SIRESS

How to update your ASP and FINCopy files for

SIRESS SWIFT services

Version 4.0   June-2015

Contents

1 Introduction

The SIRESS SWIFT FINCopy service ASP file was updated in April 2013. When a service's Application Service Profile (ASP) file or the FinCopy Profile (FCP) files are modified, it is mandatory that all the service participants update the new files on their systems as requested by the service administrators, prior to commencing with any testing and/or live traffic

1.1 What changes in the April 2013 ASP file update?

The April 2013 update for the SIRESS service SRS, changes the service RMA bypass setting to NO. This means that RMA bypass will no longer be possible between service participants so RMA Authorisations must be exchanged and completed before FIN messages can be exchanged.

1.2 What actions must participants take?

SIRESS participants must take the following actions:

1. Change the profile of their SRS Live and Test FINCopy services. This action depends on the FIN interface being used. See section 1.3 for more details.
2. Exchange RMA Authorisation messages with all the SIRESS participants you have a business relationship.

1.3 Changing the FINCopy profile overview

This action depends on the FIN interface being used. Each of these actions is explained in detail later in the document.

- Alliance Access or Alliance Entry users must:
  - download the latest ASP file from swift.com download centre
  - Import and activate the new FINCopy profiles using the FCP files contained within the ASP file.

- Lite and Lite2 users:
  - SWIFT will automatically update the ASP and FCP file and profiles when they are changed.

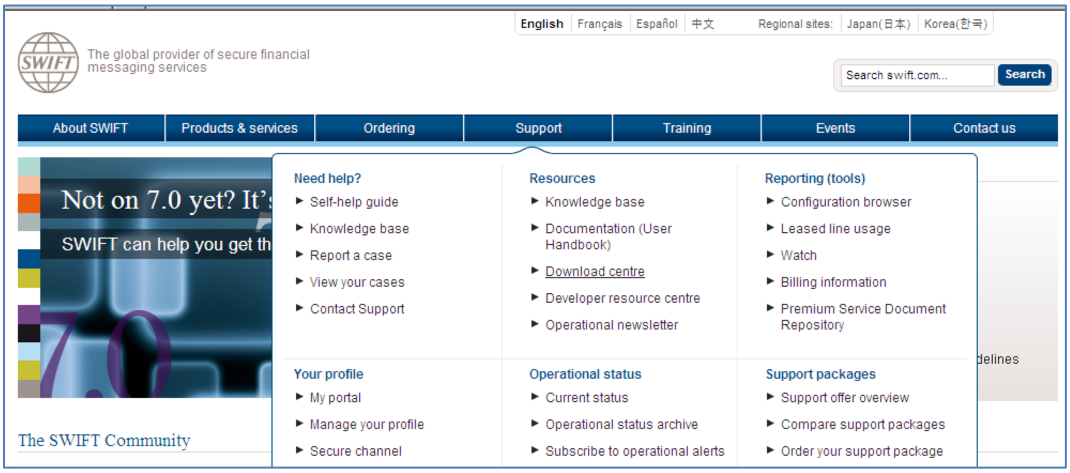
- Service Bureau users:
  - Participants should inform their service bureau that the ASP and FCP files and profiles need to be updated and provide the schedule for the change.
  - The Service bureau will then follow the same procedure as Alliance Access or Alliance Entry users.

- Participants using non SWIFT FIN Interfaces:
  - These participants should contact their interface vendors to obtain instructions on how to perform the update to the FINCopy profile(s) of the SRS service.

2 Installing a Value-Added Service Parameter File for Alliance Access / Entry

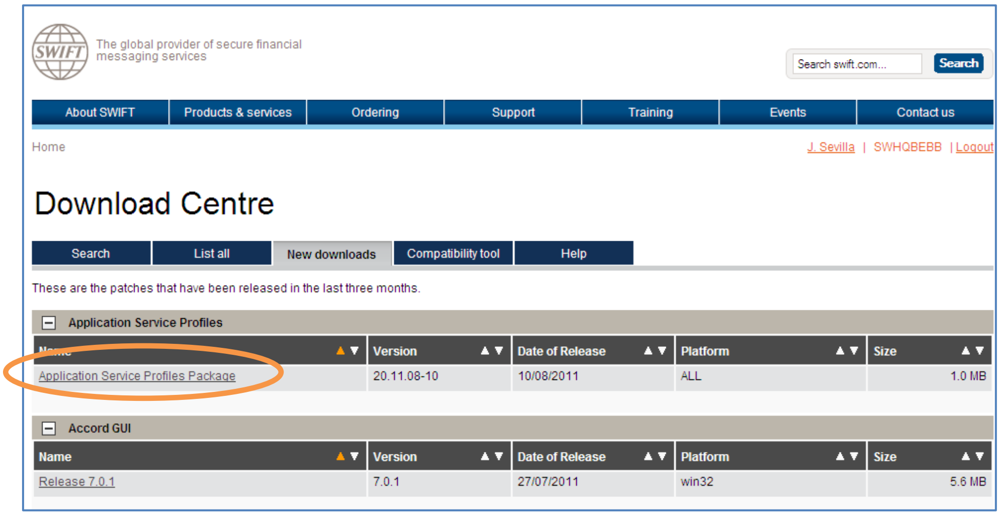
2.1 Retrieve latest ASP file

To download the ASP file you will be requested to logon to swift.com and your profile will need to have access to the Support Application "Download Center". Go to www.swift.com main page": Select from menu bar , support > download centre

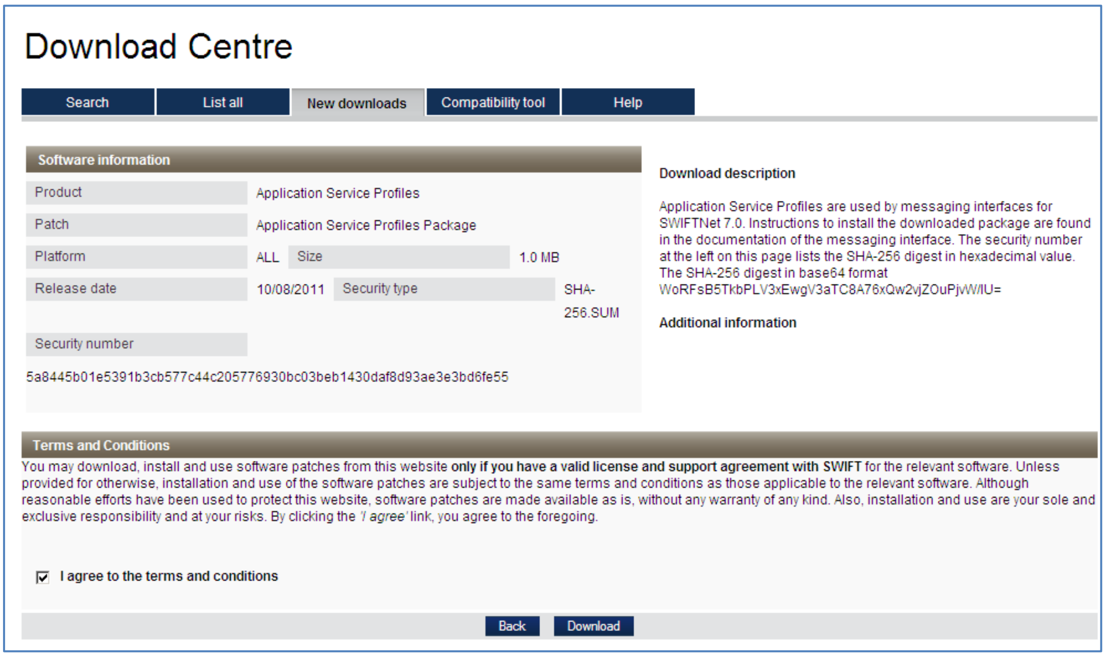


From the download centre page, select **[new downloads]()** tab

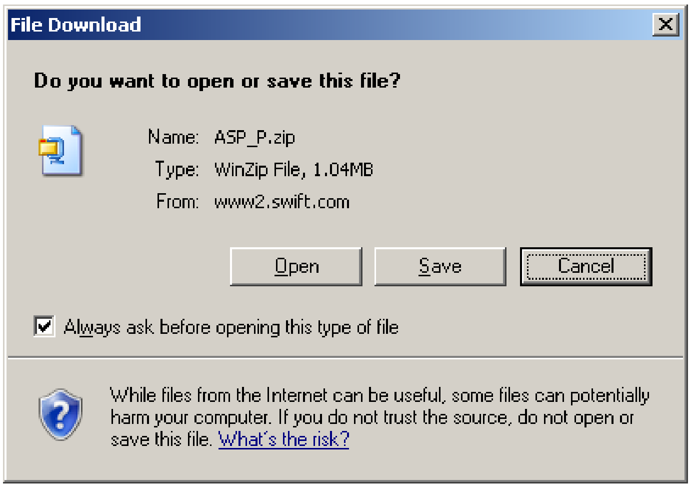
from the list select [Application Service Profiles Package]()



The Application Service Profile (ASP) page in the download centre will pop-up.



Once selected you have to agree on terms and conditions, then you can start the download:



2.2 Managing FCP FINCopy Service Parameter Files

For more information on how to install / configure / activate the FCP files please read the Alliance Access 7.x.x System Management Guide sections 7.2 to 7.5. All documentation can be found at swift.com > support > documentation (here). The actions can be performed using Alliance Workstation or WebPlatform. Below are the instructions using Alliance Workstation.

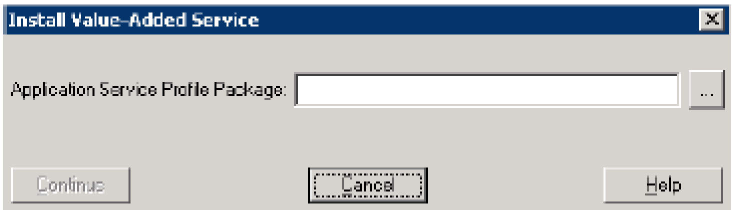
The ASP package must be downloaded from www.swift.com and stored in a dedicated directory for the installation. The ASP package (a .zip archive file) contains four types of files. The FINCopy Profile files **.FCP** contain the FINCopy Profiles.

2.2.1 Installing Value-Added Service Parameter Files

FCP files are installed one by one

1. Start the Alliance Access server in *housekeeping mode*.
2. Run the SWIFT Support application.
3. From the Value-Added Service menu, select Install.

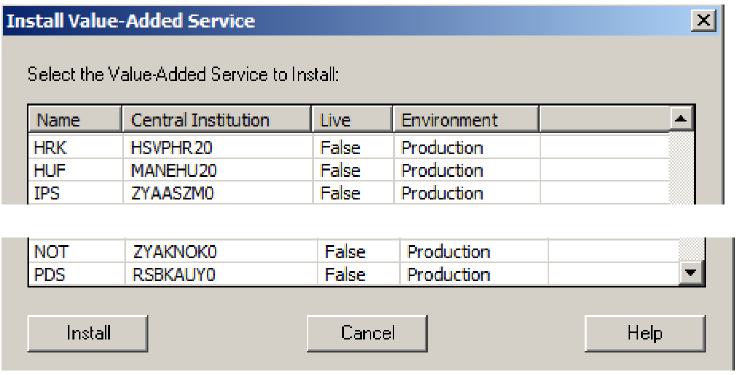
The Install Value-Added Service window appears.



4. In the **Application Service Profile Package** field, enter the location and name of the file (ZIP file) that contains the FIN Copy Profile to be installed (or use the browse button (...) to locate it). If the file is not located on the current drive, then enter the drive name first.

5. Click Continue .

Once the file is located all the .FCP files will displayed.



The following values are displayed for the FIN Copy profiles:

- Name: 3-character code of the FIN Copy profile
- Central Institution: the BIC8 of the Central Institution
- Live: Indicates that the FIN Copy profile is live.
- Environment: the environment to which the FIN Copy profile refers (Production or ITB)

6. Select the Services to Install

Install the 2 SRS services

Name	Central Institution
SRS	SARBZAJS (Live)
SRS	ZYCQZAJ0 (Test)

2.2.2 Assign a Value Added Service to a Destination

To send and receive copy service messages using a particular value-added service, the service must be assigned to a destination on your system.

From the Value-Added Service menu, select Destinations. The Own Destination dialog box appears.

2.2.3 Activate the Value Added Service

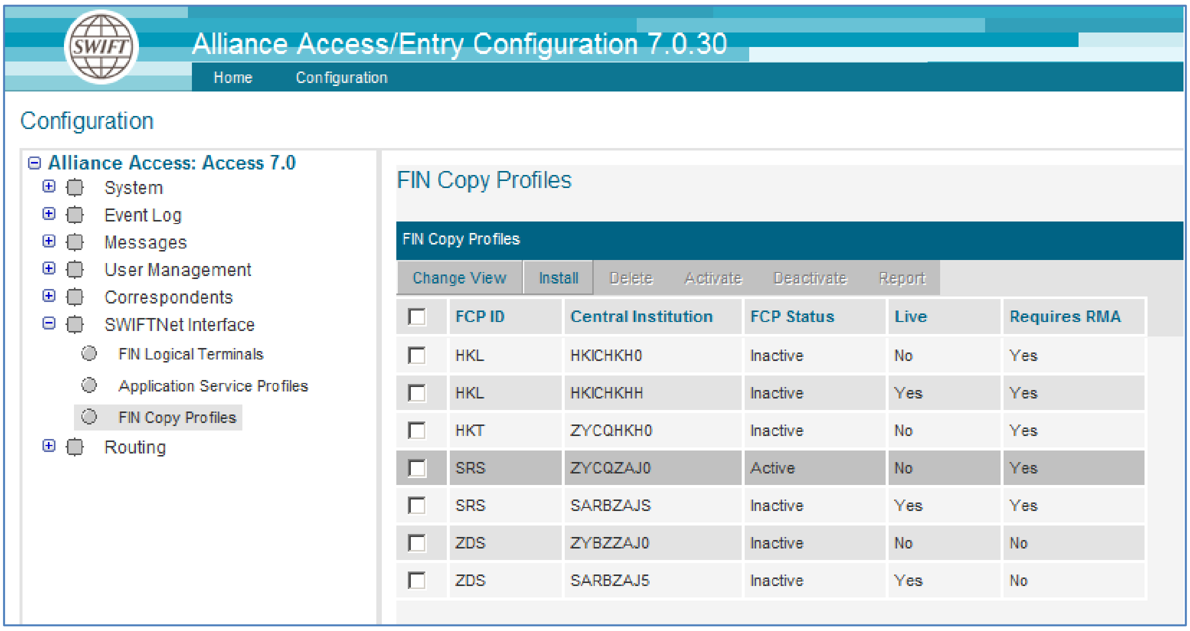
To send and receive copy service messages using a particular value-added service, the service must be Activated.

From the Value-Added Service menu, select Activate. The State field in the Value- a**dded Service** window changes to Active for the selected service.

2.2.4 Verify the installation is correct and completed

Below is the screen shot of the SRS FINCopy Profiles as seen using Alliance WebPlatform. Note the value of the Parameters that you should also see on you server(s) for the SRS services:

- Requires RMA = YES. This is the value you should see for the new service profile.
- FCP Status = Active. Required to be able to use the service.



2.2.5 Start Alliance in Operational Mode

To resume normal operations, once the SRS service have been configured and Activated. Alliance Access Server can be started in Operational mode.

3 RMA Authorisation messages

3.1 Overview of Relationship Management

Relationship Management is a service on SWIFTNet that allows users to control the traffic that they want to accept from other users.

The issuer can control the following types of information:

- which correspondent can send him traffic

It is the BIC that identifies the correspondent (for example, BANKBEBB).

- which traffic the correspondent can send
- when the correspondent can send traffic

The overall objective of Relationship Management is to stop unwanted traffic before it leaves the sender's messaging interface. This has many benefits: by not receiving unwanted traffic, users save time and effort in treating this traffic, and are less exposed to the risks of wrongly processing such unwanted traffic. This helps protect the users against audit and regulatory compliance risks, and helps to avoid fines and damage to reputation.

Please refer to the RMA Service 7.0 – Operations Guide for more information on RMA (link of swft.com/documentation)

3.2 Exchange RMA Authorisation messages

Exchange RMA Authorisation messages with all the SIRESS participants you have a business relationship. Depending on the business relationship you may need to have authorisations to send and/or receive.

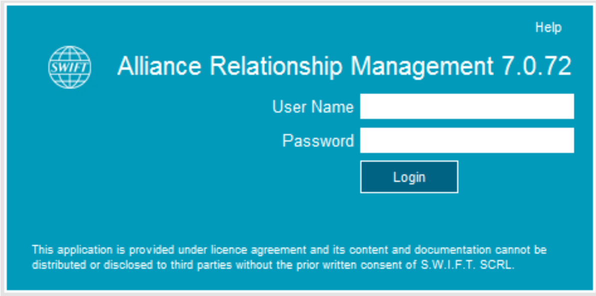
When both parties provide permission to send messages to the other party, the relationship is bilateral. In this case, the GUI of the party that receives the messages displays two authorisations:

- authorisation to receive - authorisation that the party gave to a correspondent
- authorisation to send - authorisation that the correspondent gave to the party

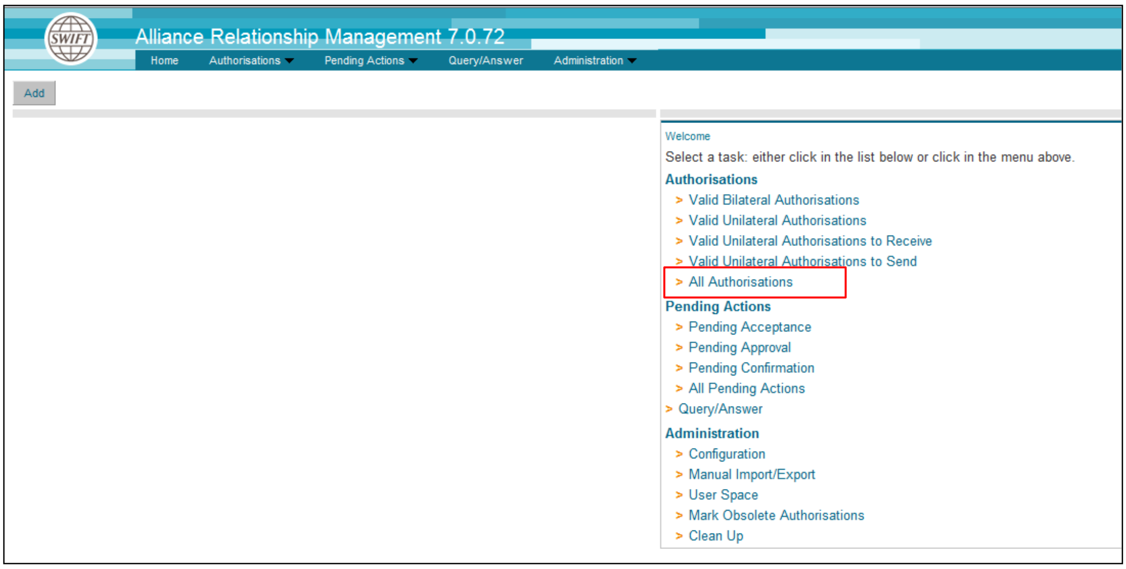
3.3 Steps to issue a RMA Authorisation

- Go to Relationship Management Application

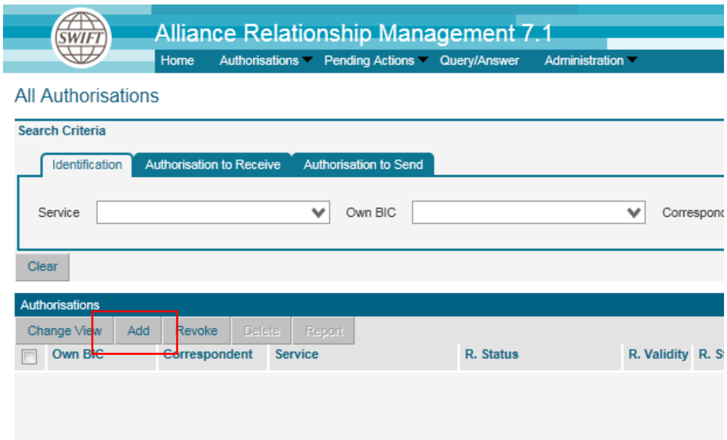
Open the RMA GUI on your respective URL   https://<AWPSERVER> /swp/group/rma/



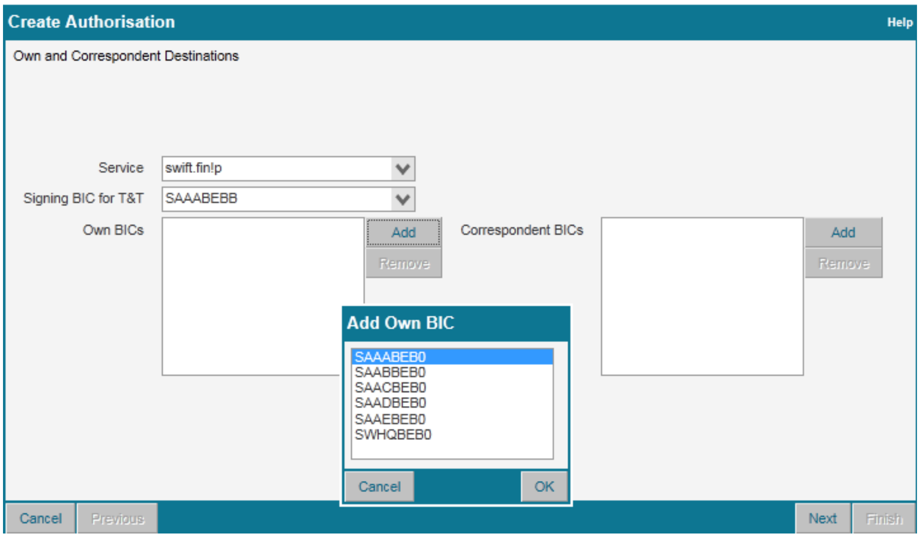
- Select All Authorisations



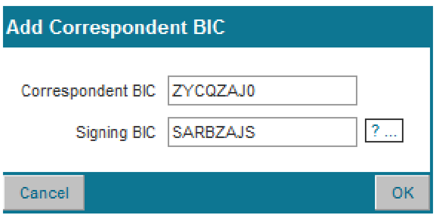
- To define a new authorisation select the option Add



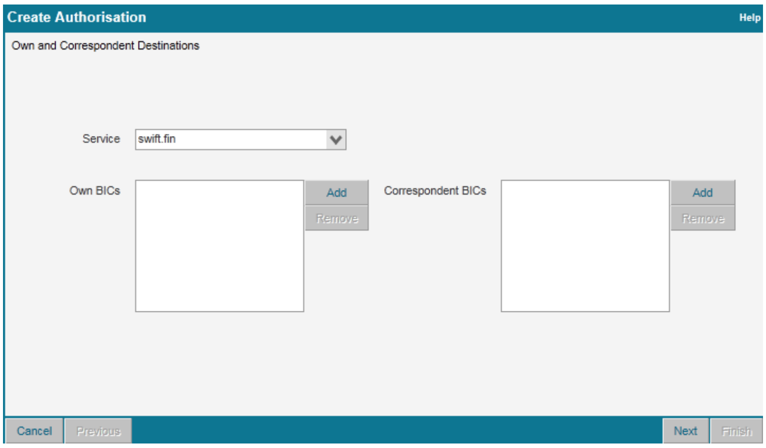
- Options during the creation process for **swift.fin!p** and **swift.fin**:
    - Select in the service field swift.fin!p
    - Ensure you have your own <u>Live BIC in field Signing BIC</u> for T&T
    - Own BICs select your T&T BIC that will be used for the test with the SIRESS service



    - For the correspondent BIC, you have to add the Siress correspondent BIC. Here too Siress Live BIC is required in the signing field.

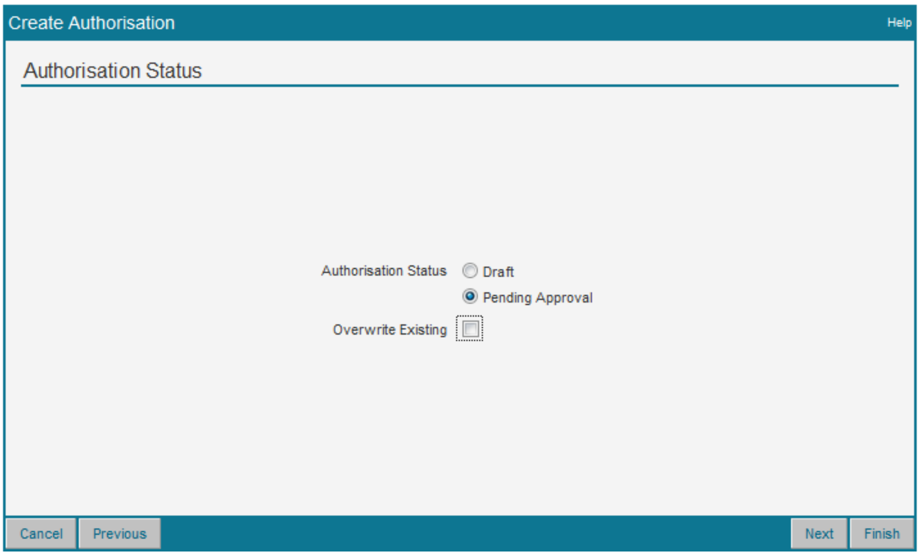


- For the FIN Live service, you select in the service field swift.fin



For the Live service the signing BIC is not requested. Automatically the entered live BIC in the Own field will be used for signing. Same process will be applied for the correspondent BIC.

- Finalisation of the RMA creation
    - Press Next
    - select pending approval
    - Unselect the box overwrite

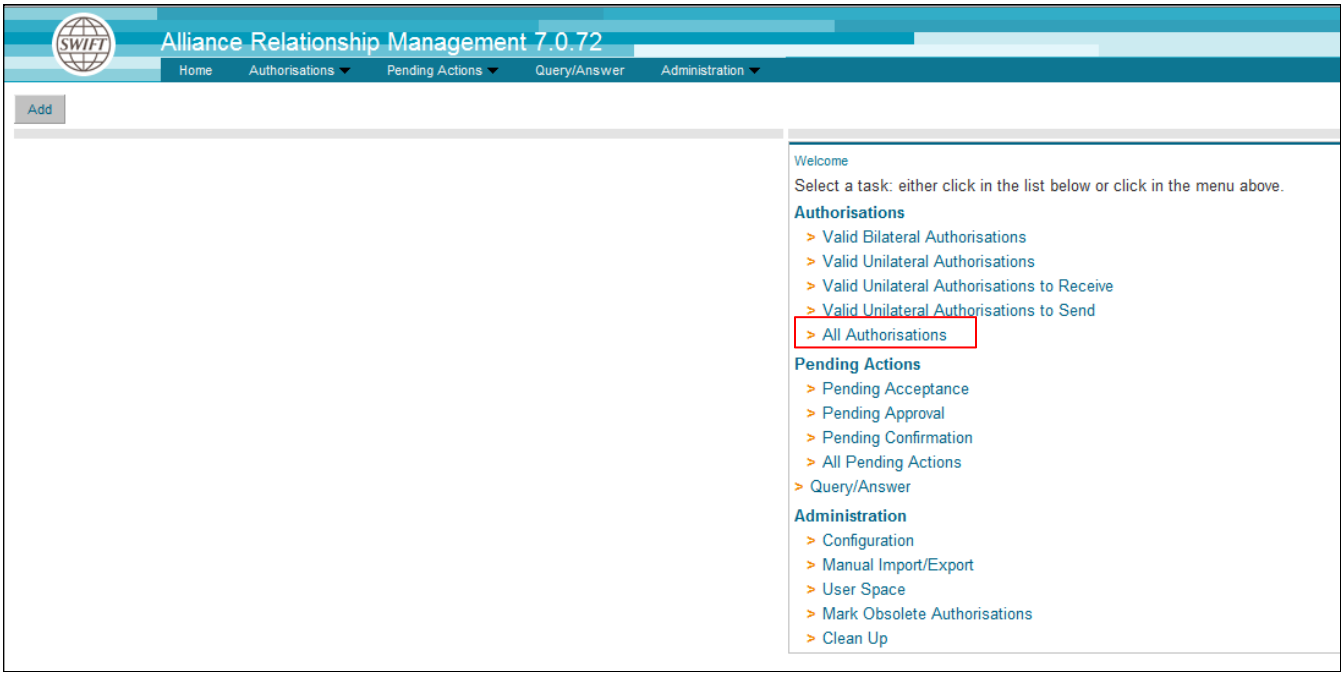


-
    - Press Next

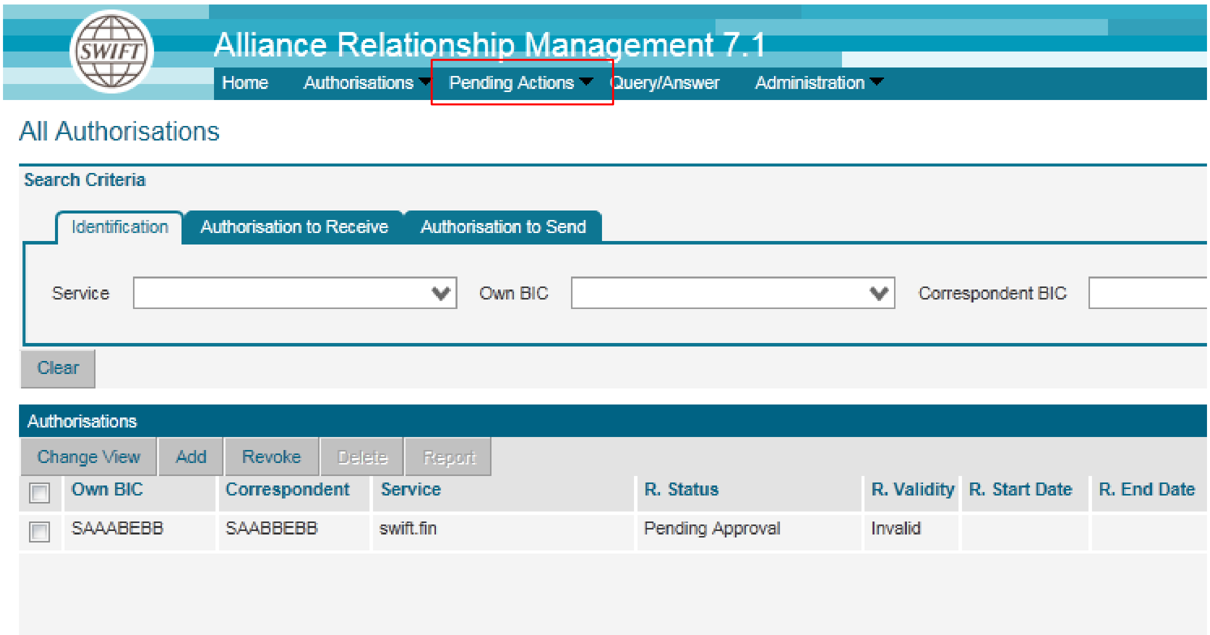
Your RMA request is sent to SIRESS (correspondent BIC = SARBZAJS)

3.4 Steps to approve a received request RMA Authorisation

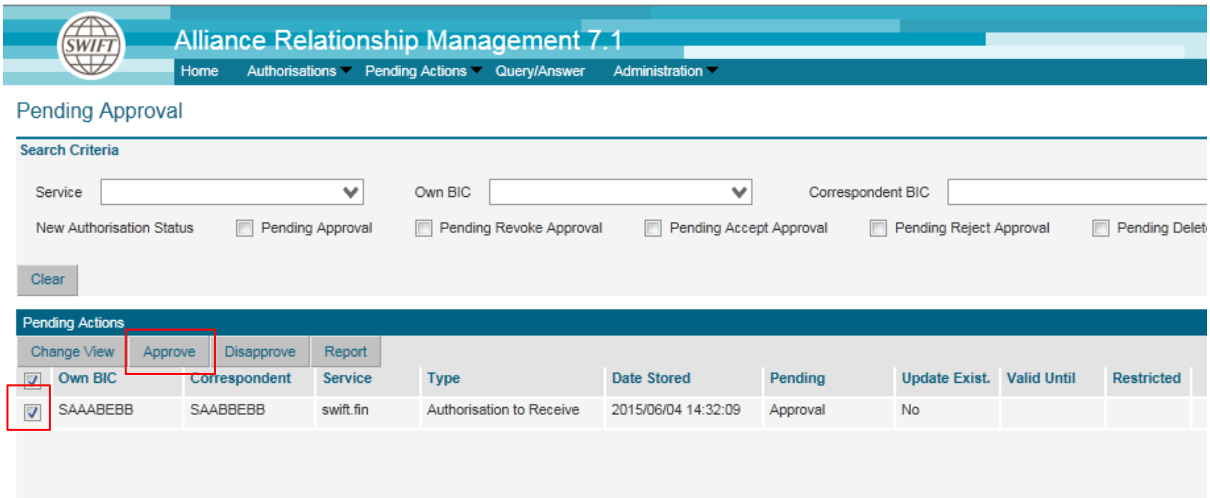
- Go to All authorisation page



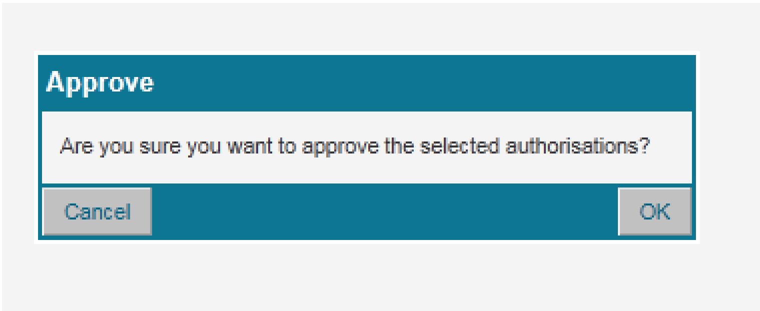
- Select Pending Actions in the menu



- In bottom area, you can see all received requests.



- Tick the Box in the beginning of the line
- Select Approve in the menu
- You received a request to confirm the approval.
- If ok for you press OK



Now both sides should be enabled. You now have an authorisation to receive and send.

Reminder:

You have to exchange RMA with SIRESS as well as with all the banks you wish to conduct business with in SIRESS.

Tip

You can also watch our ***How to create RMA's video*** on SWIFT.com by clicking on the below link:

https://www2.swift.com/search/kb/fetchTip.faces?tip=5019591