Registration & Payments User Guide

Contingency Payment Access
Contents

Contingency Payment Access 4

Introduction 4

1. Self-Registration 4
   1.1. Password 4
   1.2. Client Identification Number and Client Details 6
   1.3. User Profiles – Adding Users 7
   1.4. Payment Account Details 8
   1.5. User/Payment Relationship 9
   1.6. Review and Submit 10

2. Install SWIFT 3SKey Token Client Software 12
   2.1. Token Software Installation Prerequisites 12
   2.2. Download the Installation Software 13

3. Create a SWIFT 3SKey User Group (For Administrators) 16
   3.1. Overview 16
   3.2. Procedure 16
   3.3. Add User to a User Group (For Administrators) 17
   3.4. Token Activation within the SWIFT 3SKey Portal 19
   3.5. Token Renewal 20
   3.6. Token Replacement 20

4. Assigning a User’s 3SKey Token with Contingency Payment Access 21

5. Logging on to Contingency Payment Access 24
   5.1. Homepage 26
   5.2. Navigation 26
      5.2.1. Task 26
      5.2.2. Payments 26
      5.2.3. Activity 27
      5.2.4. Admin 27
   5.3. Admin 27
      5.3.1. New User Setup 27
      5.3.2. Edit a User 28
      5.3.3. Deactivate a User 29
      5.3.4. New Payment Account Setup 29
      5.3.5. Edit an Account 30
      5.3.6. Deactivate an Account 31
5.3.7 User Account Relationship Setup 32
5.3.8 Remove a User Account Relationship 32

6. Payments 33

6.1 Making a Payment 33
6.1.1 Same Day Domestic Payment 33
6.1.2 SEPA Credit Transfer 35
6.1.3 International Payments 36

6.2 Authorising a Payment 38
6.3 Cancelling a Payment 38
6.4 Sending a Payment to Repair 38
6.5 Processing a Payment once Sent to Repair 39
6.6 Copying a Previous Payment 39
6.7 Payment Statuses 39

Activity Log 40

Appendices 41

Contingency Payment Access Amendment Form 41
Contingency Payment Access

Introduction

Contingency Payment Access offers an alternative method to instruct urgent/high value payments should you be unable to access your primary electronic banking application, such as Business Online Banking, Business Internet Banking and Barclays.Net, for any reason. The payment types available through Contingency Payment Access are:

- Same Day Domestic Payments
- SEPA Credit Transfers
- Barclays International Payments.

The system is intended to be used under dual control, each payment instruction created requiring authorisation by a second user. Sole user access and authorisation can be configured but is not recommended.

Please note: regardless of your authorisation requirements, all payments will need to be digitally signed using SWIFT 3SKey Tokens followed by the entry of a one-time passcode that will be sent to the user’s registered mobile number.

Any admin tasks can be submitted by the client administrator but certain tasks, such as adding an additional account, must then be verified by the Barclays Client Support Team.

1. Self-Registration

Contingency Payment Access self-registration URL: https://contingency.barclayscorporate.com

Contingency Payment Access allows you to self-register. In order to complete the registration, the below six steps must be completed:

1.1 New Registration / Password
1.2 Client Details
1.3 User Profile (Users’ Details)
1.4 Payment Bank Account Details
1.5 User / Payment Relationship
1.6 Review, Sign and Submit

1.1 Password

- Navigate to https://contingency.barclayscorporate.com

The login screen will display:
- Select Register

**Please note:** any fields ending with an asterisk (*) are mandatory.

The New Registration screen will display:

![New Registration Screen](image)

- Enter a Password (this will be used for the registration process only, allowing you to save and return in order to complete the registration at a later point if you require; the password will not be required again once the registration is complete). The password must contain between 6-20 characters, one letter, one number and one special character
- Confirm the Password
- Enter the characters shown on screen
- Select Save and Continue
- You will be presented with a Client Identification Number (Client ID):

![Contingency Payment](image)

*Your Client ID is - 100053.*

Please record this number for future reference.

- Select OK

It is very important that you make a note of this Client ID for future reference.
1.2 Client Identification Number and Client Details

The Client Details section will display:

Complete the following details:

- **Business Name**
- **Contact Name** – this is for the key person who will be a point of contact should there be any queries at the registration stage or thereafter.
- **Phone Number** – of the above contact
- **Email Address** – of the above contact
- **Payment Authorise**
  - **Dual (2 Stage Process)** – Payments require authorisation from a second user; this is the default option and it is highly recommended this be used
  - **Sole (1 Stage Process)** – Payments require no authorisation; this is not recommended
- **Address**
- **Select Save and Continue.**
1.3 User Profiles – Adding Users

The User Profile screen will display:

![User Profile Screen]

Complete the following details for each person you wish to have access to the service:

- User Name
- Email Address
- Mobile
- Functions – select one or more of the following:
  - Payment Entry – Will allow a user to enter a payment into the system
  - Payment Authorisation – Will allow a user to authorise a payment which has been entered by another user
  - Administrator – Will allow adding/removing of users, adding accounts and setting the user to account relationships
- Payment Limit (GBP)
- Select Save.

The details of the user will be updated under the Existing Users section:

![Existing Users Screen]

Repeat the steps above to create additional users.

Please note: if you require authorisation for payments, you will be required to add a minimum of two users.

- Select Continue
1.4 Payment Account Details

The Payment Account Details screen will display:

![Payment Account Details Screen](image)

Complete the following details:

- IBAN
- BIC
- Account Currency
- Description
- Select Save.

The details of the account will be updated under the Existing Accounts section:

![Existing Accounts](image)

Repeat the steps above to add further accounts.

- Select Continue
1.5 User / Payment Relationship

The User/Payment Account Relationship screen will display:

![User/Payment Account Relationship Screen]

To allocate which accounts you wish each user to have access to, select from the following:

- Select User: either all or an individual user can be selected
- Select Payment Account: either all or an individual account can be selected.

Please note: If you select All for the User and Payment Account, all users will have access to debit all accounts when making payments.

- Select Save

The details of the user account relationship will be updated under the Existing Relationships section:

![Existing Relationships]

Repeat the steps above to create additional relationships.

- Select Continue
1.6 Review and Submit

The Review and Submit screen will display:

![Review and Submit Screen](image)

Please note: Once the registration has been submitted, the details cannot be amended.

- Review the details entered
- Select Submit and Print.
The details you have completed will be updated on the form.

In the section provided, please confirm whether each user requires a SWIFT 3SKey security token (see next section), Sign and Date the printed copy, and send it directly to your Relationship Team to complete the registration process.

A copy of the PDF document will also be emailed to the main contact details entered during registration.
2. Install SWIFT 3SKey Token Client Software

Contingency Payment Access uses SWIFT 3SKey Tokens for secure user login. 3SKey is designed to be bank agnostic and the tokens are personal to the individual user. A number of banks are already offering it as an optional security token as an alternative to the proprietary tokens developed for use with their specific electronic banking platforms. As such, if any of your users already have 3SKey tokens, they will be able to use these with Contingency Payment Access without the need to order tokens from Barclays.

3SKey Tokens for your users must also be assigned to a user group for your Organisation within the SWIFT Portal. The creation of a user group within the SWIFT Portal requires two tokens – for this reason, even those companies with only one user of Contingency Payment Access will require two 3SKey tokens.

In order to use 3SKey tokens on a particular machine, software drivers must first be installed.

2.1 Token Software Installation Prerequisites

Administrator rights for the particular machine are likely to be required to install the necessary drivers and software.

The PC must be running one of the following operating systems:

- Windows Vista (32-bit) with Service Pack 1 or higher
- Windows 7 (32-bit or 64-bit), optionally with a Service Pack
- Windows 8 (32-bit or 64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.9 (Mavericks).

To access the 3SKey portal, the PC must use one of the following versions of Internet Explorer:

- Internet Explorer 8.0 (32-bit)
- Internet Explorer 9.0 (32-bit)
- Internet Explorer 10.0 (32-bit)
- Internet Explorer 11.0 (32-bit)
- Firefox.

Please note: Windows 8 users must ensure that desktop mode is switched off before launching Internet Explorer.

The PC must have free space of at least 500 MB.

To check this:

- Open Windows Explorer
- Right-click the C: drive
- Select Properties.

A System (C:) Properties window opens:

![System Properties Window](image)

The PC requires a 32-bit version of the Java Runtime Environment (JRE). The minimum supported versions are 1.6.0_32 for Java 6, 1.7.0_7 for Java 7, or Java 8.
2.2 Download the Installation Software

Complete the following steps:

- Navigate to http://www.3skey.com
- Select Install the 3SKey software
- Save the software installation file onto the PC. The file name is 3SKey_token_install.zip
- Run the software installation file
- Navigate to the folder in which the installation software zip file is saved
- Double-click the file. The following window appears:

- Double-click the software installation file contained within the zip file (3SKey_token_install.exe)
- Select Run.

The Welcome to the SWIFT Token Client Installer window opens:

- Select Next

**Important**: although it is possible to customise the options, SWIFT recommends that you accept the proposed installation options.

The pop-up displays the proposed folder location for the software installation files:

- Select Next
The pop-up displays the confirmed settings chosen for installation:

- Select Install

The installer then runs a test to verify that the PC can support the token software installation. This can take a few moments to complete.

The SWIFT Token Client Installer confirmation window opens and will display the configuration results:

- The tests compare the recommended conditions for installation to the actual conditions of the user’s PC. The result in each case appears as one of the following:
  - OK
  - Warning
  - ERROR.

If there is a Warning/ERROR, then an explanation appears in the lower half of the screen. In the case of a Warning, the installation can continue; however, it may cause issues when accessing the SWIFT portal. In the case of an ERROR, the installation cannot complete.

- Select Next
The Installation Complete window will display:

- Select Finish

The Reboot notice window opens and gives the option to Restart Now or Restart Later. Please note, in order to complete the installation, the computer must be rebooted.
3. Create a SWIFT 3SKey User Group (For Administrators)

3.1 Overview

You will require two free USB ports to complete this exercise. If the SWIFT 3SKey portal detects that the token with which you have logged in does not belong to a user group, then it displays an information screen and prompts you to create a user group for your organisation, with two administrators. For this reason, even organisations wishing to configure Barclays Contingency Payment Access for Sole User Access and Authorisation will require two 3SKey tokens in order to create the required User Group and activate the tokens, even if only one will actively be used with Contingency Payment Access.

Important: the creation of the user group is not complete until you have created both Administrators. You therefore require two inactive tokens and two free USB ports.

3.2 Procedure

Return to www.3skey.com – you will be presented with this page:

![3SKey Welcome Page](image1)

Click “Getting Started: Administrators” from the right hand menu and you will be presented with the following page:

![3SKey Getting Started Page](image2)

You will already have completed points 1 and 2. Before going to point 3, we recommend you open another tab and navigate to www.3skey.com again on that new tab; that way you will be able to follow the instructions which will still be open in the original tab and action them in the new tab.
When you click login, enter the default password we sent you with the token and follow the instructions. The system will display the information screen that prompts you to create a user group. Creating the user group then consists of the following steps:

1. On the Warning page, select Continue
2. Insert the second administrator token but do not remove the first token.
3. The second administrator token’s unique ID displays automatically.

The portal updates the Create user group page:

![Create user group page](image)

4. Enter the password for the second token. This is the default password that you received with the tokens.
5. Set an alias for the second administrator token. The default alias is Admin2, but you can change this if required.
6. Set an alias for your own token. The default alias is Admin1, but you can change this if required.
7. Click Create user group.

When the user group created successfully page appears, remove the second Administrator token.

8. Pass the token to the second administrator, who must activate the token.
9. Click Continue to activation to activate your own token.

For more information about activating your token, see “Activate a Token”.

3.3 Add User to a User Group (For Administrators)

Overview

You can use this page to add new users to your user group and specify the role that they should have. Users are identified by the Unique ID on the token that they will use.

For each user that you add, you require both an admin token and a new, inactive token.

Insert a new token in a second USB port and complete the fields on the Add User page.

Important: do not remove the token with which you logged in to the 3SKey portal.
The Add User screen is displayed:

This screen contains the following fields:

**Token** – Select the Unique ID of the new token from the drop-down list. If you do not see the correct Unique ID, then click Refresh to refresh the list.

**Password** – Specify the password that was supplied with the new token.

**Alias** – You can use the Alias field to specify a name with which to identify the Unique ID. The alias is used only within your organisation to manage the tokens on the 3SKey portal. It has no impact on the use of the token to sign.

You can use the following characters for the alias:

- A–Z
- a–z
- 0–9
- _, and space.

You cannot use accented characters (for example, é or ö), or any punctuation characters except those listed.

**Role** – The role assigned to a Unique ID determines the functions that a user can access when logged in to the SWIFT Portal in relation to 3SKey with that Unique ID. By default, Unique IDs are added to the 3SKey user group with the standard user role. You can also create an administrator by selecting admin from the drop-down list.

A token with the user role gives access to the following functions related to 3SKey:

- Use the certificate on the token to sign or authenticate transactions with a bank
- Change the token’s password
- Generate a new security code
- Revoke the certificate that is on the token
- Carry out recovery of the certificate on the token.

This requires a second token that an administrator has prepared for recovery.

- Carry out the reset of a token that has been set up for reset by an administrator
- View the key information that is stored on the token (for example, the Unique ID and the validity period)
- Renew the token before expiry (after three years).
A token with the admin role gives access to the same functions as a token with the user role. These functions are identical for the two types of users. In addition, tokens with the admin role give access to the following functions:

- Set up and maintain a SWIFT 3SKey user group that contains tokens with the admin role and tokens with the user role
- View the tokens in the user group and the status of the tokens
- Revoke tokens of users in the group
- Set up a token for the recovery of a Unique ID (either user role or admin role)
- Set up for reset a token that is locked or whose password is lost
- Finalise adding the token.

When all fields are correctly specified, select Add.

The 3SKey portal confirms that the token has been added to the user group:

![Add user screen](image)

Remove the token that you have added from the USB port.

- If there are further tokens to add to the user group, then select Add Another
- If you have finished adding all tokens to the user group, then select Done.

Before each user can log in to Contingency Payment Access for the first time they will need to associate their 3SKey Token with it.

3.4 Token Activation within the SWIFT 3SKey Portal

Each User's token must be activated within the SWIFT 3SKey Portal before it can be used with Barclays Contingency Payment Access.

- Insert the 3SKey token into a USB port; do not remove the token from the USB port during this procedure
- Go to [http://www.3skey.com](http://www.3skey.com)
- Select Login
- A prompt to enter the default password provided by your administrator will display
- The Unique ID appears (for example, corp12345678)
- Select Next.

The token activation screen will display:

![Token activation screen](image)

- Follow the steps on screen to change the password
- **Important:** please note, if the password is lost or if it is entered incorrectly five consecutive times, then the token becomes locked and a new token will have to be issued
• Select Next
• The system will run through an automatic process
• Select Download to save the security code – which will be in the form of a TXT file*

*Important: please note, the security code is generated automatically during token activation; this must be stored safely. If the password or token is lost, then a new token is needed and the secure code can be used to transfer the Unique ID to that new token so that the user is not recreated from scratch.

When activation of the token is complete, the following screen appears:

![Activation complete screen]

The token is now activated within SWIFT. The active token must now be assigned to a User Profile within Contingency Payment Access.

Please note: for further assistance or troubleshooting regarding the SWIFT token, please refer to http://www.swift.com/3skey/index.html

3.5 Token Renewal

The certificate of a 3SKey token expires three years after activation. It is your responsibility to renew the certificate using the SWIFT portal. After renewal, when you next log on to Contingency Payments Channel, it will recognise that the certificate has changed on the token. You will then be prompted to confirm the renewal and a one-time password will be sent as a text message to your registered mobile. When prompted, the one-time password must be entered. If the value entered matches the value generated, and is entered within five minutes from the time of generation, the renewed token will be registered to that user.

3.6 Token Replacement

If the 3SKey token is lost or damaged, you will be provided with a replacement by your administrator. You must then activate the token using the SWIFT portal. After activation, when you next log on to the Contingency Payments Channel, you will be challenged to enter your email address and client ID, as the token will not be recognised. The user will then be prompted to confirm the replacement and a one-time password will be sent as a text message to your registered mobile. When prompted, the one-time password must be entered by the user. If the value entered matches the value generated, and is entered within five minutes from the time of generation, the replacement token will be registered to that user.
4. Assigning a User’s 3SKey Token with Contingency Payment Access

- Navigate to https://contingency.barclayscorporate.com (note the Channel is not supported on Google Chrome or Windows Edge browser)

The Login screen will display:

- Insert your token
- Select Login

The Authenticate screen will display:

- Select Authenticate
A warning screen will display:

- Tick “I accept the risk and want to run this application”
- Select Run
- You might then see the following – if you do, click “Don’t Block”.

The password box will display:

- Enter the password you have set for your token
- Select OK.
The Token Association screen will display:

![Token Association Screen](image)

Complete the following details:

- Email
- Client ID
- Select *Send OTP (One time Passcode)*
- [There is no need to click “View Certificate Details” but you may do so if you want to see all other fields under 3SKey Details populated.]

A confirmation popup will display:

![Confirmation Popup](image)

- Select OK

The password box will display:

![Password Box](image)

- Enter the password you have set for your token
- Select OK.

A One Time Passcode will be sent to the user's registered mobile phone number.

- Enter the One Time Passcode received

**Please note:** this must be entered within five minutes. If you have not managed to enter it within the allocated time, there is an option to “Resend One Time Password”.

Once this is completed, the Token is successfully registered and you can proceed to log in (you will not need to complete this step again).
5. Logging on to Contingency Payment Access

Navigate to https://contingency.barclayscorporate.com

- Insert the token
- Select Login.

The Authenticate screen will display:

- Select Authenticate
A warning screen will display:

- Tick "I accept the risk and want to run this application"
- Select Run
- You might then see the following – if you do, click "Don’t Block”.

The password screen will display:

- Enter your password
- Select OK.

The homepage will display.
5.1 Homepage

Once a User is logged in to Contingency Payment Access, they will be presented with the homepage. How the Homepage appears will vary depending on the user’s entitlements.

The following options are available:

5.1.1. Tasks – There are two tabs within this widget; authorise and repair. This will detail the total number of items pending approval/awaiting repair

5.1.2. Quick Links – This will allow you to navigate straight to the desired screen using the hyperlinks

5.1.3. Processed Transactions – This will detail the last five payments processed through the system. There is an option to View All that will expand the view and allow all payments to be viewed

5.2 Navigation

The Contingency Payment Access Channel contains multiple tabs across the top of the screen. The tabs displayed will vary depending on your user entitlements and are used to navigate around the system.

5.2.1 Task

The Task tab contains the following worklists:

- To Authorise – This will list all payments submitted by another user and awaiting approval
- To Repair – This will list all payments sent to repair and awaiting resubmission
- To Complete – This will list all incomplete payments
- To Approve – This worklist will be available to the Admin on a dual authorisation client and will list all users pending approval after an amendment.

5.2.2 Payments

The following payment types are available via Contingency Payment Access:

- Same Day Domestic Payment
- SEPA Credit Transfer
- International Payment.
5.2.3 Activity

The Activity tab contains the following lists:

- **Payment Activity** – Will list all payment activity
- **Audit Log** – Will list an audit of all activity.

5.2.4 Admin

The Admin tab contains the following:

- **Client Details** – Will detail the client name and address
- **Users** – Will list all users and their user status. The admin can add, amend and deactivate users from this screen
- **Accounts** – Will list all accounts and their status. The admin can add, amend and deactivate accounts from this screen
  - **User Account Relationship** – Will list all User to account relationships, the admin can add, amend and remove relationships from this screen.

5.3 Admin

If you have admin rights you will be able to create, modify and remove the following:

- **Users**
- **Accounts**
- **User Account relationships**.

5.3.1 New User Setup

- **Navigate to Admin > Users**

Complete the following details:

- **User Name**
- **Email Address**
- **Mobile**
- **Functions** – select one or more of the following:
  - **Payment Entry** – will only allow a user to enter a payment into the system
  - **Payment Authorisation** – will allow a user to authorise a payment which has been entered by another user
  - **Administrator** – will allow adding/removing of users, adding accounts and setting the user to account relationship
  - **Payment Limit (GBP)**
- **Select Save.**
The details of the user will be updated under the Existing Users section:

- Select Request Approval

The Bank will provide final approval. Please complete the amendment form at the end of this Guide and send it to your Relationship Director.

A new token will be sent and the user will be required to follow the steps in sections 1 – 6 of the guide.

Repeat the steps above to create additional users.

5.3.2 Edit a User

- Navigate to Admin > Users
- From the list, locate the user you wish to edit
- Select Edit.

Details will show under User Profile:

- Amend the details as required
- Select Save.
If you are a dual authorisation client:

- A message will display stating: “The amendment(s) has been submitted”
- A second administrator will need to log on
- Navigate to Task > To Approve
- Select the User and click Authorise.

5.3.3 Deactivate a User

- Navigate to Admin > Users
- From the list, locate the User you wish to deactivate
- Select Deactivate
- A message will display stating: “The user has been deactivated”.

If you are a dual authorisation client, this action will not require authorisation.

5.3.4 New Payment Account Setup

Navigate to Admin > Accounts

Complete the following details:

- IBAN
- BIC
- Account Currency
- Description
- Select Save.

The details of the account will be updated under the Existing Accounts section:

- Select Request Approval
The Bank will provide final approval. Please complete the amendment form at the end of this Guide and send it to your Relationship Director.

Repeat the steps above to add further accounts.

**Please note:** once new accounts have been approved by the bank, the User Account Relationship must be set up in order for users to have visibility of these accounts.

### 5.3.5 Edit an Account

- Navigate to Admin > Accounts
- From the list, locate the Account you wish to deactivate
- Select Edit.

Details will show under Payment Account Details:

- Amend the details as required
- Select Save
- A message will display stating: "The account has been updated successfully".

If you are a dual authorisation client:

- Select Save
- A message will display stating: "The Payment(s) has been submitted"
- A second administrator will need to log on
- Navigate to Task > To Approve
- Select the User and click Authorise.
5.3.6 Deactivate an Account

- Navigate to Admin > Account

The accounts will be listed under Existing Accounts:

- From the list, locate the Account you wish to deactivate
- Select Deactivate
- A message will show stating: “The account has been updated successfully”.

If you are a dual authorisation client, this action will not require authorisation.
5.3.7 User Account Relationship Setup

- Navigate to Admin > User Account Relationship

Relationships will be displayed under Existing Relationships:

![Image of Barclays account relationship setup](image)

To select which accounts you wish each user to have access to, choose from the following:

- Select User: either all or an individual user can be selected
- Select Payment Account: either all or an individual account can be selected.

**Please note:** if you select “All” for the User and Payment Account, all users will have access to debit all accounts when making payments.

5.3.8 Remove a User Account Relationship

- Navigate to Admin > User Account Relationship
- From the list, locate the Relationship you wish to remove
- Select Remove.

**Please note:** by clicking “Remove All” all existing relationships will be removed.

If you are a dual authorisation client, this action will not require authorisation.
6. Payments

6.1 Making a Payment

- Navigate to Payments

There are three types of payment available:

- Same Day Domestic Payment
- SEPA Credit Transfer
- International Payment.

![Barclays Payment Screen](image)

6.1.1 Same Day Domestic Payment

- Select your debit account from the dropdown next to Same Day Domestic Payment
- Select Next.

The following tickbox will display:

![Payment on Behalf of Screen](image)

If you are making the payment on behalf of another entity/third party, please tick Yes and complete the following details:

- Third Party Name
- Third Party Post Code
- Third Party Town
- Third Party Country.

Otherwise, leave the tickbox blank.

If submitting Third Party and Fourth Party Payments as a Payment Service Provider (PSP), this channel is not appropriate. Whether you are classified as a Payment Service Provider will be determined in accordance with the Payment Services Regulations 2017. The definition includes Financial Institutions and other payment institutions. If you have any questions, please contact your Relationship Team.
The Same Day Domestic Payment screen will display as below:

Complete the following details:

- Payment Date
- Payment Currency
- Payment Reference
- Payment Amount
- Beneficiary Details
- IBAN/Sort code and Account Number
- Account Name
- Payment Details.

If you have sole user access (not recommended):

- Select Submit to SWIFT
- Enter your password
- Select OK
- A one-time security code (OTSC) will be sent to your registered mobile number. Enter the code into the Enter Security Code field
- Select Verify
- A message will display stating: “The Payment(s) has been submitted”.

If you are a dual authorisation client:

- Select Submit for authorisation
- A message will display stating: “The Payment(s) has been submitted”.

Refer to the “Authorising a Payment” Section for details on what steps the payment Authoriser should take.

Please note: selecting Save will place the payment in the To Complete worklist under Tasks, allowing a User to complete the payment at a later stage.
6.1.2 SEPA Credit Transfer

- Select your debit account from the dropdown next to SEPA Credit Transfer
- Select Next.

The following tickbox will display:

![Image of tickbox]

If you are making the payment on behalf of another entity/third party, please tick Yes and complete the following details:

- Third Party Name
- Third Party Post Code
- Third Party Town
- Third Party Country.

Otherwise, leave the tickbox blank.

If submitting Third Party and Fourth Party Payments as a Payment Service Provider (PSP), this channel is not appropriate. Whether you are classified as a Payment Service Provider will be determined in accordance with the Payment Services Regulations 2017. The definition includes Financial Institutions and other payment institutions. If you have any questions, please contact your Relationship Team.

The SEPA Credit Transfer screen will display as below:

![Image of SEPA Credit Transfer screen]
Complete the following details:

- Payment Date
- Payment Currency
- Payment Reference
- Payment Amount
- Beneficiary Details
- BIC & IBAN
- Account Name
- Payment Details.

If you are a sole authorisation client:

- Select Submit to SWIFT
- Enter your password
- Select OK
- A one-time security code (OTSC) will be sent to your registered mobile number. Enter the code into the Enter Security Code field
- Select Verify
- A message will display stating: “The Payment(s) has been submitted”.

If you are a dual authorisation client:

- Select Submit for authorisation
- A message will display stating: “The Payment(s) has been submitted”.

Refer to the “Authorising a Payment” Section for details on what steps the payment Authoriser should take.

Please note: selecting Save will place the payment in the To Complete worklist under Tasks, allowing a User to complete the payment at a later stage.

6.1.3 International Payments

Please refer to our International Payments Guide for general guidance:
www.barclayscorporate.com/information/international-payments/barclays-net.html

- Select your debit account from the dropdown next to International Payments
- Select Next.

The following tickbox will display:

![Tickbox Image]

If you are making the payment on behalf of another entity/third party, please tick Yes and complete the following details:

- Third Party Name
- Third Party Post Code
- Third Party Town
- Third Party Country.

Otherwise, leave the tickbox blank.

If submitting Third Party and Fourth Party+ Payments as a Payment Service Provider (PSP), this channel is not appropriate. Whether you are classified as a Payment Service Provider will be determined in accordance with the Payment Services Regulations 2017. The definition includes Financial Institutions and other payment institutions. If you have any questions, please contact your Relationship Team.
The International Payments screen will display as below:

Complete the following details:

- Payment Date
- Payment Currency
- Payment Reference
- Payment Amount
- Beneficiary Details
- BIC / NCSC Code
- IBAN / Account Number
- Account Name
- Payment Details.

If you are a sole authorisation client:

- Select Submit to SWIFT
- Enter your password select OK
- A one-time security code (OTSC) will be sent to your registered mobile number. Enter the code into the Enter Security Code field
- Select Verify
- A message will display stating: “The Payment(s) has been submitted”.
If you are a dual authorisation client:

- Select Submit for authorisation
- A message will display stating: “The Payment(s) has been submitted”.

Refer to the “Authorising a Payment” Section for details on what steps the payment Authoriser should take.

**Please note:** selecting Save will place the payment in the To Complete worklist under Tasks, allowing a User to complete the payment at a later stage.

### 6.2 Authorising a Payment

- Navigate to Task > To Authorise
- The To Authorise screen will display:

![Barclays Contingency Payment Screen](image)

- Select the payment you wish to authorise and click Authorise
- A confirmation pop-up will appear, select OK
- A one-time security code (OTSC) will be sent to your registered mobile number. Enter the code into the Enter Security Code field and select Verify
- A message will display stating: “The Payment(s) has been authorised”.

### 6.3 Cancelling a Payment

- Navigate to Task > To Authorise
- Select the payment you wish to cancel and select Cancel
- A confirmation pop-up will appear, select OK
- A message will display stating: “The Payment(s) has been cancelled”.

### 6.4 Sending a Payment to Repair

- Navigate to Task > To Authorise
- Select the payment you wish to send to repair and select Send To Repair
- A confirmation pop-up will appear, select OK
- A message will display stating: “Request for Repair has been sent”.
6.5 Processing a Payment once Sent to Repair

- Navigate to Task > To Repair
- Select the payment you wish to repair and select Edit
- The Payment Details screen will display and allow you to make the relevant changes
- Select Submit for authorisation.

Please note: selecting Save will place the payment in the To Complete worklist under Tasks, allowing a User to complete the payment at a later stage.

For dual clients, a message will appear stating: “Payment has been submitted for authorisation”. If you are a sole client, the payment will be submitted with no requirement for authorisation.

6.6 Copying a Previous Payment

Any payment previously made can be used as a template for another payment; this saves the need to re-key the beneficiary details etc. A copy can be made of any previously completed payment from each of the three payment types: Same Day Domestic Payment, SEPA Credit Transfer, International Payment. The amount and date fields are blanked out when the previous payment is copied but all other details copy across to a new instruction.

- Navigate to Activity
- Locate the payment you wish to copy
- Click on “Create Copy”
- Enter Payment Date, Amount and Reference
- Amend any other details as necessary
- Submit the payment as described previously in this section.

6.7 Payment Statuses

- Pending Authorisation – This status is displayed when the payment is waiting for authorisation
- Pending Repair – This status is displayed when a payment request is sent for repair by an authoriser
- Pending Completion – This status is displayed when a payment is saved without being submitted and requires completion by the user
- Authorisation Cancelled – This status is displayed when a payment request is cancelled by any authoriser
- Queued for Submission – This status is displayed after authorisation but before the transaction has been accepted by the bank
- Transaction Submitted – This status is displayed after the payment instruction has been submitted to the bank for processing
- Transaction Processed – Only displayed after receiving a positive acknowledgment that the instruction has reached the bank
- Transaction Failed – Only displayed after receiving notification that the payment instruction failed to reach the bank.
Activity Log

- Navigate to Activity

The Payment Activity screen will display:

```
<table>
<thead>
<tr>
<th>International (Ref: CC150605163741690)</th>
<th>View</th>
<th>Create Copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Date</td>
<td>05/06/2015</td>
<td></td>
</tr>
</tbody>
</table>

Transaction Rejected
10.00 GBP

<table>
<thead>
<tr>
<th>International (Ref: CC1506021502422220)</th>
<th>View</th>
<th>Create Copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Date</td>
<td>22/06/2015</td>
<td></td>
</tr>
</tbody>
</table>

Transaction Failed
10.00 EUR
```

This screen will display all payment activity. Next to the payment reference there are two hyperlinks:

- **View** – Allows you to view the payment details
- **Create Copy** – Allows you to make a copy of the payment.

There is a second page on the Activity tab, Audit Log; if you click on this, the Audit Log screen will display:

```
<table>
<thead>
<tr>
<th>USER NAME</th>
<th>TYPE</th>
<th>ENTITY</th>
<th>FIELD NAME</th>
<th>OLD VALUE</th>
<th>NEW VALUE</th>
<th>DATE &amp; TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mike Foggon</td>
<td>Client User</td>
<td>Michelle Postlethwaite</td>
<td>Authorisation Status</td>
<td>Modified On</td>
<td></td>
<td>03/07/2015 11:58:16:963</td>
</tr>
<tr>
<td>Mike Foggon</td>
<td>Client User</td>
<td>Michelle Postlethwaite</td>
<td>Description</td>
<td>Modified On</td>
<td></td>
<td>26/03/2015 12:58:17:747</td>
</tr>
<tr>
<td>Mike Foggon</td>
<td>Payment Account</td>
<td>IF078BARC09602735</td>
<td>Open For Edit</td>
<td>Modified On</td>
<td></td>
<td>23/03/2015 12:01:23:617</td>
</tr>
</tbody>
</table>
```

This screen will display an audit of all activity.
Appendices

Contingency Payment Access Amendment Form

This form should be used to confirm the following amendments which you must first initiate via the administration function within the Contingency Payment Access system:

1. Additional User Details

<table>
<thead>
<tr>
<th>User Name</th>
<th>User’s Email</th>
<th>User’s Mobile Phone Number</th>
<th>Payment Limit</th>
<th>Functions¹ (Admin, Payment Entry, Payment Authorisation)</th>
<th>3SKey Required?*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ State whether the user is being granted Admin rights, payment entry, payment authorisation or any combination of these three. New users will need to be approved by Barclays before they become active – in addition, you will need to complete this form for all new users in order to advise Barclays to send 3SKey tokens (if required)*

*3SKey is the security token each user will need to access the service. Enter Yes unless a user already has a 3SKey token for another application.

2. Additional Payment Account Details

<table>
<thead>
<tr>
<th>IBAN (Please provide the account number in International Bank Account Number format)</th>
<th>Account Description (e.g. No 1 Account)</th>
<th>Currency (e.g. GBP)</th>
<th>SWIFT BIC (required for non-Barclays accounts or accounts overseas)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Execution

For and on behalf of:

<table>
<thead>
<tr>
<th>Authorised Signature*</th>
<th>Authorised Signature*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
</tr>
<tr>
<td>Position</td>
<td>Position</td>
</tr>
<tr>
<td>Date</td>
<td>Date</td>
</tr>
</tbody>
</table>

*Where you are a company incorporated in the UK, this application should be signed by two directors. For a company with a sole director, the application should be signed by a director and company secretary or a director and witness. If you are one of the following UK entities, this application should be signed as follows:

- Sole Trader — to be signed by the Proprietor
- Club/Association/Society — two members to sign
- Ordinary/Personal Trust/Lloyds Syndicate — all trustees to sign
- Partnership (four partners or fewer) — all partners to sign
- Partnership (five or more partners) — two authorised partners to sign.

If your business is incorporated in a country other than the UK, please refer to the document "Barclays.Net Channels Country Conditions", which is available from the Help function, for guidance on how to sign.

Bank Use Only

Barclays Branch Contact Details

| Relationship Manager/ |
| Director              |
| Email                 |

Contact Number

| Authorised Signature | Branch Stamp |

Note to Relationship Team: ensure correct tariff is applied for the three payment types against any new accounts registered. See Products and Services Intranet for Guidance.

---

You can get this in Braille, large print or audio by calling 0800 400 100* (via Text Relay or Next Generation Text Relay if appropriate). Barclays also welcomes calls via SignVideo for BSL users. Visit barclays.co.uk/signvideo

*Calls to 0800 numbers are free from UK land lines and personal mobiles, otherwise call charges may apply. Please check with your service provider. To maintain a quality service we may monitor or record phone calls. Lines are open 7 days a week, 7am to 11pm.

This document is used by Barclays Bank PLC and Barclays Bank UK PLC. Details of your service provider are set out in your customer agreement.

Item ref: 3915274. April 2018.