilot or Live services)

Institution BIC: SECURE44

Request authorization: Single

Requesting Security Officer: John Smith

Case Number: 1

Request type: Revoke PKI certificate

SNJ or SNL Domain ID, or Distinguished Name: snj01676

Additional comments:

Request signature

Sign your request by entering the requested cell values from your Secure Code Card

Serial number: 18815 2

Requested cells: H8 - E3 - A6

Enter cell values: H8 E3 A6 3

I agree with the request terms described above.

cancel update reset 4 5 submit

3. In the Enter cell values row, type your password values in the three columns. To do this, compare the values listed in the Requested cells field (H8, E3, A6) against your Serial Number table. The values are not case sensitive.

	A	B	C	D	E	F	G	H	
1	PF5	U8T	3JQ	K6F	F2V	4Y9	68L	5TB	1
2	BCZ	NSD	DHN	5QX	2EN	ZD6	J6M	39D	2
3	V4A	MED	NFY	5VB	2FC	L7X	QAL	FN7	3
4	GCG	NLQ	DXC	VL9	Y2T	XDS	C9Y	UVG	4
5	962	NRY	ST2	QX7	V7J	XBA	UGN	SRS	5
6	KJV	VTG	5VC	A37	BBH	EUL	YCD	2XF	6
7	K5Y	8G4	RYC	T59	KHC	DMS	2CJ	9QU	7
8	P53	AJ4	HPJ	HVY	5S9	EMR	GEB	RH6	8
	A	B	C	D	E	F	G	H	

- Read the Request confirmation text, then click the **I agree with the request terms described above box**.
- Click **submit**. All security officers in your institution receive an e-mail message that notifies them of your request.

View confirmation

- Read the final confirmation message.
- Click **main** to return to the Secure Channel home page.

2.3.1.2 Monitoring the Security Request Status

Description of Request States

You can monitor the status of your security request while the SWIFT Customer Security Management department processes it. Possible Request States are as follows:

- **Validation ongoing**

The Request history field initially shows all requests in the "Validation by SWIFT ongoing" state.

- **Pending approval**

If your institution has made a dual authorisation request, then the Request history field shows the status "Request pending approval of second SO". In this case, another security officer has to log on to Secure Channel, click the request, and sign the same request with their secure code card.

- **Completed**

When SWIFT Customer Security Management has processed your request, the Request history shows the state of your request as "Completed".

- **Failed**

In rare cases, if SWIFT cannot process your request, the Request history shows the state of your request as "Failed". SWIFT Customer Security Management sends an e-mail with this status update.

Request Number	Institution BIC8	Request type	Request date	Last update
20446	SECUBE44	Revoke PKI certificate sni01676	2008-01-29	2008-01-29 13:48 UTC
Case Number:				
Request authorization:				
Requesting Security Officer:				
Entity type:				
SNI or SWL Domain ID, or Distinguished Name:				
Request history:				
2008-01-29 13:48 UTC - Validation by SWIFT ongoing				
» Clone request				

To make another similar security request, click **Clone request**. This feature is useful when your request has failed, and you need to re-enter a new request with the same parameters.

2.3.2 Creating and Monitoring Security Requests (With Delivery of New Secrets)

Prerequisites for PC configuration

When requests involve new secrets, the Secure Channel application sends security officers an e-mail at the end of the process to inform them that the request is in the state "pending download". The e-mail contains a link to download the new secrets.

When requests involve new secrets, the Secure Channel application sends security officers an e-mail at the end of the process to inform them that the request is in the state "pending download". The e-mail contains a link to download the new secrets.

The security officer or an operator must open this link in a standard internet browser on a PC that is connected to SWIFTNet.

Note Since the link provided is always the same URL (<https://secure-channel.swiftnet.sipn.swift.com> for the Live/Pilot network or <https://secure-channel-itb.swiftnet.sipn.swift.com> for the integration testbed network), the URL can be stored in the browser favourites or on the desktop of the PC.

The security officer or an operator must open this link in a standard internet browser on a PC that is connected to SWIFTNet.

The PC that you can use to open this link can be:

- an SNL-Host
- a PC that is used for a Browse service
- a dedicated PC on a dial-up connection

The PC *must* have the following configuration:

- The PC must be connected in a LAN segment that connects to a VPN-box. In addition, the IP address of the PC has to be allowed on the VPN-box. This is done by provisioning the IP address of the PC in the VPN-box. Alternatively, you can use a proxy server or work through network address translation (natting) so that the IP address of the PC is translated into another (provisioned) IP address.
- The firewall between the PC and SWIFTNet must be configured for a "Global Approach to Browse Service Access" as described in section 7.1 of the *Network Configuration Tables Guide*:

```
<...> All SWIFTNet Browse Web servers have, or will have, globally unique IP addresses in the subnet range 149.134.0.0 /17 This is a range of IP addresses in CIDR notation. Another notation for their range is 149.134.0.0 mask 255.255.128.0. Their range covers the IP addresses from 149.134.0.0 up to 149.134.127.255 (inclusive). <...>
```

- If the security level of the internet browser is set to "high", then you need to:
 - Add the download URL (<https://secure-channel.swiftnet.sipn.swift.com>) to the trusted sites
 - Enable "META REFRESH" in your internet options

This configuration is not required if the security level of the internet browser is set to "low" or "medium".

2.3.2.1 Creating New Security Requests

Creating the request

In Secure Channel, select the tab for your environment:

- **SWIFTNet Production** if your request is linked with a Live or Pilot service on the production network
 - **SWIFTNet ITB** if your request is linked with the integration testbed network

Note You must be registered as a SWIFTNet security officer for the selected network.

- Click **Create new security request**.



Enter information

- If you have a case open with the SWIFT Support Centre that is associated with your request, then enter the 8-digit number in the **Case Number** field (optional).

 A screenshot of the 'Create new security request' form in the 'Secure Channel' interface. The form is titled 'Create new security request' and has a progress indicator showing 'Step 1: enter information', 'Step 2: verify and accept', and 'Step 3: view confirmation'. The form is divided into three sections:

- Request general information:**
 - Environment: Production (Pilot or Live services)
 - Institution BICB: SECBEE44
 - Request authorization: Single
 - Case Number: [text input field]
- Request details:**
 - Request type: Recover PKI certificate
 - SNJ or SNL Domain ID, or Distinguished Name: Other DN: cn=usar, ou=payments, o=secube44, c=us (circled in red)
- Additional comments:** [text input field]

 At the bottom of the form, there are buttons for 'cancel', 'reset', and 'next' (highlighted with a red circle).

- Select your Request type from the drop-down list. For example, **Recover PKI certificate**.
- Select the SNJ or SWIFTNet Link domain ID, or Distinguished Name that are specific to the request. For example, to revoke the PKI certificate of a security officer, enter the Distinguished Name of that security officer.
- Enter your comments related to the request in the **Additional comments** box (optional).
- Click **next**.

Verify and accept

1. Verify that you have the correct information under **Request details**.
2. In the **Request Download Password** section, enter your own download password. The password must contain at least eight characters, and is case sensitive. It must contain at least one uppercase and one lowercase character, and one number. This download password is used by the operator who has access to the SNL-host or to another PC in the SWIFTNet environment, to view the new secrets when the request is ready for download.

The screenshot shows the 'Create new security request' form in the SWIFTNet Production environment. The form is divided into four main sections:

- Request details:**
 - Request Number: 12517
 - Environment: Production (Pilot or Live services)
 - Institution BIC: SECUBE44
 - Request authorization: Single
 - Requesting Security Officer: John Smith
 - Case Number:
 - Request type: Recover PKI certificate
 - SNL/ or SNL Domain ID, or Distinguished Name: cn=user,ou=payments,os=secube44,o=swift
 - Additional comments:
- Request Download Password:**
 - Please enter a Download Password that you can compose.
 - Download Password: [masked]
 - Re-type Download Password: [masked]
 - The Request Number associated with this Download Password is 12517 - note that you will need to specify both the Request Number, and the Download Password you have just provided, when you proceed with the download of secrets. Your secrets are ready for download when you receive an e-mail stating that your request is pending download.
- Request signature:**
 - Sign your request by entering the requested cell values from your Secure Code Card.
 - Serial number: 18809
 - Requested cells: E4 - C4 - G3
 - Enter cell values: [t] [y] []
- Request confirmation:**
 - The logged user declares to have full capacity and authority to make this request on behalf of the above mentioned institution. There will be a charge of EUR 500 (or EUR 1000 when done in emergency) for every security request that is submitted. Recovery/revocation of SNL certificates and Security Officer registrations/changes are free of charge.
 - I agree with the request terms described here above.

3. In the Enter cell values row, type your password values in the three columns. To do this, compare the values listed in the Requested cells field (E4, C4, G3) against your Serial Number table. The values are not case sensitive.
4. Read the Request confirmation text, then click the **I agree with the request terms described above box**.
5. Click **submit**. All security officers in your institution receive an e-mail message that notifies them of your request.

View confirmation

1. Read the final confirmation message.
2. Click **main** to return to the Secure Channel home page.

2.3.2.2 Monitoring the Security Request Status

Description of Request States

You can monitor the status of your security request while the SWIFT Customer Security Management department processes it. Possible Request States are as follows:

- **Validation ongoing**

The Request history field initially shows all requests in the "Validation by SWIFT ongoing" state.

- **Pending approval**

If your institution has made a dual authorisation request, then the Request history field shows the status "Request pending approval of second SO". In this case, another security officer has to log on to Secure Channel, click the request, and sign the same request with their secure code card.

- **Pending download**

When SWIFT Customer Security Management has processed your request, the Request history shows the state of your request as "Pending download", which means the new secrets are ready for download.

- **Failed**

In rare cases, if SWIFT cannot process your request, then the Request history shows the state of your request as "Failed". SWIFT Customer Security Management sends an e-mail with this status update.

Request Number	Institution BIC8	Request type	Request date	Last update
12517	SECUBE44	Recover PKI certificate cm-user.payments@secube44.o-swift	2007-08-31	2007-08-31
Case Number:				
Request authorization:		Single		
Requesting Security Officer:		JOHN SMITH		
Entry type:		ON		
SNJ or SML Domain ID, or Distinguished Name:		cm-user.payments@secube44.o-swift		
Request history:				
		2007-08-31 12:48 UTC	Validation by SWIFT ongoing	
		2007-08-31 13:04 UTC	Pending download	

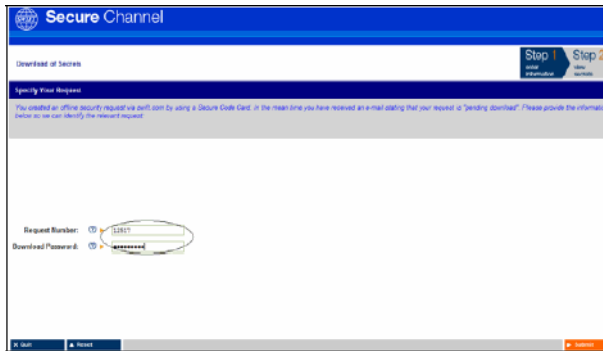
Clone request

2.3.2.3 Downloading the New Secrets

Procedure

1. Verify that your request shows the state as "Pending download". This happens when:
 - The request has moved to the section Requests pending download on the main screen of your application, and the Request history shows the state of your request as "Pending download".
 - The requesting security officer received the following e-mail message. In case of dual authorisation, the approving security officer also receives the message:


```
Dear <Name>,
The following request, created through the SWIFT Secure Channel, has
been approved by SWIFT: <Request ID>
Requesting Security Officer: <Name>
Approving Security Officer: <Name>
Request type: <Name>
In order to collect the requested secrets, please connect to the
following address using your MV-SIPN connection: <URL provided>
To view the request details and history, connect to the <URL provided>
application.
Best regards,
SWIFT Customer Security Management
```
2. Prepare the **Download Password** that was entered when you submitted the request as well as the **Request Number**. Communicate this password and the request number to the operator who will collect the new secrets. If you have access to a PC connected to your SWIFTNet environment, then you can collect the secrets yourself.
3. Click the link that is provided in the e-mail. A screen opens and requests that you enter the **Request Number** and **Download Password**.



4. Click **submit**.
5. The new secrets are displayed on the screen as shown in the following example. The screen layout is different for PKI secrets and for secrets that are required for the SWIFTNet Link installation.

Screen for PKI secrets



Screen for SWIFTNet Link installation secrets



Important SWIFT strongly advises you to save or print the secrets that display on the screen. New secrets can be shown only once. If you close the window, then there is no way to re-display the new secrets apart from re-entering a new security request.

2.4 How to Manage Security Officers

Introduction

This chapter explains the functionality of the **Manage security officers** tab, which allows you to do the following tasks:

- view security officer profiles
- register a new security officer
- terminate (deregister) a security officer
- update your own address details
- view the audit report on registration activities

Secure Channel



Tip The environment tab selected appears in a lighter colour. In the previous screen, this means that SWIFTNet ITB is selected.

Important You define your two initial security officers when you join SWIFT. These security officers receive both online (node and certificate in the Enterprise Directory) and offline (use of Secure Channel) capabilities.

The *register* and *terminate (deregister) a security officer* functions allow you to add or terminate any SWIFTNet security officers as long as at least **two** registered security officers remain. You can terminate your initial security officers and add or terminate additional security officers.

2.4.1 View Security Officer Profiles within a PKI Hierarchy

Description of the Manage security officers tab

The **Manage security officers** tab (www.swift.com > Support > Secure channel), displays the following items:

- the **SWIFTNet PKI hierarchy** (or scope) for the institution BIC of the logged on user
- the **security officer profiles** for all the BICS in the SWIFTNet PKI hierarchy including the following information:
 - **Email address**
 - **Full Name**
 - **BIC**
 - **Registration status**
 - **SCC status**

Secure Channel - Security Officer Profiles

SWIFTNet Production SWIFTNet ITB Help

Logged in user
Swift.com account [alice.smith@swift.com](#) ?

SWIFTNet PKI hierarchy

Institution BIC SWHQBE99
Institution administration status This institution is administering
BIC(s) under administration scope BEBDBE77 BEBDBE88 BEBDBE95 BECQBE23 BECQBE45 BECQBE58 BECQBE59 BECQBE99 COEHBEBB COEVBEBB COEWBEBB COEXBEBB COEYBEBB COEZBEBB COPZBEBB OTHBGRAX OTHBLULL PTSTBEBB PTSWBEBB PTSWBEBB PTSWBEBB SAESVAVA SAESVECA SAESVUVU SMAIBE25 SWBDBEBA SWBDBEBB SWBDBEBC SWBDBEBD SWBDBEBE SWBDBEBF SWBDBEBG SWBDBEBH
Authorisation option Single

Security officer profiles

Email address	Full name	BIC	Registration status	SCC status
bob.armstrong@swift.com	Bob Armstrong	SWHQBE99	Correct	Inactive
alice.smith@swift.com	Alice Smith	SWHQBE99	Correct	Active
william.jones@swift.com	William Jones	PTSTBEBB	Correct	No SCC

Add new security officer ? Add Get SCC status ?

>> [Audit Report](#)

← [homepage](#)

Tip PKI hierarchy includes the following:

- all of the security officers of your own institution
- all of the security officers of the institutions (if any) that have delegated their PKI security to you, known as administered institutions

If you are the security officer of an administering institution, then you can see the security officers of the administered institutions if any.

Tip If the **Registration status** shows anything other than **Correct**, then click the status. A page appears that explains how to correct your registration.

SCC status definitions

Click the status link for **Inactive** or **No SCC** and then follow the recommendations listed on the screen.

- **Active**

The owner has activated the secure code card and can use the card to sign security requests.

- **Inactive**

SWIFT has generated a personal secure code card for the security officer and mailed the card to the person. However the security officer has not yet activated the card with the **Manage Secure Code Cards** function on Secure Channel.

- **No SCC**

SWIFT has not yet generated a personal secure code card for the security officer.

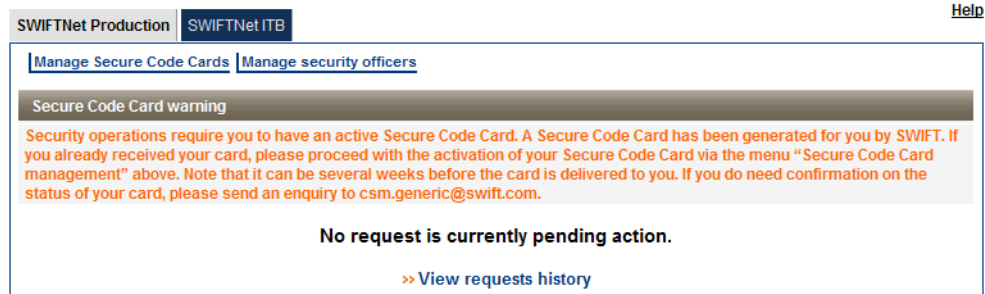
Audit Report

Click **Audit Report** to see all past and ongoing SWIFTNet security officer registration activities. These activities include those from the Undertaking/Joining process.

To view security officer profiles

1. Access Secure Channel at www.swift.com > Support > Secure channel).
2. Security officers for both Production and ITB environments first must select the *SWIFTNet Production* or the *SWIFTNet ITB* environment.

Secure Channel



The previous screen show that the secure code card for the Production environment is not yet activated. The card must be activated first. For more information about how a security officer activates a card, see "Activating a Card" on page 8.

3. Click **Manage security officers**. The ITB environment is selected when the secure code card is activated correctly (**SWIFT ITB**. tab appears in a lighter colour). The warning message is no longer displayed as shown in the following screen.

Secure Channel



The **Secure Channel - Security Officer Profiles** screen appears.

4. To view the latest **SCC status**, click **Get SCC status**. The screen is refreshed.
5. To view the security officer identity, address, and registration details, click the appropriate name under **Full name**.

The **Secure Channel - Security Officer** screen appears.

Secure Channel - Security Officer

Security officer identity	
Institution BIC	SWHQBEBB
Swift.com account	alice.smith@swift.com
First name	Alice
Last name	Smith
Institution name	▶ SWIFT

6. Click **Back to list** to return to the previous screen.

2.4.2 Register a New Security Officer

Three steps to register a new security officer

1. enter information
2. verify and accept
3. view confirmation

Enter information

1. Access Secure Channel at www.swift.com > Support > Secure channel).
2. Security officers for both Production and ITB environments first must select the *SWIFTNet Production* or the *SWIFTNet ITB* environment.
3. Click **Manage security officers**.

The **Secure Channel - Security Officer Profiles** screen appears.

4. Ensure that the new security officer that you want to register is not already registered under **Security officer profiles**.

Security officer profiles			
Email address	Full name	BIC	Registration status
bob.armstrong@swift.com	Bob Armstrong	SWHQBEBB	SWIFTNet SO
alice.smith@swift.com	Alice Smith	SWHQBEBB	SWIFTNet SO
william.jones@swift.com	William Jones	PTSTBEBB	SWIFTNet SO

5. All security officers must have an account on swift.com under the appropriate BIC. If they do not, then an account (or a multi-profile extension of an existing account to more BICs) must be requested. For more information, see the *Swift.com Registration and Administration User Guide* at www.swift.com > Support > Secure channel, Useful links.

To see whether a user is a registered on swift.com, do the following:

- Click your name and BIC in the upper right hand of the screen.
- Click **Manage your profile**.
- Click **User profile** (under **Personal profile**).
- Click **Search users**.
- Click **Start search**.

The search results appear on the screen.

6. Add a user by typing in the complete e-mail address in the **Add new security officer** box.

Security officer profiles			
Email address	Full name	BIC	Registration status
bob.armstrong@swift.com	Bob Armstrong	SWHQBEBB	SWIFTNet SO
alice.smith@swift.com	Alice Smith	SWHQBEBB	SWIFTNet SO
william.jones@swift.com	William Jones	PTSTBEBB	SWIFTNet SO

Add new security officer (?)

7. Click **Add**. In case of a multi-profile swift.com account, you are prompted to select the BIC for which the new security officer must be defined.
8. Complete the mandatory fields (next to an orange triangle).

Secure Channel - Security Officer

SWIFTNet Production		SWIFTNet ITB	
Security officer identity			
Institution BIC	SWHQBEBB		
Swift.com account	john.smith@swift.com		
First name	John		
Last name	Smith		
Institution name	▶ <input type="text"/>		
	<input type="text"/>		
	<input type="text"/>		
Address details			
Building (optional)	<input type="text"/>		
Street	▶ <input type="text"/>		

- In the **SWIFTNet SO** row, select the check box **Check this flag to grant the SWIFTNet SO role to listed person**.

Registration details	
Institution BIC	SWHQBEBB
SWIFTNet SO	<input checked="" type="checkbox"/> Check this flag if you want to grant the SWIFTNet SO role to listed person
<input type="button" value="Back to list"/> <input type="button" value="Save"/>	

- Click **Save**.

Verify and accept

- The **Create new security request** screen appears with details of the request.

Create new security request	Step 1 enter information	Step 2 verify and accept	Step 3 view confirmation
Request details			

- Under **Request signature**, complete the values.
- In the **Enter cell values** row, type your password values in the three columns. For more information, see "Verify and accept" on page 16.

Important Verify that the **Serial number** on screen matches the number printed on your personal secure code card.

- Select the check box **I agree with the request terms described here above**.
- Click **submit**.

Request signature		
Sign your request by entering the requested cell values from your Secure Code Card.		
Serial number:	11860	
Requested cells:	G7 - E7 - B7	
Enter cell values:	5xx - ap2 - hcx	
Request confirmation		
The logged user declares to have full capacity and authority to make this request on behalf of the above mentioned institution. There will be a charge of EUR 500 (or EUR 1000 when done in emergency) for every security request that is submitted. Recovery/revokes of SNL certificates and Security Officer registrations/changes are free of charge.		
<input checked="" type="checkbox"/> I agree with the request terms described here above.		
cancel	update	reset submit

View confirmation

1. The **Create new security request** screen appears to confirm the request.

Create new security request	Step 1 enter information	Step 2 verify and accept	Step 3 view confirmation
Your request has been successfully created. A confirmation e-mail has just been sent to you and other Security Officers administering the concerned institution. Another e-mail will be sent to you when your request status evolves. You can also monitor it via this application.			

2. Click **homepage**.
Pending and recently updated requests are listed on the **Secure Channel** screen.
3. Click a specific **Request Number** for further details.

[Create new security request](#) | [Manage Secure Code Cards](#) | [Manage security officers](#)

Requests pending Swift processing		
Request Number	Institution BIC8	Request type
804518	SWHQBE88	Change security officer profile John Smith (SWHQBE88)

4. Click **Manage security officers** to view the updated **Security officer profiles**.

Next steps by SWIFT

1. SWIFT sends an e-mail to both the requesting security officer and the new security officer to confirm the request.
2. SWIFT completes the security officer registration by the next business day.
3. SWIFT sends the new security officer a personal secure code card by courier service within a few days.

2.4.3 Terminate a Security Officer

Three steps to terminate (deregister) a security officer

1. enter information
2. verify and accept
3. view confirmation

Enter information

1. Access Secure Channel at www.swift.com > Support > Secure channel).
2. Security officers for both Production and ITB environments first must select the *SWIFTNet Production* or the *SWIFTNet ITB* environment.
3. Click **Manage security officers**.

The **Secure Channel - Security Officer Profiles** screen appears.

4. To terminate (deregister) a security officer, click the **Full name** of the person that you want to terminate.

Security officer profiles		
Email address	Full name	BIC
bob.armstrong@swift.com	Bob Armstrong	SWHQBEBB
john.smith@swift.com	John Smith	SWHQBEBB
alice.smith@swift.com	Alice Smith	SWHQBEBB
william.jones@swift.com	William Jones	PTSTBEBB

5. In the **SWIFTNet SO** row, clear the box **Uncheck this flag to remove the SO role for this person**.

Registration details	
Registration status	This user is correctly configured as a SWIFTNet SO on swift.com
SCC status	No SCC was found for this user
Institution BIC	SWHQBEBB
SWIFTNet SO	<input type="checkbox"/> Uncheck this flag if you want to remove the SO role for this person
<input type="button" value="Back to list"/> <input type="button" value="Save"/>	

6. Click **Save**.

Verify and accept

1. The **Create new security request** screen appears with details of the request.
2. Under **Request signature**, complete the values.
3. In the Enter cell values row, type your password values in the three columns. For more information, see "Verify and accept" on page 16.

Important Verify that the **Serial number** on screen matches the number printed on your personal secure code card.

4. Select the check box **I agree with the request terms described here above**.
5. Click **submit**.

View confirmation

1. The **Create new security request** screen appears to confirm the request.
2. Click **homepage**.
Pending and recently updated requests are listed on the **Secure Channel** screen.
3. Click a specific **Request Number** for further details.
4. Click **Manage security officers** to view the updated **Security officer profiles**.

SWIFT completes the security officer termination (deregistration) within minutes. Termination includes the revocation of the secure code card.

2.4.4 Update your Own Address Details

Three steps to update your own security officer details

1. enter information
2. verify and accept
3. view confirmation

Important It is important to maintain your address details. If you need a new secure code card (for example, after a revoke), then SWIFT mails your personal secure code card to this address.

Enter information

1. Access Secure Channel at www.swift.com > Support > Secure channel.
2. Security officers for both Production and ITB environments first must select the *SWIFTNet Production* or the *SWIFTNet ITB* environment.

3. Click **Manage security officers**.

The **Secure Channel - Security Officer Profiles** screen appears.

4. On the **Swift.com account** row, click your e-mail address.

The **Secure Channel - Security Officer** screen appears.



Important You can only update the security officer address details for yourself. You cannot update this information for other security officers.

5. Update the appropriate fields.
6. Click **Save**.

Verify and accept

1. The **Create new security request** screen appears with details of the request.
2. Under **Request signature**, complete the values.
3. In the Enter cell values row, type your password values in the three columns. For more information, see "Verify and accept" on page 16.

Important Verify that the **Serial number** on screen matches the number printed on your personal secure code card.

4. Select the check box **I agree with the request terms described here above**.
5. Click **submit**.

View confirmation

1. The **Create new security request** screen appears to confirm the request.
2. Click **homepage**.
Pending and recently updated requests are listed on the **Secure Channel** screen.
3. Click a specific **Request Number** for further details.
4. Click **Manage security officers**, then either click your e-mail address on the **Swift.com account** row or click your full name under **Security officer profiles** to view the updated address details.

SWIFT completes the update of the address details within minutes.

3 For Alliance Security Officers

Introduction

Alliance security officers can use Secure Channel to view Alliance licence keys.

Alliance security officers must first be registered as Alliance LSO or RSO.

3.1 How to Register as an Alliance Security Officer

Description

This section describes how to register as an Alliance security officer to receive the access rights to the Alliance functionality within the Secure Channel application.

The following are possible assignments of Alliance LSO/RSO roles:

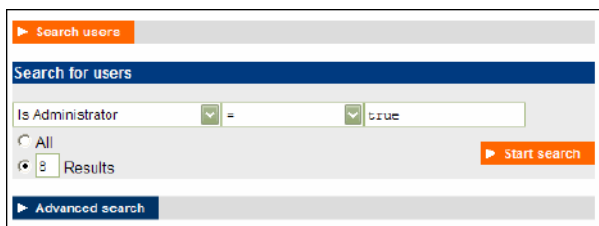
- A first registered user is assigned the *Alliance LSO* role, and a second registered user is assigned the *Alliance RSO* role. This is the typical configuration.
- Both the *LSO* and *RSO* roles are assigned to a single user. This user will be able to see the complete master and initialisation licence keys (part 1 and 2).
- The roles *LSO* and *RSO* are assigned to more than two users. Multiple users have the *LSO* or *RSO* roles.

The swift.com administrator manages all assignments of Alliance LSO/RSO roles. The administrator can assign or revoke the *LSO* and *RSO* roles to and from any registered user within the institution. SWIFT does not perform any intervention or validation.

Procedure

1. You must first be a registered user for the online services on swift.com. To register, open www.swift.com, click Register now. A swift.com administrator in your institution must approve your registration request before you can use the online services.
2. Contact your swift.com administrator to activate your *Is Alliance LSO* or *Is Alliance RSO* role in your user profile.

If you do not know the names of the swift.com administrators for your institution, then go to swift.com > Manage your profile > User profile > Search users. Create the condition "Is Administrator" "=" "true", then click Start search. You can now see the swift.com administrators for your institution or BIC.



The screenshot shows a search interface with the following elements:

- A search bar at the top with a "Search users" button.
- A section titled "Search for users" containing a search criteria field: "Is Administrator" followed by a dropdown arrow, an equals sign, another dropdown arrow, and the value "true".
- Below the search criteria, there are radio buttons for "All" and "Results" (which is selected).
- A "Start search" button is located to the right of the search criteria.
- At the bottom, there is a link for "Advanced search".

Personal information		help
Login	John.Smith@swift.com	
First Name	John	
Last Name	Smith	
Full Name	John Smith	
Registration number	200164883	
Telephone Number	+32 4746	
Telephone Country code	32	
Local phone number	4746	
Is Administrator	True	
Is SWIFTNet LIVE SO		
Is SWIFTNet ITB SO	True	
Is SWIFTAlliance LSO	True	
Is SWIFTAlliance RSO	True	

3.2 How to View Your Alliance Licence Keys

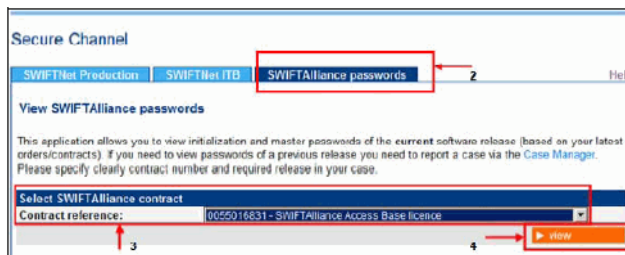
Description

The Alliance functionality on Secure Channel allows you to see the master and initialisation licence keys. These licence keys are required for the installation of Alliance software. SWIFT no longer sends licence keys on paper.

You can see the licence keys for all the contracts that are registered with SWIFT in a particular organisation (BIC8).

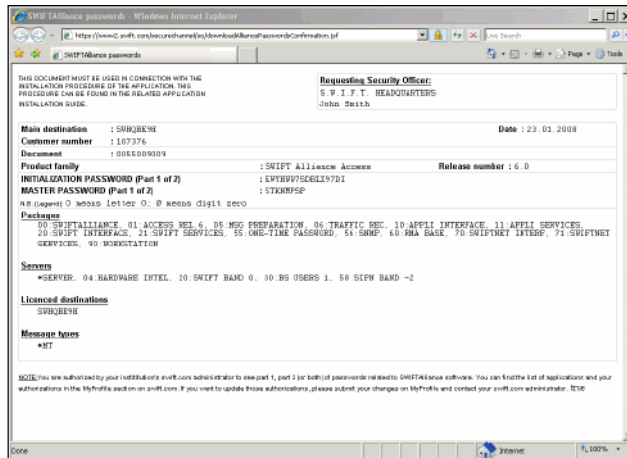
Procedure

1. In Secure Channel (www.swift.com > Support > Secure channel), click the **Alliance passwords** tab.
2. Select your **Contract reference** from the drop-down list, then click **view**.



After selecting "view", the following window pops up which shows the Alliance Licence Keys (and other information such as Packages and Servers) for the contract that you have selected.

Ensure that you have pop-ups enabled in your browser or the new window will not be visible.

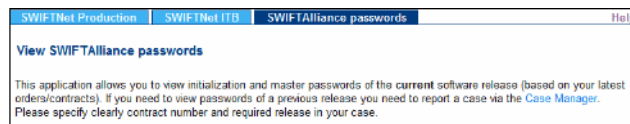


The security officer in the previous example is assigned the role of *Is Alliance LSO*. Therefore this security officer can see Part 1 of the licence keys. A security officer with the role of *Is Alliance RSO* would see part 2 of the licence keys. A security officer with both roles would be able to view both parts (1 and 2) of licence keys.

Important SWIFT strongly advises you to save or print (from the browser window) your current set of licence keys, so that you are able to re-install the current release in the future, if required.

Licence keys from previous releases

Secure Channel only shows the licence keys for the software release that corresponds with your current contract. If you want a password for a previous release, then click **Case Manager** or contact the SWIFT Customer Support Centre.



Legal Notices

Copyright

SWIFT © 2010. All rights reserved.

You may copy this publication within your organisation. Any such copy must include these legal notices.

Confidentiality

This publication may contain SWIFT or third-party confidential information. Do not disclose this publication outside your organisation without the prior written consent of SWIFT.

Disclaimer

SWIFT supplies this publication for information purposes only. The information in this publication may change from time to time. You must always refer to the latest available version on www.swift.com.

Translations

The English version of SWIFT documentation is the only official version.

Trademarks

SWIFT is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: SWIFT, the SWIFT logo, Sibos, SWIFTNet, SWIFTRReady, and Accord. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.