Corporate User's Internet Banking Site Administrator's Guide (RBSR)

Republic Online

Republic Bank

TABLE OF CONTENTS

How do I register?

Registration Requirements

The first step in registering your business for Internet Banking, is to ensure you have the following requirements:

1. **Site Administrator:**

   Your Company will be required to assign a Site Administrator, who will be responsible for the Company's internet banking profile, as well as adding company users, and assigning permissions to these users.

2. **New Customer ID**

   New Customers: Your Customer ID will be given to you at the onboarding stage

   Existing Customers: Your Customer ID would have been communicated to you via letter/email. If you have not received this information please contact your Engagement Lead/Relationship Manager.

3. **Mobile Device**

   RepublicOnline requires that all users register a mobile device which will be used as the second-factor authentication device when logging in.

Existing Customer’s Registration Process

Existing Customers!

Here’s what you need to do…

STEP 1

<u>Company Official/Director/Site Administrator must:</u>

1. Identify your Company’s Internet Banking Site Admininstrator.
2. Attend virtual demo/training session with the Bank officials.
3. Complete the Registration form provided with users’ details.
4. Obtain authorization from Company’s Authorised Signatories *(as noted on the company mandate held at the bank)* and include company stamp on document.
5. Return completed registration form to the Bank.

Once the users have been created an email notification will be sent to the email addresses registered on the form, confirming that their Company’s IB profiles have been created.

STEP 2

Site Administrators:

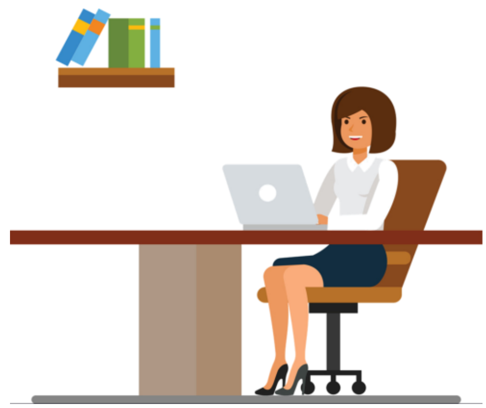
6. Retrieve email sent from the Bank with the temporary password assigned.

7. Log on to Online Banking from the website using the username selected at registration and the Temporary password sent via email from the Bank.

8. Complete the first loging process and setup of security devices **(refer to First login process on pg 25)**

9. Proceed to create/setup other company users as required.

New Customer's Registration Process



<u>Company Official/Director/Site Administrator</u>

10. Log on to Online Banking from the website

11. Go to the bottom of the screen in the *Register for RepublicOnline* section and select the ***Corporate*** link (as shown below)

STEP 1

- Complete the 5-step process, **(see page 10)**, to register your company/business.
- Print completed form and obtain authorization from Company's Authorised Signatories *(as noted on the company mandate held at the bank)* and include company stamp on document.
- Scan completed form and forward to **rbsribsupport@republicbanksr.com**

Once the user has been created an email notification will be sent to the email addresses registered on the form, confirming that the Company's IB profiles has been created

STEP 2

Site Administrator

12. Retrieve email sent from the Bank with the temporary password assigned

13. Log on to Online Banking from the website using the username selected at registration and the Temporary password sent via email from the Bank.

14. Complete the first login process and setup of security devices **(refer to First login process on pg 25)**

15. Proceed to create/setup other company users Proceed to the site and create/setup other company users as required.

The Online Registration Process

includes the following five (5) steps:

Step 1:
Accept Terms and Conditions

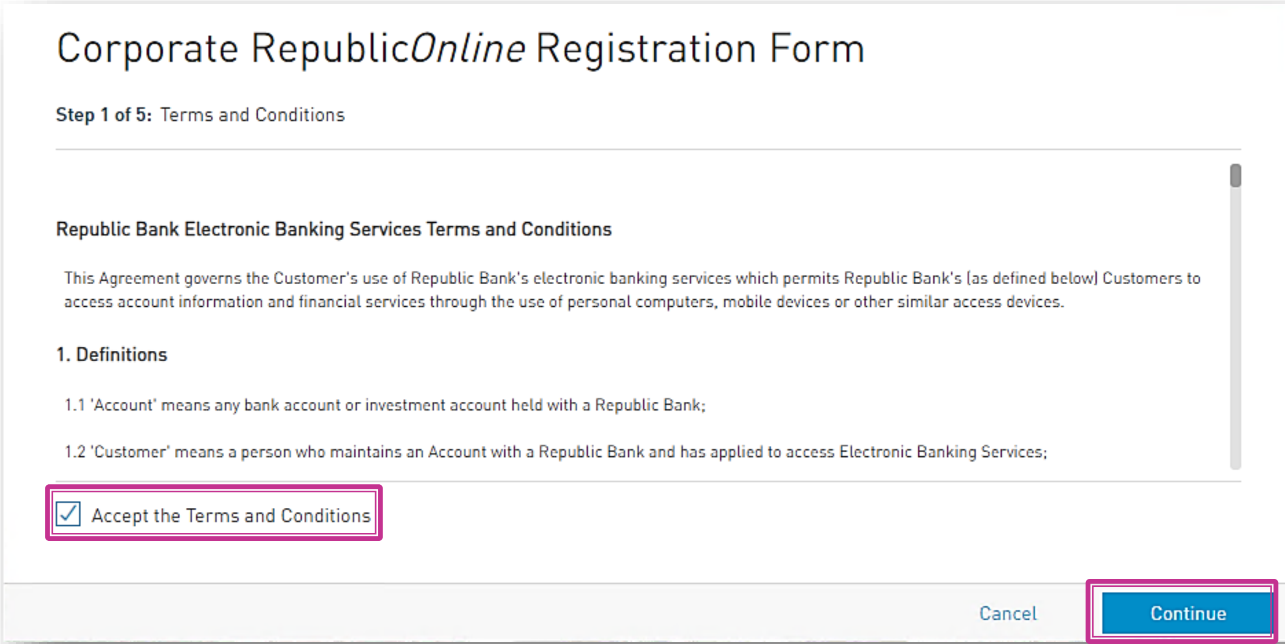
Step 2:
Input Business' and Company's Information

Step 3:
Input Administrator's Info

Step 4:
Confirm Data

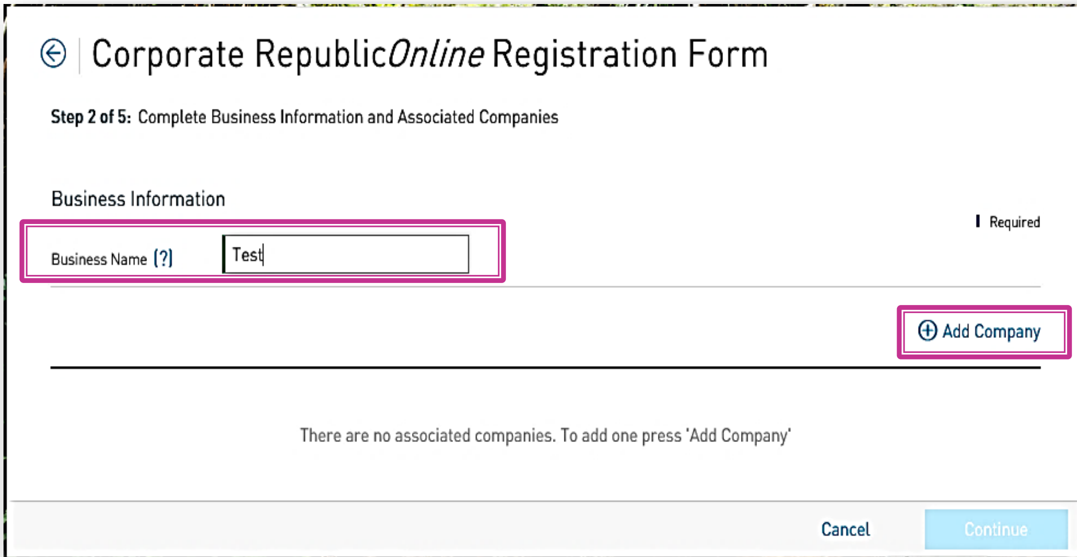
Step 5:
Download Registration Form and Obtain Autorization

Step 1: Accept Terms and Conditions



- Please read the Republic Online Terms and Conditions carefully
- Select the radio button labelled "Accept Terms and Conditions" once completed and Continue to proceed.

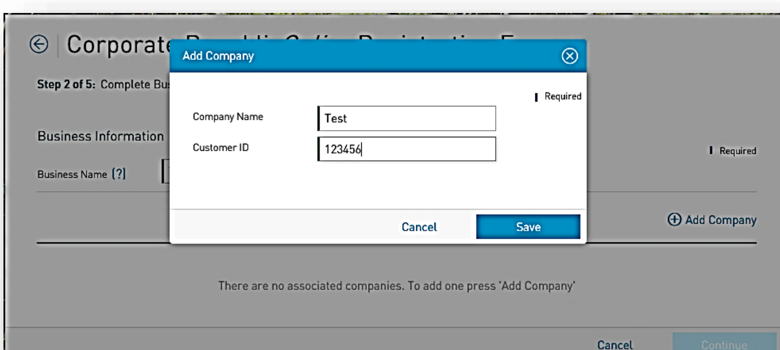
Step 2: Input Business' and any Associated Company's Information

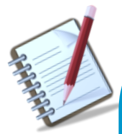


All mandatory fields will be denoted by the blue bar at the beginning of the field.

Required

- Please input the name of your business in the field provided
- Select the 'Add Company' option to input all associated companies.
  - For each company, the company name and customer ID are required (as shown below).

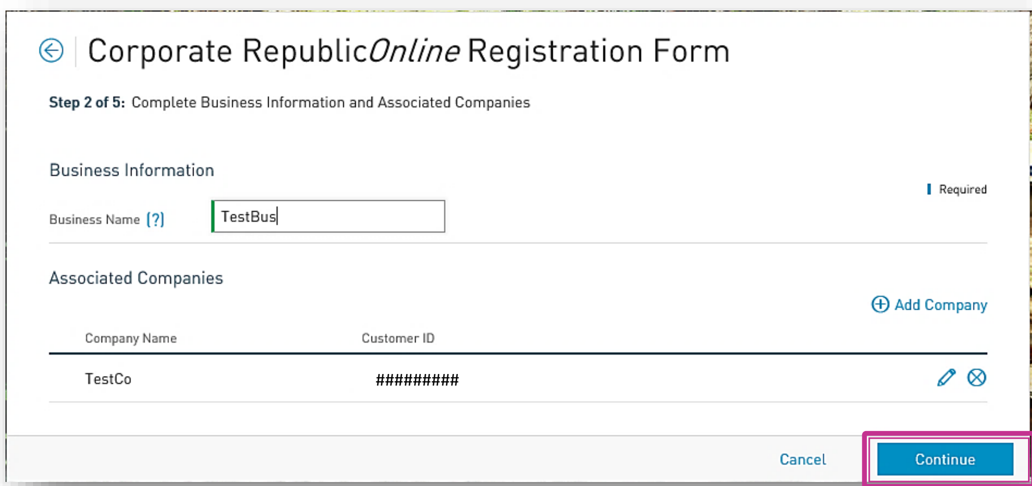




- **BUSINESS NAME: If your business comprises a group of companies, the business name would be the group name and then each company should be listed under the 'Add Company' option.**

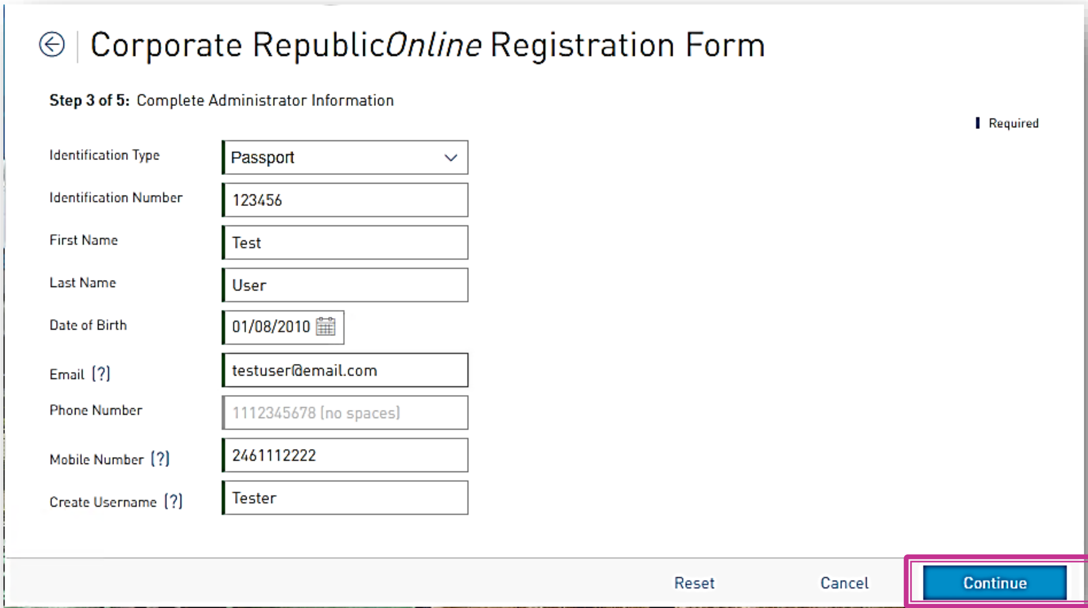
If you only have one company then the Business Name and Company Name would be the same.

- **CUSTOMER ID: The Customer ID will be provided by the Bank either at registration or, via mail. If you have not received your Customer ID, please contact your Engagement Lead.**

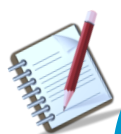


- Once you have finished inputting your company/companies' information, you will be redirected to the screen above.
- Select Continue to proceed to step 3.

Step 3: Input Administrator's Information

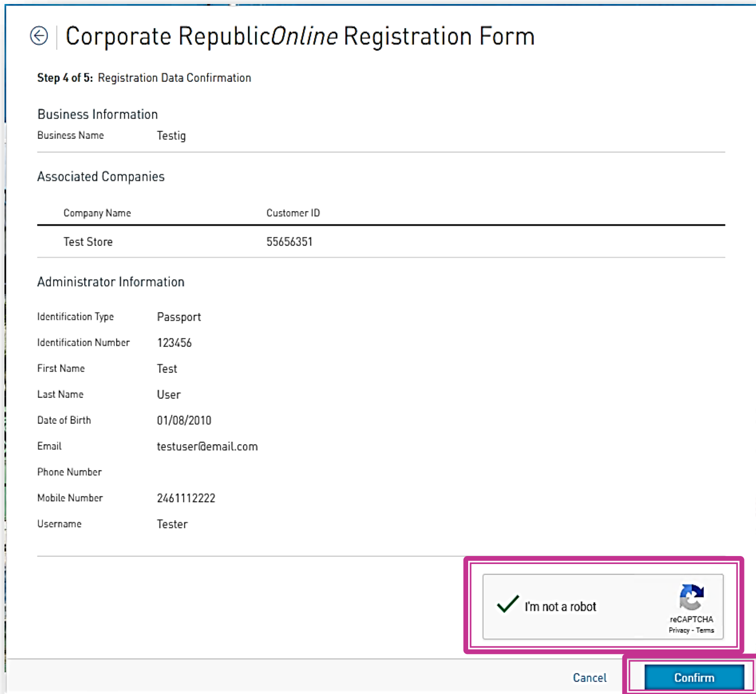


- Please enter the details of the Company Administrator (your details).
- Once completed select **Continue** to proceed to step 4.



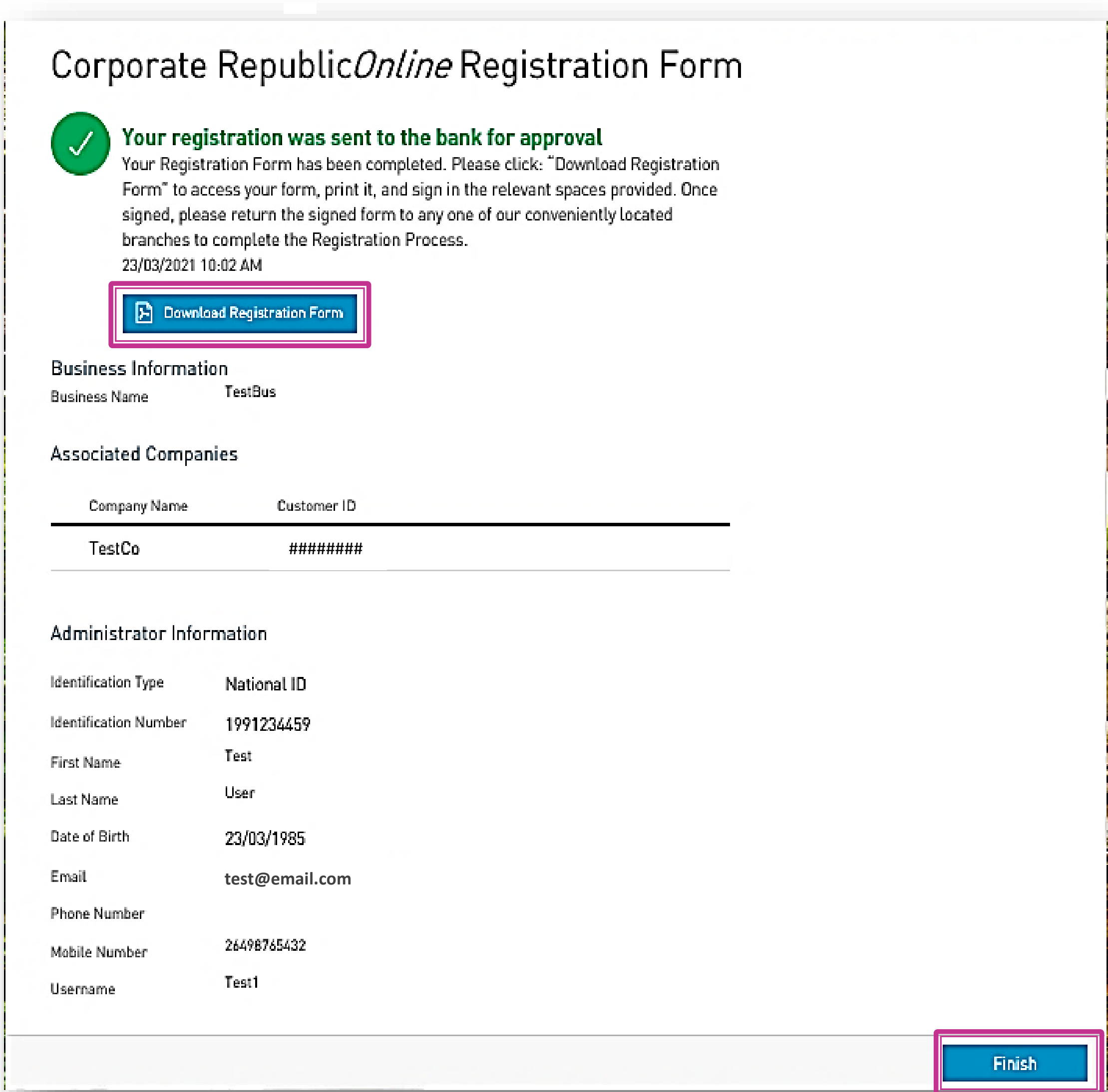
- **_ID type and Number_: These will be used for future instances where the user needs to be verified**
- **_Date of birth:_ Used to validate the age of the user. All Corporate RepublicOnline users must be _18yrs_ or older.**
- **_Email:_ This email will be used to confirm registration of user, send temporary passwords (OTPs) and any future correspondence for resetting the user's account.**
- **_Mobile Number:_ Mobile devices are required to be registered for second factor authentication.**
- **_Username:_ All users have the flexibility of creating their own unique Username (alphanumeric/no special characters allowed)**

Step 4: Registration Data Confirmation



- Once all the required data has been entered, you will be required to confirm the details on the confirmation page.
- Confirm the reCaptcha by selecting the radio button labelled '***I am not a robot***'.
- Select Confirm to proceed to Step 5.

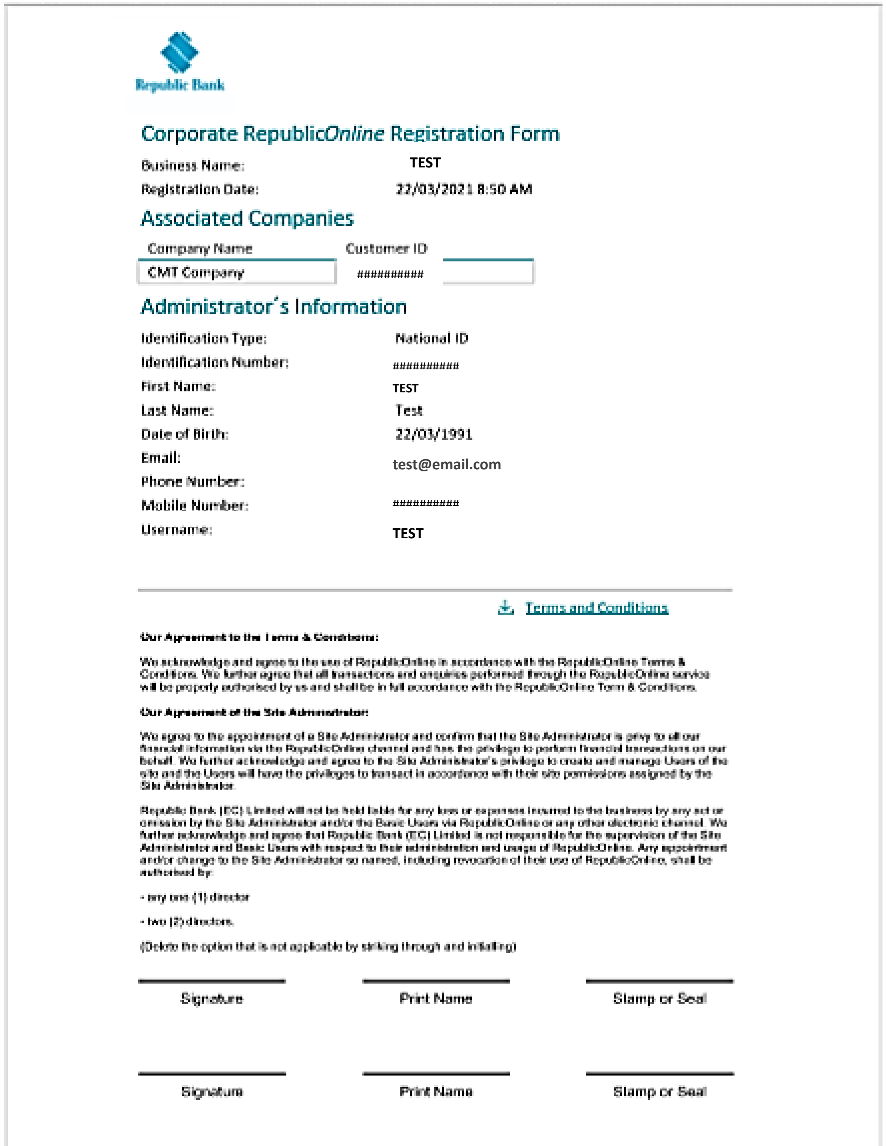
Step 5: Authorisation



When the data is verified, the user will receive the confirmation message above, confirming that the request has been submitted to the Bank for approval.

> **The request will not be approved until the bank receives and validates the authorized registration form which bears the Director's signatures and company official stamp as listed in the Bank's records.**

- Click on the **Download Registration Form** to retrieve the registration form.



Republic Bank

Corporate Republic*Online* Registration Form

Business Name: TEST

Registration Date: 22/03/2021 8:50 AM

Associated Companies

Company Name	Customer ID
CMT Company	##########

Administrator's Information

Identification Type:	National ID
Identification Number:	##########
First Name:	TEST
Last Name:	Test
Date of Birth:	22/03/1991
Email:	test@email.com
Phone Number:	
Mobile Number:	##########
Username:	TEST

Terms and Conditions

Our Agreement to the Terms & Conditions:

We acknowledge and agree to the use of RepublicOnline in accordance with the RepublicOnline Terms & Conditions. We further agree that all transactions and enquiries performed through the RepublicOnline service will be properly authorised by us and shall be in full accordance with the RepublicOnline Term & Conditions.

Our Agreement of the Site Administrator:

We agree to the appointment of a Site Administrator and confirm that the Site Administrator is privy to all our financial information via the RepublicOnline channel and has the privilege to perform financial transactions on our behalf. We further acknowledge and agree to the Site Administrator's privilege to create and manage Users of the site and the Users will have the privileges to transact in accordance with their site permissions assigned by the Site Administrator.

Republic Bank (EC) Limited will not be held liable for any loss or expenses incurred to the business by any act or omission by the Site Administrator and/or the Basic Users via RepublicOnline or any other electronic channel. We further acknowledge and agree that Republic Bank (EC) Limited is not responsible for the supervision of the Site Administrator and Basic Users with respect to their administration and usage of RepublicOnline. Any appointment and/or change to the Site Administrator so named, including revocation of their use of RepublicOnline, shall be authorised by:

- any one (1) director

- two (2) directors.

(Delete the option that is not applicable by striking through and initialing)

Signature	Print Name	Stamp or Seal
Signature	Print Name	Stamp or Seal

- Print the form and pass to the relevant company authorities who must sign and affix the company stamps on the form.

  Scan and submit the authorized form to **rbsribsupport@republicbanksr.com**

When the request is approved, the System Administrator will receive an email notification.

What makes the site secure?

What will I need to access the system?

To access the application, you will need the following:

Username:

- Users can set their own username at registration. The username is not case sensitive, but it must be unique and alphanumeric (i.e. comprise letters and numbers). Special characters (**e.g. "@", "_" or "**) are not permitted.

Password:

- Users set their password during the registration process.

(*See Password guidelines on page 22*)

Security Image:

- At your first login to the application, you must select one security image from the options provided.

- The image will be used as an anti-phishing device. Thereafter, each time you log in to Republic*Online*, the selected image will be displayed. This helps you to differentiate between the correct site versus a phishing site.

Second Factor Authentication Device:

- Users **must** register a mobile device, which will be used for authentication when logging on.
- This mobile device maybe a mobile phone or a tablet.
- Each user will also be required to select the preferred channel from the following options:

  - **SMS Code:**
    If this option is selected, each time an attempt is made to access the application via the web, a unique SMS code will be generated and sent to the registered mobile number, which the user will be prompted to enter.

  - **RepublicMobile App:**
    The Republic Mobile App offers 2 options for users:

    o ***OTP (One-time Password)***

    Each time the user attempts to login to Republic*Online*, the system will generate an OTP code which the user must retrieve via the mobile app, and input on the web login.

    o **SYNC**
    When the user attempts to login to the application via the web, the system will attempt to connect or sync with the registered mobile device. The user will be required to either "Accept" or "Reject" this connection, before proceeding.

- **SMS fees may be applicable in some cases**
- **The user will set the username at Registration. All other security features will be setup thereafter, at the user's first login.**

What are the Security Restrictions?

The following constraints have been deliberately imposed in the application to enhance the security and integrity of the system and the transactions conducted online:

Disabled Back Button

If you select the Back button, the system will terminate the operation and the login page will appear.

Session Timeout Duration

To enhance the security, the system is equipped with a Session Timeout feature which enables the application to log off after 20 minutes of inactivity. The system will advise that the session has expired and prompt you to log in again.

Unique session control

The system will only allow you to access one session at a time. In instances where you attempt to log into the system and there is already an active session using the same credentials, a warning message will appear advising that you must cancel one of the active sessions before proceeding.

What are the Password Guidelines?

Consider the following guidelines when creating your Republic*Online* password:

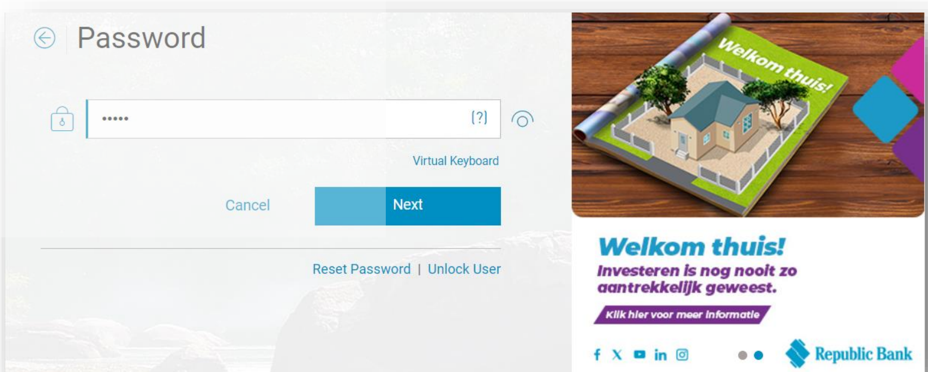
- The password should contain a minimum of 12 and maximum of 64 characters and requires atleast one Uppercase, one numeric and one special character (e.g. @#$%^&* etc)
- Avoid using names of pets, parents or friends & relatives for your passwords.
- Refrain from using passwords containing all the characters in your login ID. For example, if your login ID is 'jSmith', then your password should not be 'jSmithOne'.
- The password fields will not allow any information to be copied from the clipboard

- Spaces and other special characters are not allowed in the password.
- Change your password at regular intervals.
- Always avoid the use of the ‘saved password’ feature offered by any mailing application or software.
- Ensure you always logout of the application, terminating transactions and all possible activities.

What are the Second Factor Authentication Device Guidelines?

The following are guidelines for the use of the second factor authentication device:

- The device may be a mobile phone or a separate tablet with a sim card and/or wifi accessibility.
- The selected should belong to the Internet banking customer.
- Avoid leaving the device unattended.
- Always ensure that you use the screen lock.
- Connect to secure WIFI to conduct internet banking transactions, as public WIFI hotspots may be susceptible to hackers.
- Keep your device's operating system up-to-date, to ensure that you have the most secure and efficient experience.

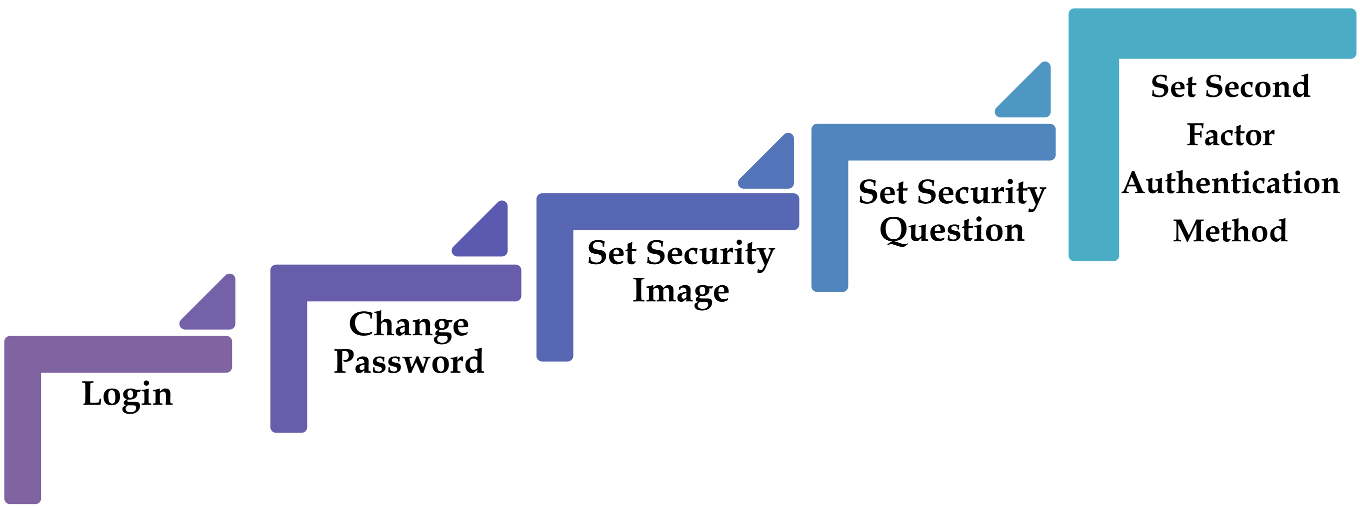

Password
Virtual Keyboard
Cancel
Next
Reset Password | Unlock User
Welkom thuis!
Welkom thuis!
Investeren is nog nooit zo aantrekkelijk geweest.
Klik hier voor meer informatie
Republic Bank

Logging in

Things I should know about the First Login

- As the site administrator, you will be the first user to access the Company's site. You will be required to login and complete the setup of your administrator profile first, then proceed to create the profiles of all other user's required by the Company.
- As the Site Administrators, you can create 2 types of users: **Basic** or **Administrative**
- All users, when created, will receive an email with a temporary password, which they must use to access the system for their first login.

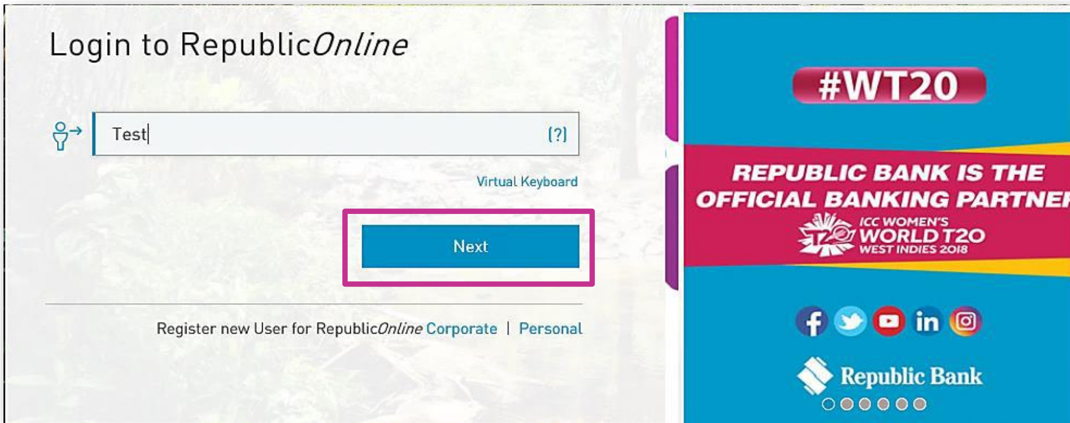
The first login entails the following **five(5)** step process for all users:



What are the steps involved in the First Login Setup?

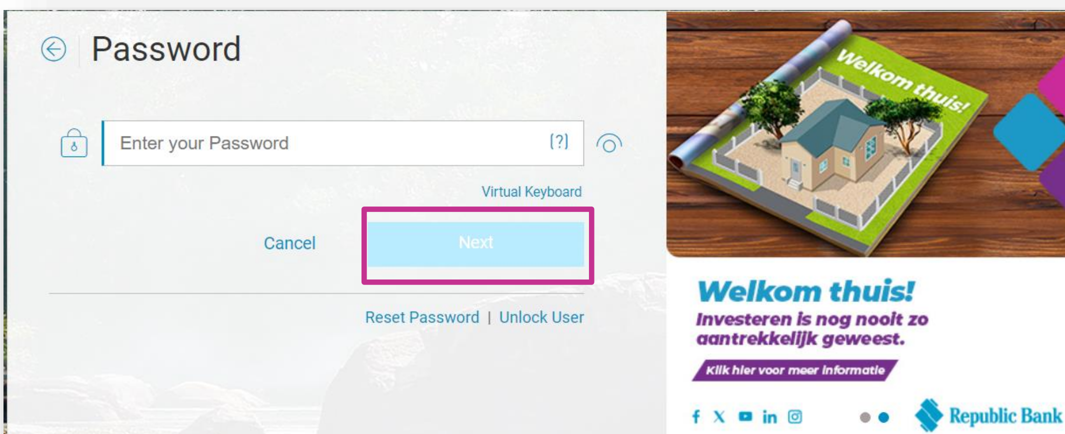
Step 1. Login

You must logon to Republic*Online* using the username chosen at registration.



- Click  to proceed.

You will then be redirected to the password screen.

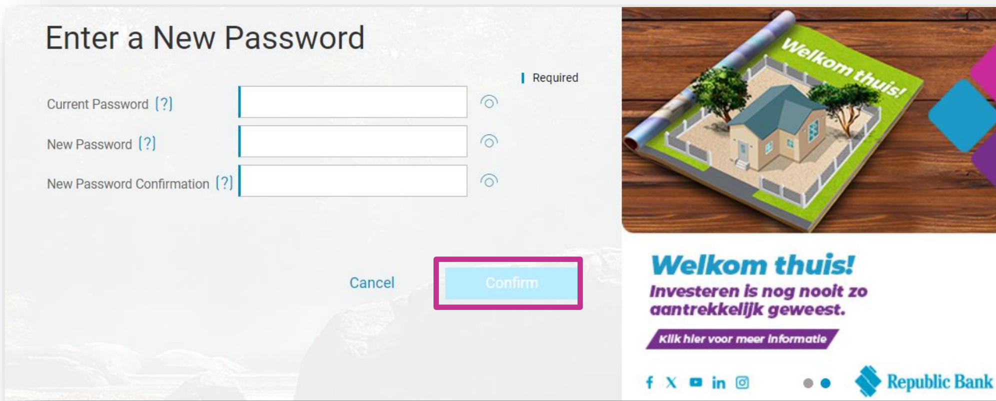


- Enter the temporary password sent via email and select to continue to step 2.

Users will have the choice of using a virtual keyboard, as an anti-key-logging device

Step 2. Change the password

When the temporary password is entered, you will be prompted to change the password:



The "Current Password" will be the temporary password sent to the user via email

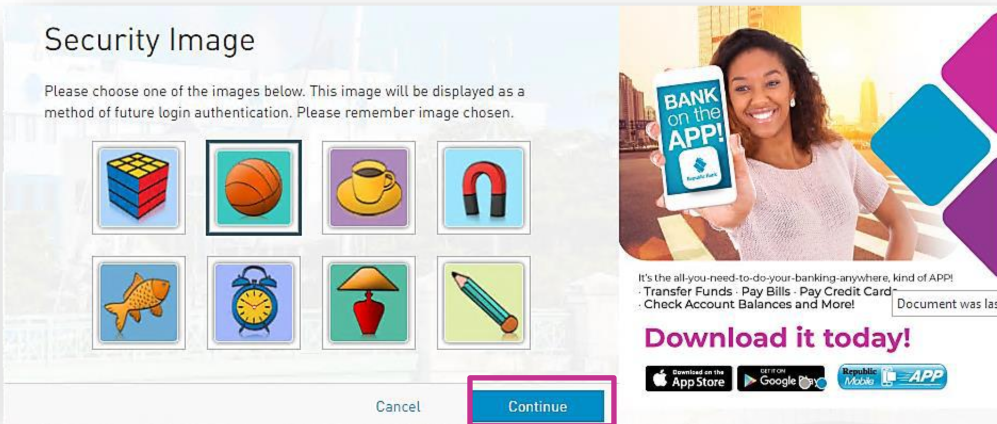
- Once this step is completed, select Confirm and continue to step 3.

The Password selected should be 12-64 characters long and must include at least one capital letter, one number and one special character

Step 3: Set Security Image

The security image functions as an anti-phishing device. The image selected here, during the security setup will appear during all the user's future logons. This reassure users that they are logging into the correct site.

Select one (1) image from the list provided.



- Click Continue to proceed to the following step of the security setup process.

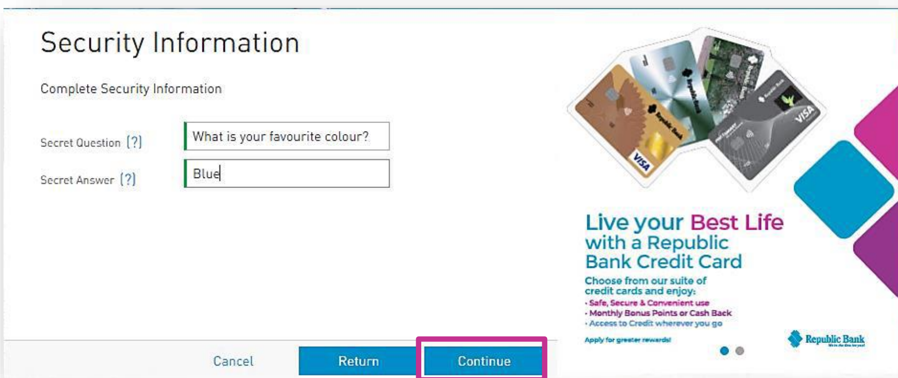
The chosen image will not be saved until all the steps are completed

- The Cancel option cancels the entire process and redirects you to the login screen.

Step 4. Set Secret Question

The secret question will be used as a validation to update personal data, security and user settings.

You must create your own secret question. The system does not provide any templates or options for the secret question.



- Enter a secret question (of your choice)

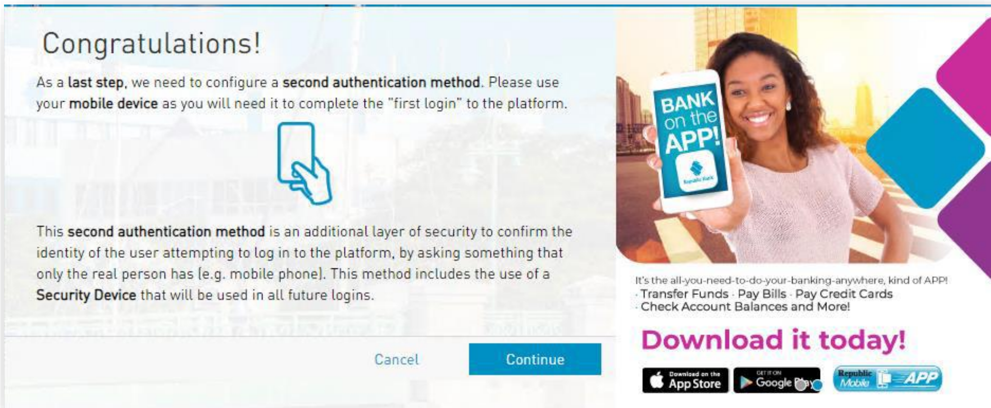
- Enter the answer to the question in the "Secret Answer" field provided.

- Select Continue and proceed to step 5 of the process.

  - **Return:** redirects user to the previous step
  - **Cancel**: takes user to the login screen

The secret question and answer are not case-sensitive

Once completed the user will receive the following message.



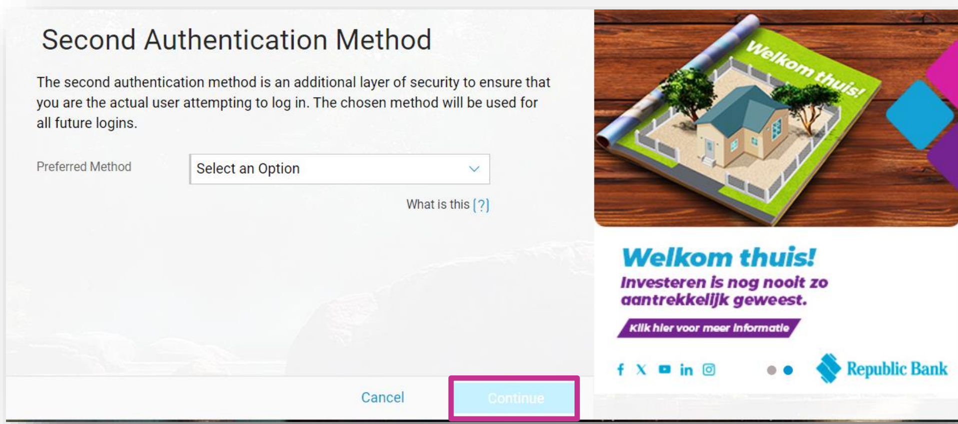
- Select 

Step 5. Select Second Authentication Method

The final step in the process is the setup of the second-factor authentication method. This security device will serve as an additional layer of security.

This step involves the enrolment of a separate, mobile device which will be used to validate the user at each login.

The options available here are *SMS* and *Mobile App.* You will be required to select one of these options and enter the mobile number, to register or enrol the device.



The second-factor authentication device will only be required for web logins only. Mobile App. users will not be required to have a separate security device when accessing the App unless they are accessing their login via another app that is NOT the Security Device

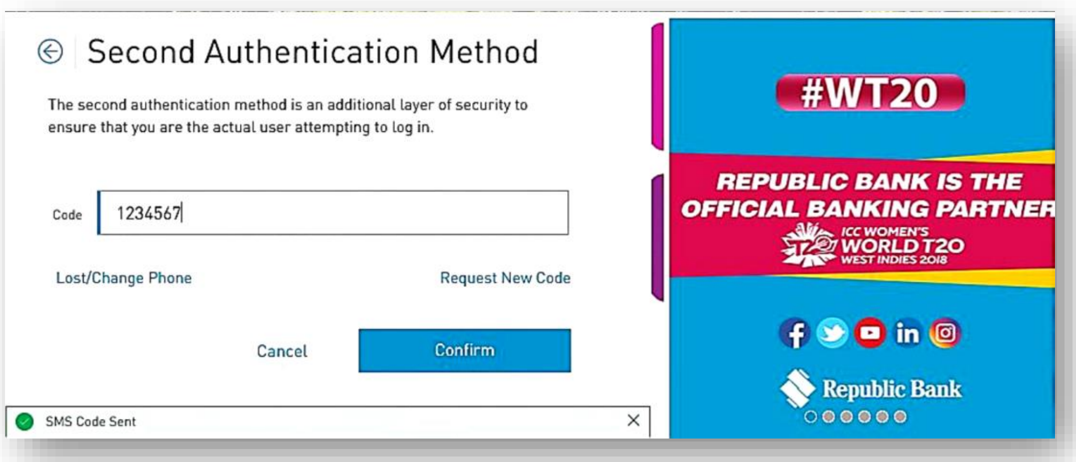
Option 1- SMS:

Once the SMS option is selected, you must perform the following:

1. Confirm Mobile Number → **2. Enter SMS Token** → **3. Confirm Action**

1: Confirm/Input Mobile Number

Input the mobile number you wish to enrol and select Confirm to proceed.



- **The SMS option requires the user to enter a local mobile number.**
- **The prefix for the mobile number being used is also required for registration (E.g.597#######)**

2: Enter SMS Token

An SMS code/token will then be sent to the mobile number entered. Enter the code received in the field labelled "Code"

3: Confirm Action

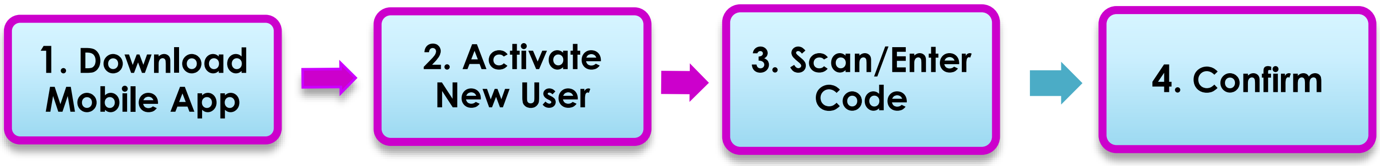
Select Confirm to complete the registration of the mobile device.

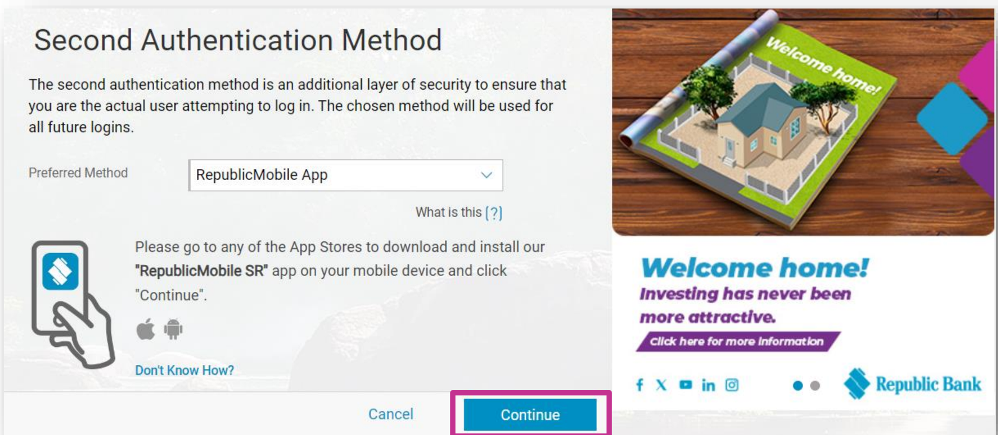
When this step is completed, you will be redirected to the Republic*Online* dashboard.

Each time an attempt is made to login to Republic*Online*, you will receive an SMS, containing a code/token which must be entered on the website to validate the user.

Option 2 - RepublicMobile App:

When the Mobile App option is selected, you will be instructed to complete the following:





1: Download the App

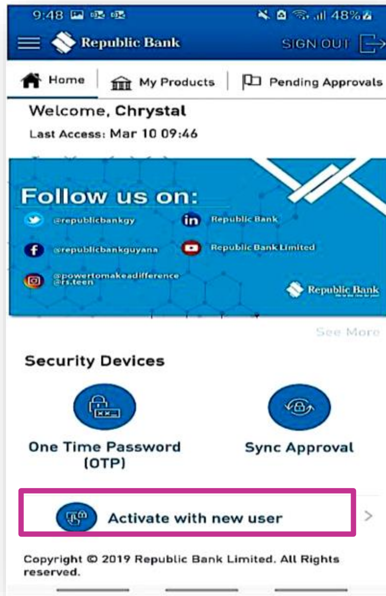
The Republic Mobile App is available on both Android and Apple devices.

Go to the relevant app store, search for **RepublicMobile SR App** and download.

GET IT ON Google Play   Download on the App Store

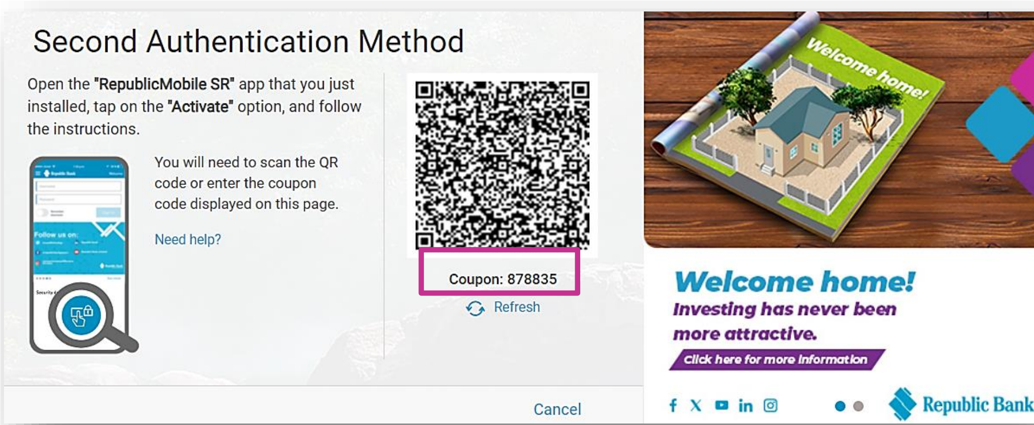
2: Activate New User

Once the Mobile App has been downloaded, you will be prompted to activate the new user. Launch the App and select the '*Activate with new user*' option at the bottom of the screen

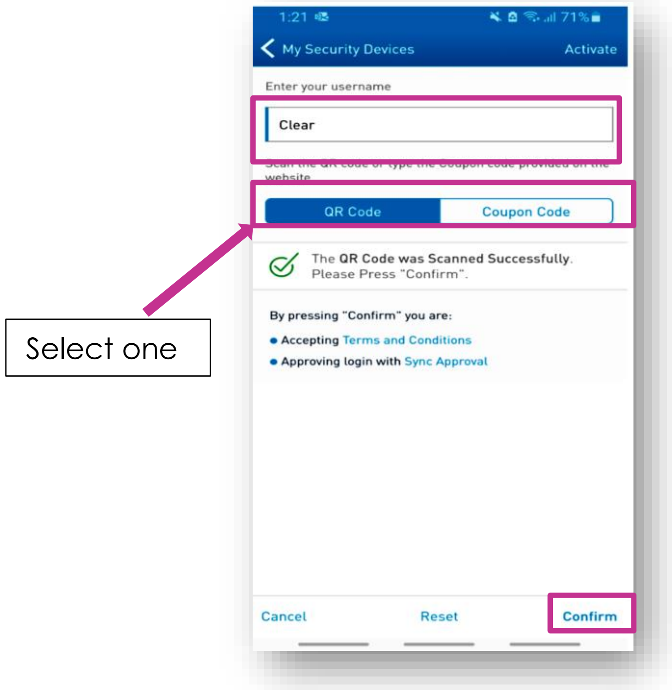


3: Scan/ Enter the Code

At this stage the website will display a QR code and a Coupon below.



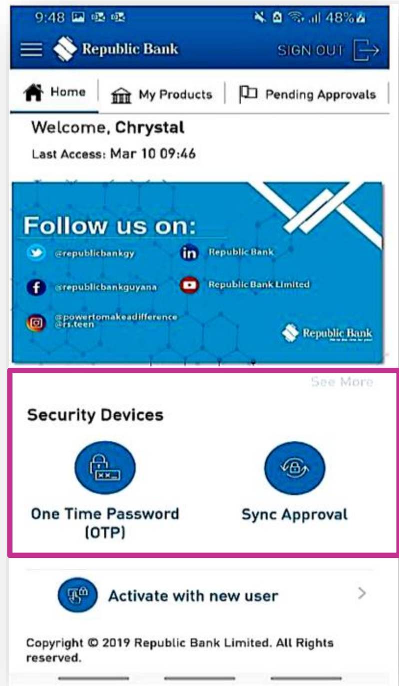
On the Mobile App, enter your Username, and then, either scan the QR code or enter the coupon displayed on the Site.



4: Confirm Action

Once the code entered has been successfully accepted, select **Confirm** to complete the registration of the mobile device.

The Mobile App offers two (2) options for users. At each login attempt to Republic Online, you must select either the (i) OTP or (ii) Sync option



OTP

To retrieve the OTP the user must go to the Mobile App to generate it. Once the OTP is obtained, enter it into the required field, and select **Next** to proceed.

OTPs are generated by the Mobile App on request. These are set to expire one (1) minute after being generated. If the incorrect OTP is entered, or, if it expires before being used, you will be required to generate another one.

Sync

When the Sync option is selected, the system will attempt to connect to or synchronize with the registered mobile device. Before proceeding, you must either Accept or Reject the request.

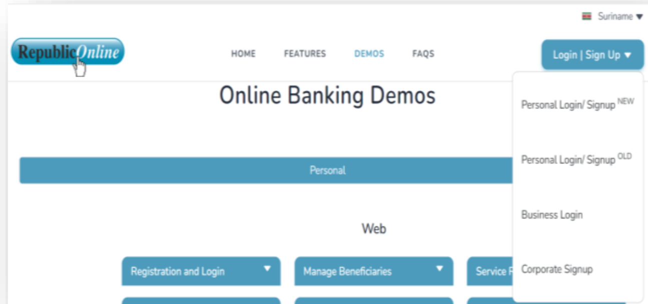
How to perform a Regular Login?

The regular login process entails four (4) simple steps

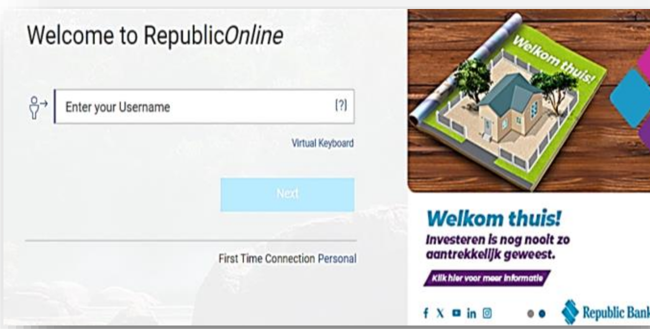
1.

Step 1: Access Republic Bank's website:

- Access the site
- Click login



2.



Step 2: Enter the Username:

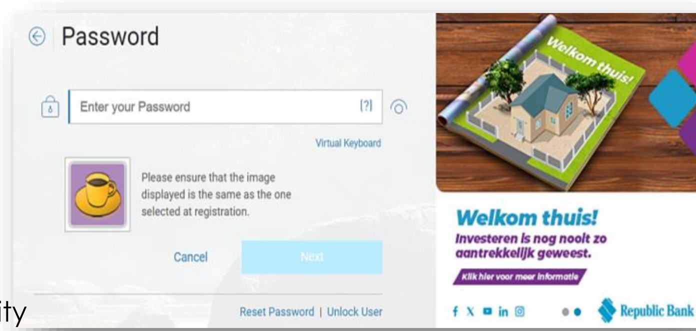
Enter your Username in the field labelled ***Enter your username*** *and click*

Next

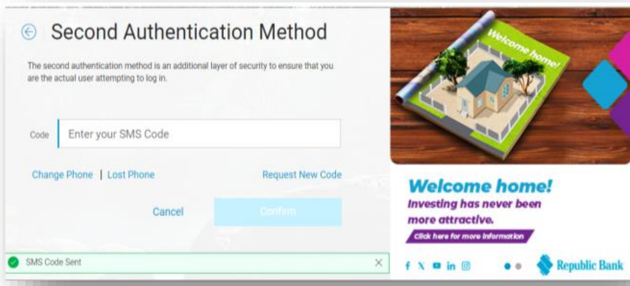
3.

Step 3: Enter the Password:

- Enter the password in the field provided.
- Ensure that the image displayed is the one selected during the security setup.
- Select Next to proceed



4.



Step 4: Second factor authentication:

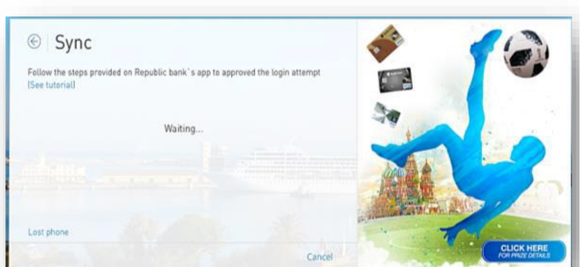
SMS: If the SMS token was selected as the second factor authentication device, the system will send a code to the associated mobile device via SMS. Enter the code in the field labelled Code and click Next to proceed.

RepublicMobile App:

If the mobile app was selected second factor authentication option, the user must select either the *OTP* **or** *Sync option*

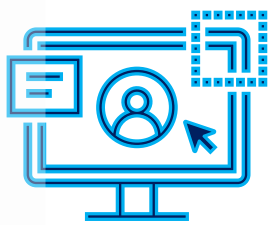
OTP: Open the RepublicMobile App on the associated mobile device to retrieve the OTP

- Enter the OTP in the field provided and click Next to proceed.



Sync: Go to the mobile device and select **Accept**.

Once this step is complete select Next to proceed to the Home Page.



Managing the Site's Administration

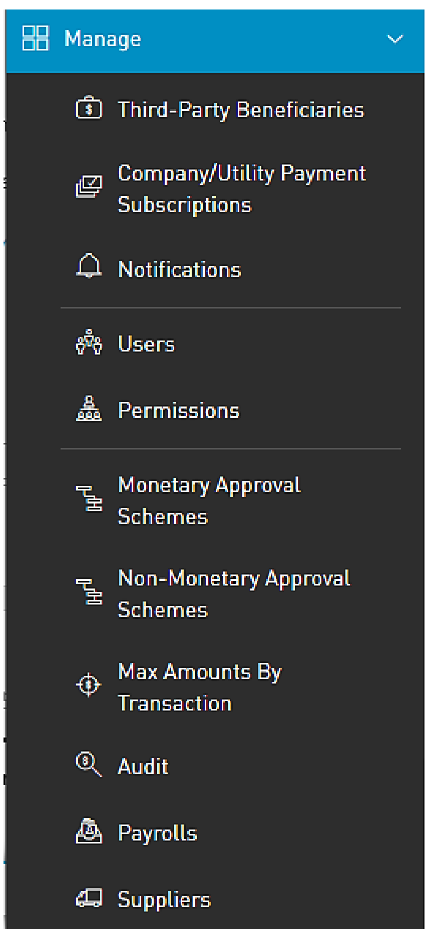
What is Republic*Online* Site Administration?

- In Corporate Republic*Online* a Business enterprise is given an Internet Banking Profile; This is referred to as the ***Business Site***.

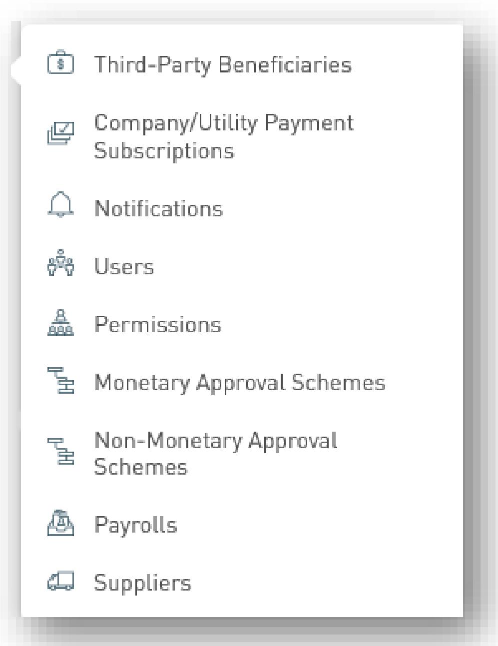
- The Site comprises all the business' companies (if applicable) as well as all their products and the services available to them.

- Each company or business is responsible for administration of their own site and has the flexibility to set-up their user how they see fit. The Bank will only intervene if assistance is requested, in cases where there may be a need to troubleshoot an issue.

- All of the administrative features on any Business' Site can be accessed via the **Manage** Tab in either the **Quick** or **Main Menu.**



OR



- This section outlines the admistration of the Business Site which will be managed by the *Site Administrator.*

What are the responsibilities of the Site Administrator?

For each Business Site, there must be a Site Administrator. The Site Administrator is created with the Business' Site and by default, this user is given administrative permissions, which enables them to conduct all the administrative and maintenance functions of the site. This includes the following:

1. Creation of users
2. Maintenance/amendment of user access (enable, delete etc.)
3. Assignment of permissions
4. Creation and maintenance of non-monetary approval schemes
5. Creation and maintenance of monetary approval schemes

The Site Administrator also has the permissions to amend their own profile as well as to create other Administrators.

What are Users, Permissions and Approval Schemes?

- These are the three (3) elements of any business site and govern how the site will be run and more importantly, who will be the key players in the running of the site.
- It is the responsibility of the Site Administrator to manage all of these, based on the company's requirements.
- In essence, the management of users is multi- layered but can be broken down by these three elements:

1- Users

- Created as a blank slate

2- Permissions

- Determine what the users can see/do on the site

3 - Approval Schemes

- Define which users can authorise/approve transactions

Users

Users (Overview)

The Site Administrator is created by the Bank and is responsible for the creation of all other company users. This administrator also has permissions to add, amend and delete users.

There are two types of users that may be created for a Business Site:

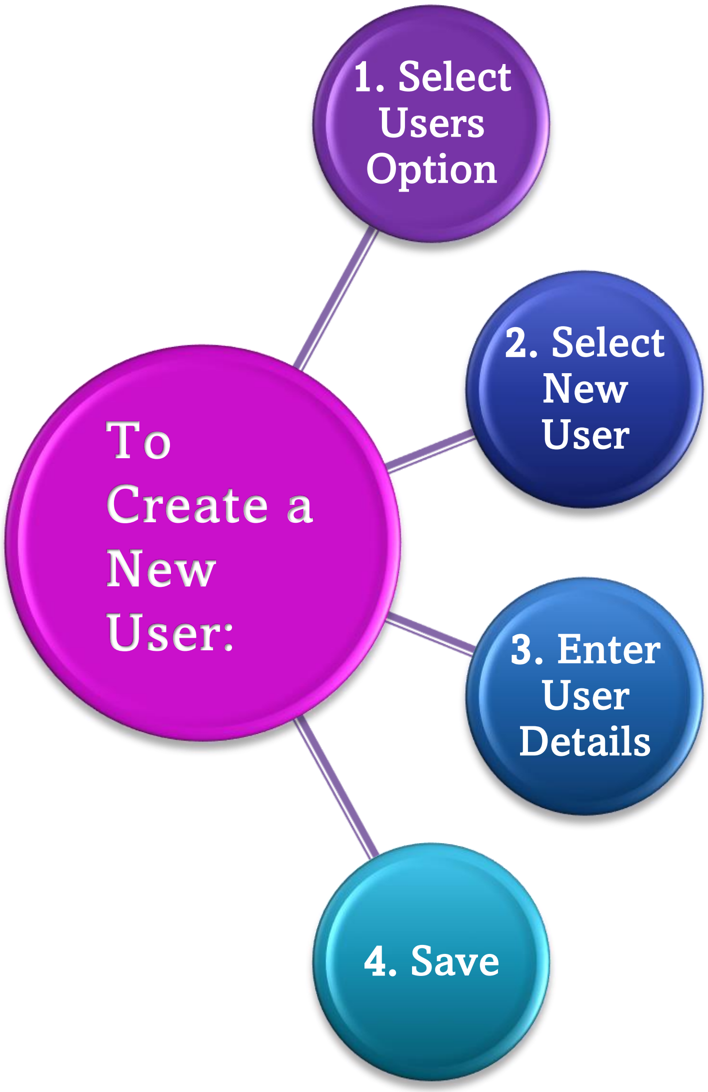
Users	***Administrator***	**Basic**
Features		
Creation	When a business site is created atleast one(1) Admininstrative User must be created with it.	Basic users are created by the Administratve user or Administrator subsequent to the creation of the site.
Default rights	Created with a default set of administrative permissions for the Site.	Created with no rights; in essence a blank slate. These users must be granted features and permissions by the Administrator.
Non-Monetary functions ***(Administrtive rights: to create/amend users, permissions, approval schemes and so on)***	By default the administrative users are granted these rights.	No default rights granted upon creation, but the administrator can grant non-monetary functions to these users if required.
Monetary Functions	By default these users are not granted monetary functions but if required, these functions can be added.	

In summary, a business has the flexibilty to create any combination of rights depending on the business need. In other words, they may create

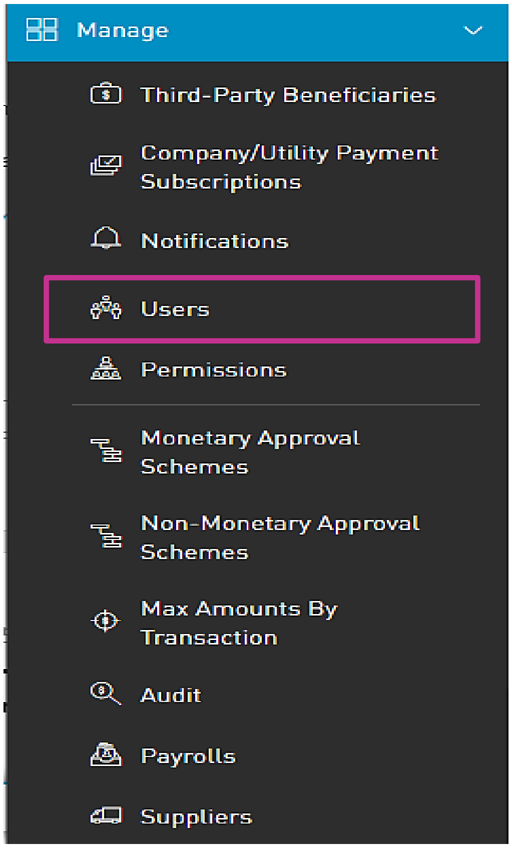
1. **User with administrator rights only**
2. **Basic User for Monetary transactions only**
3. **Administrator User with permissions for monetary transactions**
4. **Basic users with a mix monetary and administrative permission**

How to create a user?

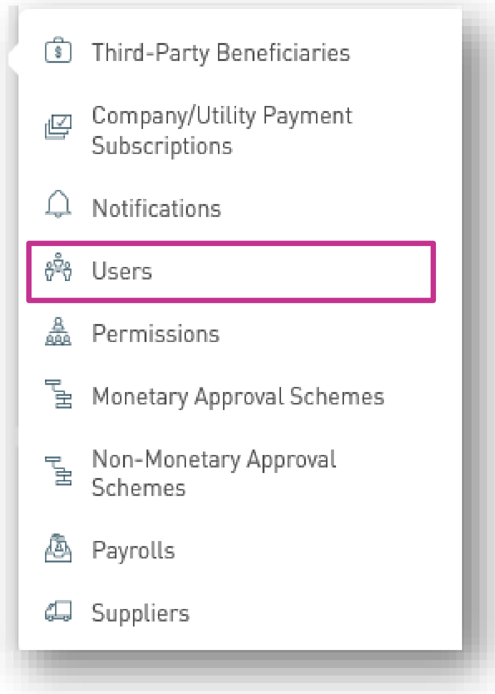
The User Creation process entails 4 steps as follows:



STEP 1: SELECT THE USERS OPTION UNDER THE THE MANAGE SECTION FROM EITHER THE QUICK OR MAIN MENU



OR



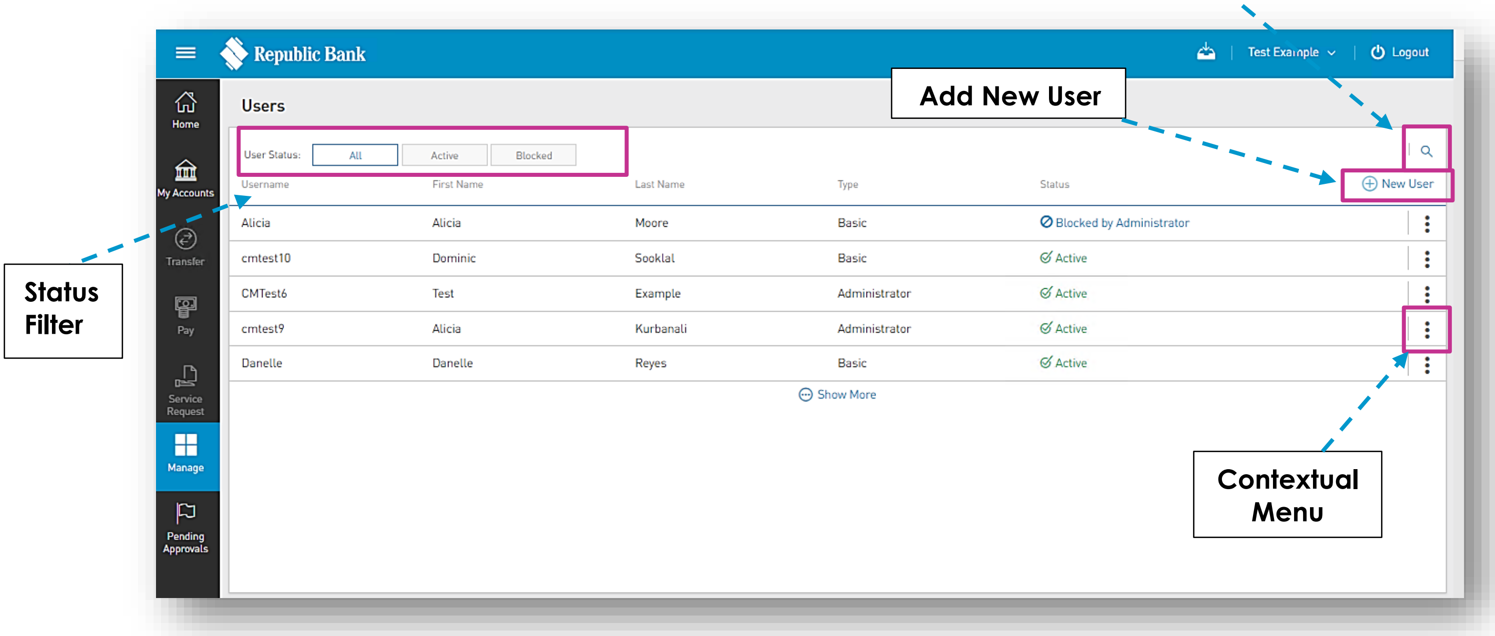
You will be redirected to the Users Page.

<u>Users Page</u>

This page contains a master list of all the Site's users, and includes the following:

1. Username
2. First and Last Name
3. Type (Basic or Administrator)
4. Status

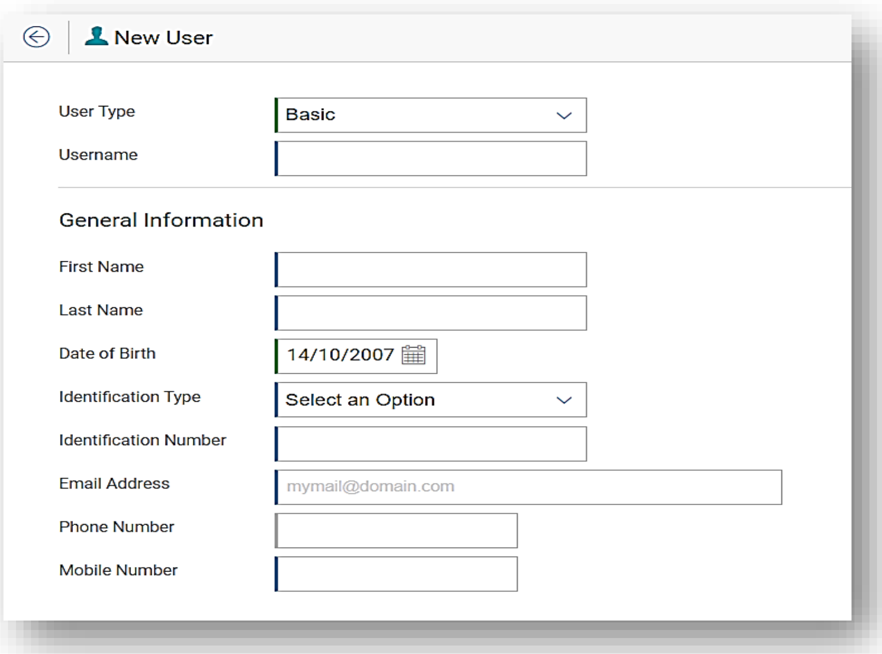
Search



Step 2: Select New User

Once this option has been selected you will be redirected to the *New User* page which contains a digital form to be completed for the new user.

Step 3: Enter the User Details



The following data will be requested for each user:

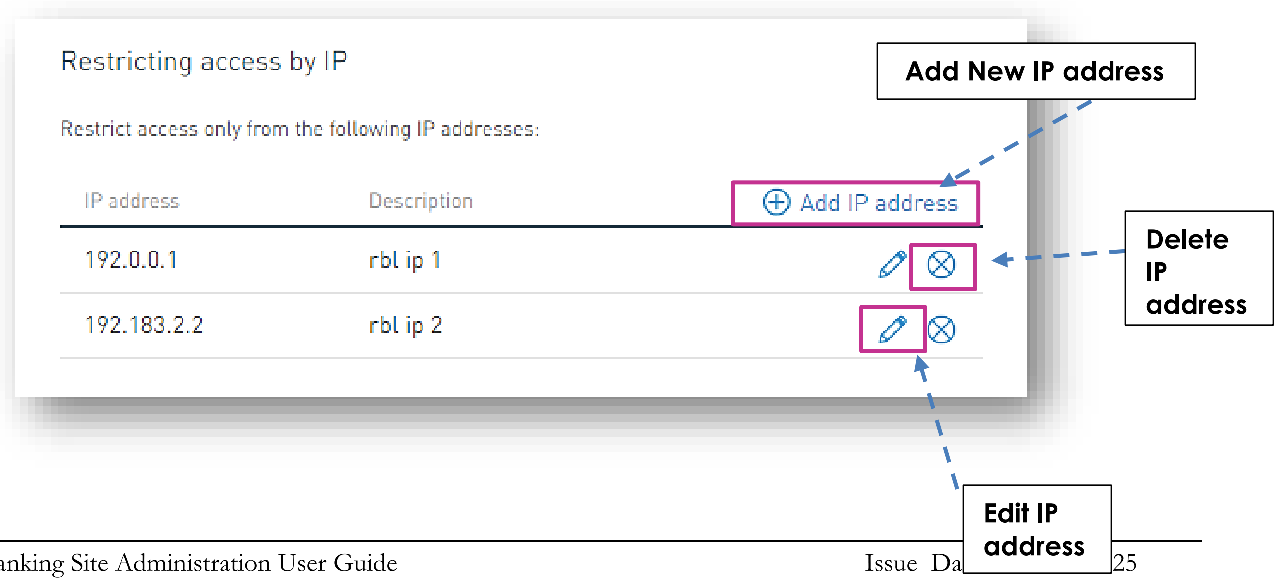
User data:

- User Type (Basic or Administrator) [Required]
- Username [Required]
- First Name [Required]
- Last Name [Required]
- Date of Birth [Required]
- Identification Type [Required]
- Identification Number [Required]
- Email Address [Required]
- Phone [Optional]
- Mobile Number [Required]

The Administrator may also restrict the user by IP Address. In this way, the user will only have access to the company's site from a specific location. **(Optional Feature)**

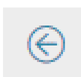
The following information will be requested:

- IP Address
- Description



STEP 4: SAVE

Once the required information has been input, select one of the following options to proceed:

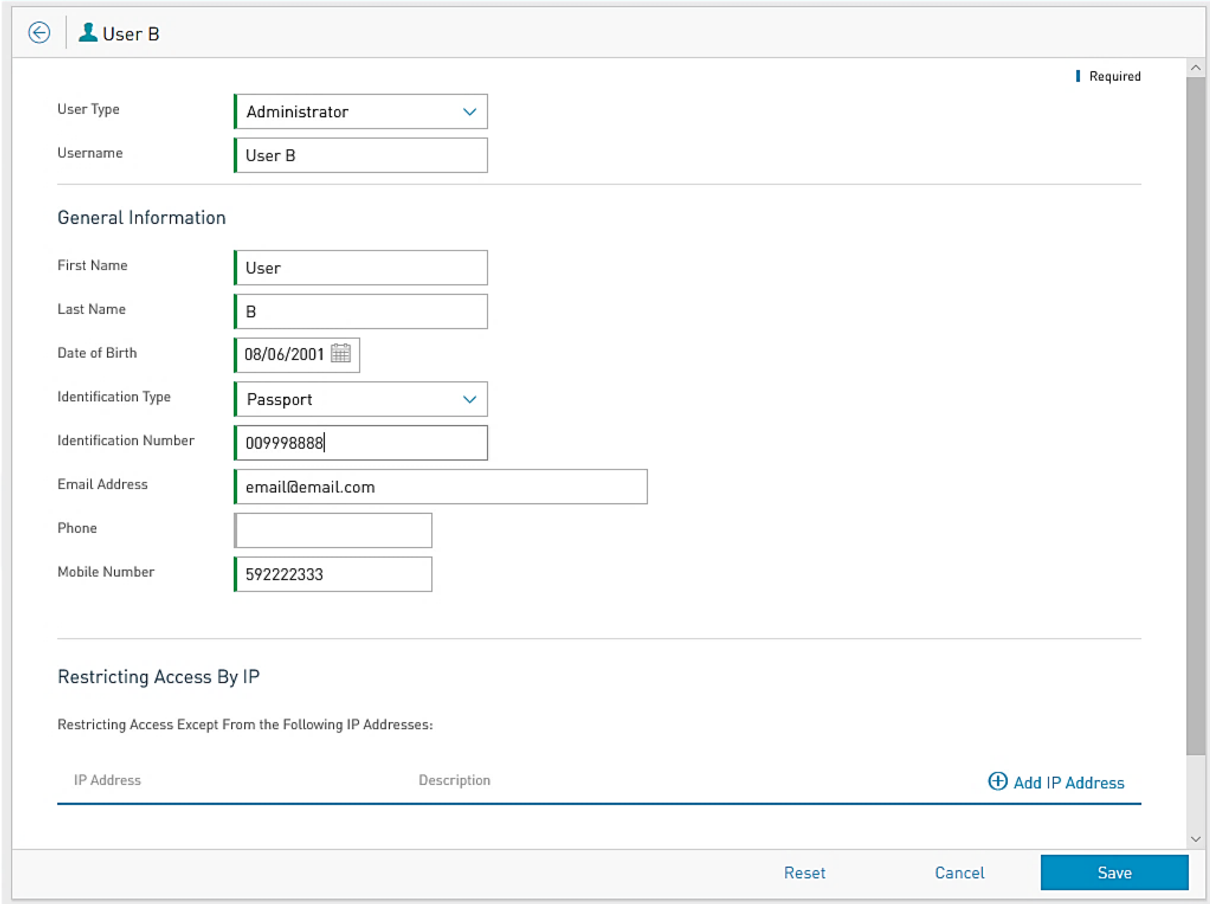
- **Save**: to save the new user.
- **Cancel**: to cancel the process
- **Reset**:to clear all the information entered in the screen.
-  to return to the previous page.

When the new user's profile is saved, he/she will receive an email notification, advising of their username and temporary password.

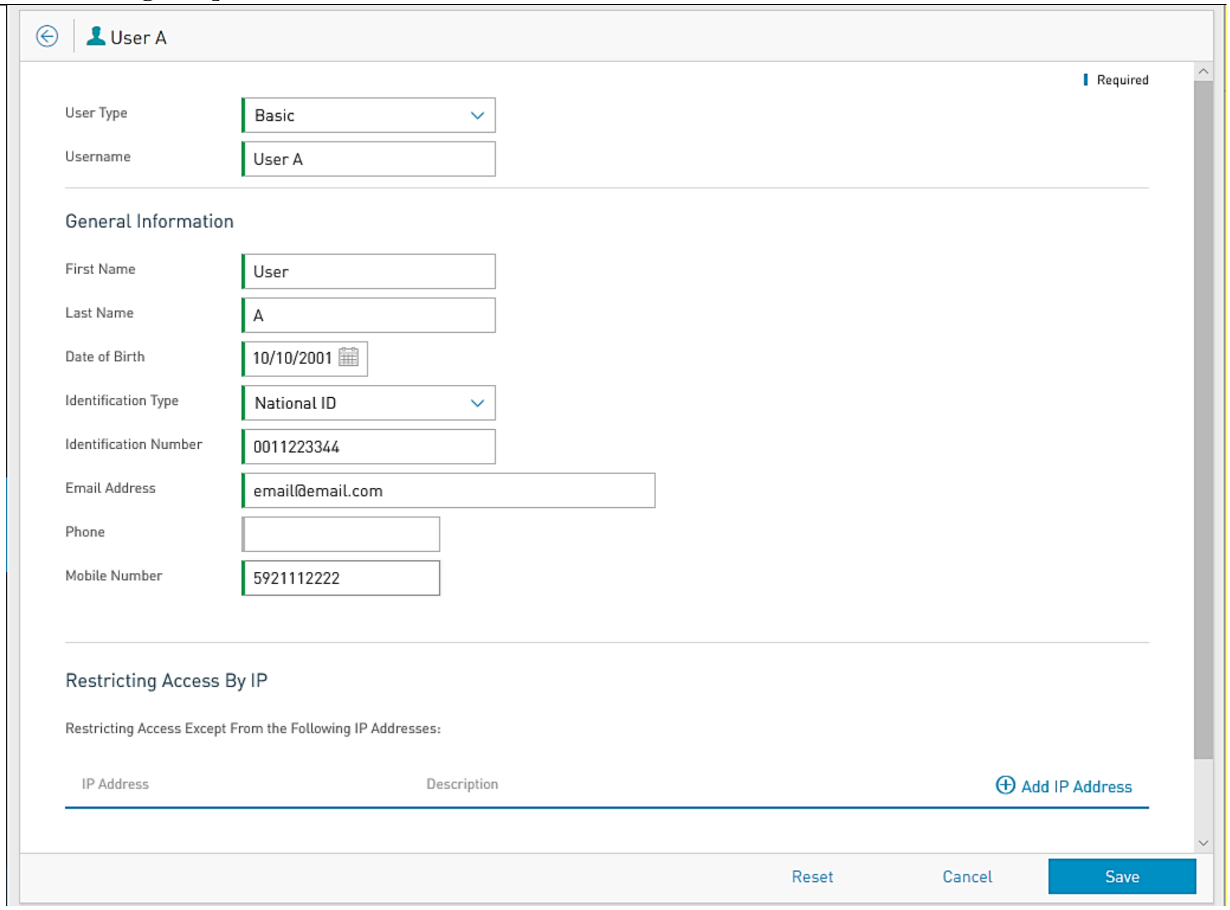
The user must then follow the First Login Setup process (25).

User Profiles

To view a user profile, select the "Edit" option on the contextual menu of the user, from the list.



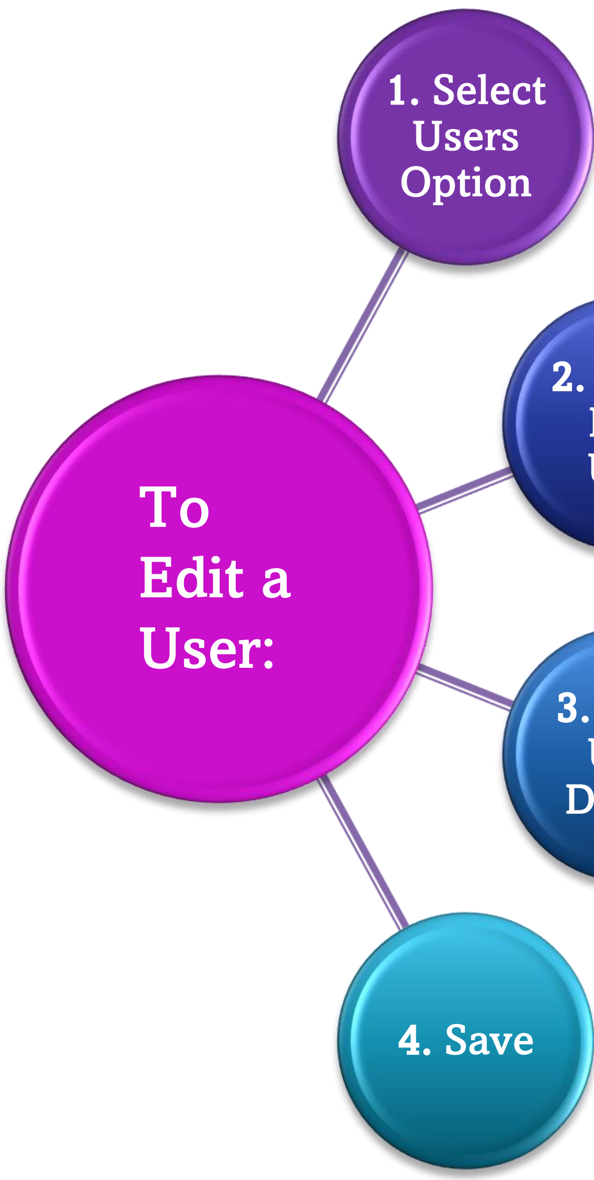
A – Example of an Administrative User Profile



B – Example of a Basic User Profile

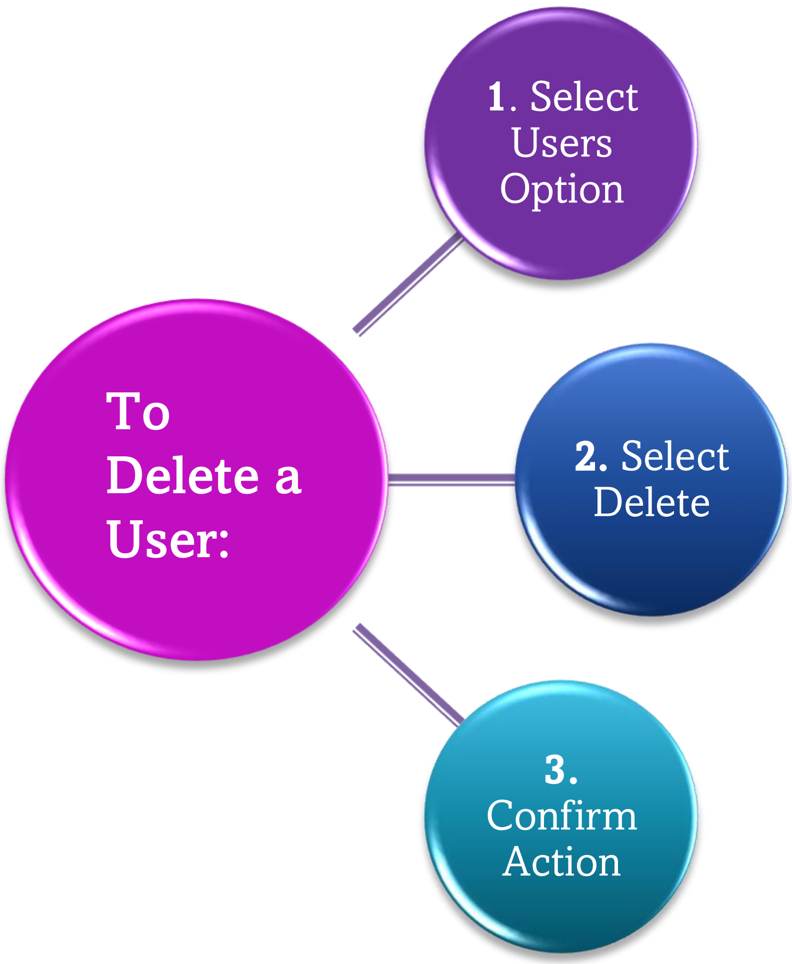
How to Edit a User?

There may be instances where a user's profile details need to be updated. The process to edit a user's profile entails **4** steps as follows:



How to Delete a User?

The process to delete a user's profile entails **3** steps as follows:

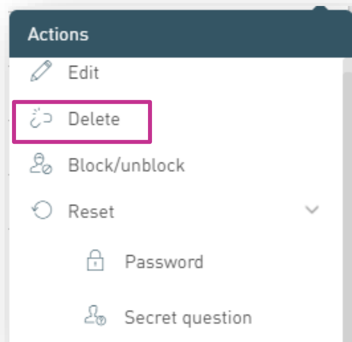


STEP 1: SELECT USERS OPTION:

Select the **Users** option under the the **Manage** section of either menu.

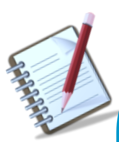
STEP 2: SELECT DELETE

Click on the ⋮ contextual menu of the respective user from the list displayed on the **Users Page** and select the "Delete" option.



STEP 3: CONFIRM ACTION

When this option is selected, a message box will appear, asking the Administrator to confirm the action. Select **Confirm** to proceed.

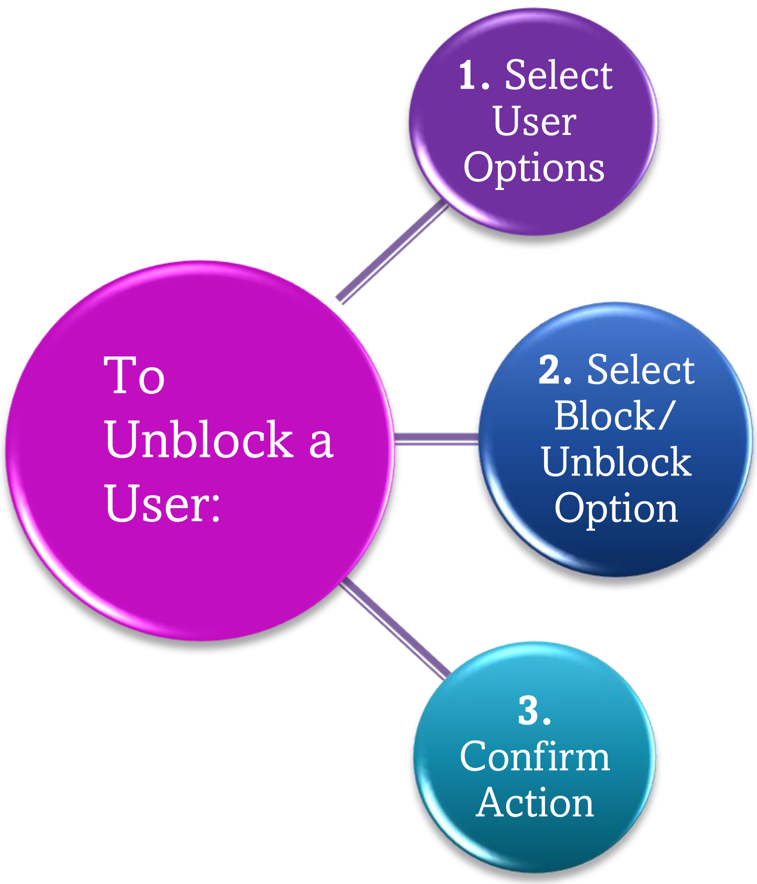


- **Only the Site Administrator, or users assigned the permission "Administration- Users" will be able to delete users.**
- **The Site Administrator cannot delete his/her own profile.**
- **A user whose profile has pending changes cannot be deleted.**
- **A company must always have at least one (1) Site Administrator. Therefore, the Site Administrator cannot be deleted unless another one exists for the Company.**

How to Block/Unblock a User?

The block and/or unblock feature is used to enable or disable a user's access when required.

The process to edit a user's profile entails **3** steps a follows:

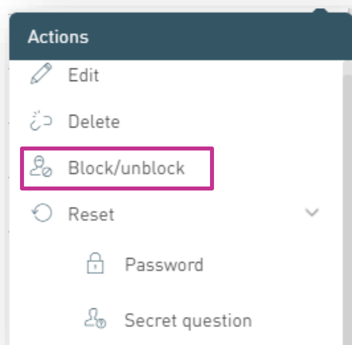


STEP 1: SELECT USERS OPTION:

Select the **Users** option under the the **Manage** section of either menu.

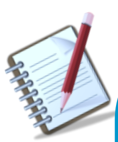
STEP 2: SELECT BLOCK/UNBLOCK OPTION:

Click on the ⋮ contextual menu of the respective user from the list displayed on the **Users Page** and select the "Block/Unblock" option.



STEP 3: CONFIRM ACTION

When this option is selected, a message box will appear, asking the Administrator to confirm the action. Select **Confirm** to proceed.

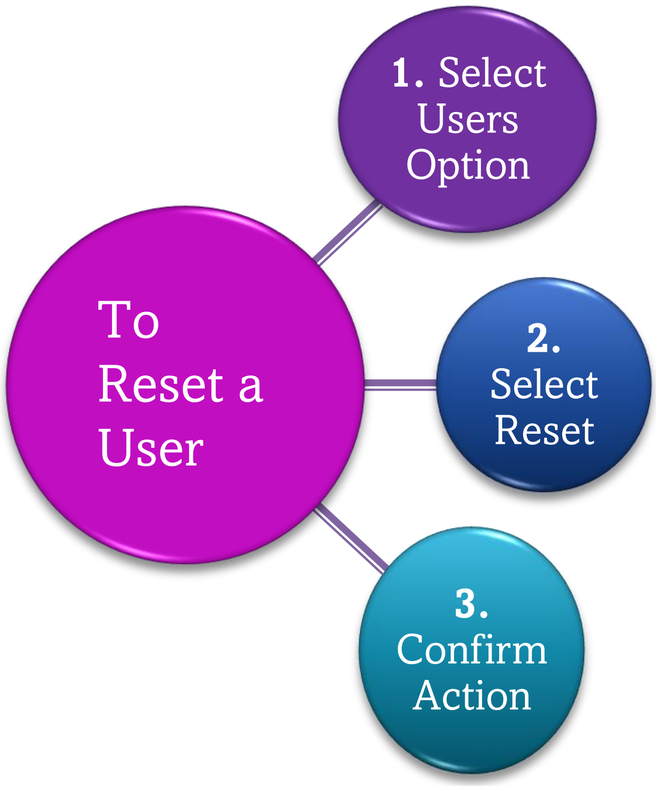


1. **An administrator can only unblock a user that was blocked by themselves or another company user.**
2. **A user whose profile has pending changes cannot be blocked/unblocked**
3. **A user that was blocked by the Bank cannot be unblocked by the company**
4. **A user blocked by security device cannot be unblocked by a company user.**

How to Reset a User?

A Company Administrator may reset Users' Passwords and/ or Secret Question if required.

The process to reset a user's profile entails **3** steps a follows:

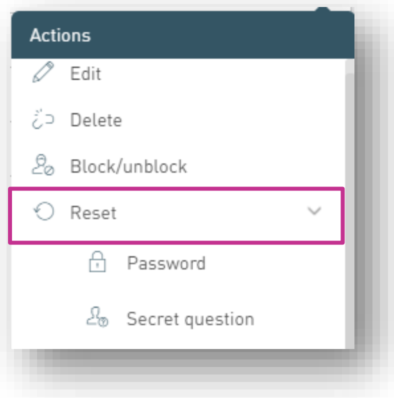


Step 1: Select Users Option:

Select the **Users** option under the the **Manage** section of either menu.

Step 2: Select Reset Option:

Click on the ⋮ contextual menu of the respective user from the list displayed on the **Users Page.** Click on the ⌄ icon to open the "Reset" options and select the option that needs to be reset (Password or Secret Question).



STEP 3: CONFIRM ACTION:

When the reset option is selected, a message box will appear, asking the Administrator to confirm the action. Select **Confirm** to proceed.

For Password Resets: An email will be sent to the user with a new password, which they will be required to change at their next login.

***For the Resetting of the Secret Question*: The user will be prompted to enter a new question and answer at their next login**

Permissions

Permissions (Overview)

Every action in a corporate site is governed by specific permissions.

Permissions are the rights or access privileges that are granted to all Republic*Online* users. These essentially define the access that the Corporate RepublicOnline user will have to the different features and transactions.

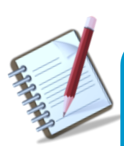
Without assigned permissions, users will be able to log on to the Site, but they will not have rights to view or conduct any transactions. Therefore,

Permissions are generally categorised into three (3) groups:

1. **Administrative** – These are related with the administration and maintenance of the site, users and so on.
2. **Product** – Associated with particular products or accounts
3. **General**

Examples:

Permission Name	Description	Permission Type
Administration – Users	Allows users to view and manage users of a site (this permission does not allow user to approve creation or edition of users)	**Administrative**
Account - Detils	Allows users to view the detail of a saving or checking account	**Product** (Chequing)
Financial Status – Assets and Liabilities	Allows users to view this web part in the dashboard	**General**



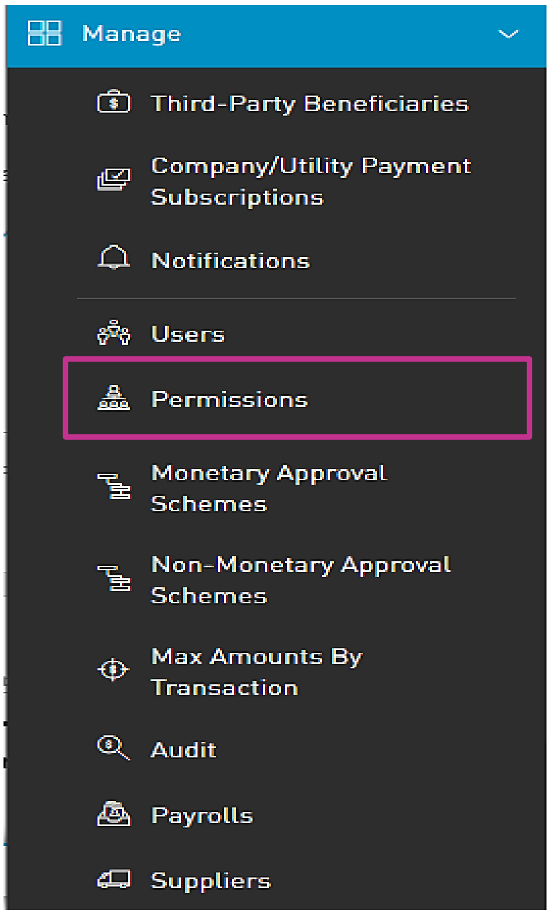
The *Permissions List* is a critical tool for the Site Administrator as it will serve as a guide in creating and amending all Corporate user profiles.

Refer to Appendices B, C and D to view the complete lists of all Corporate User Permissions

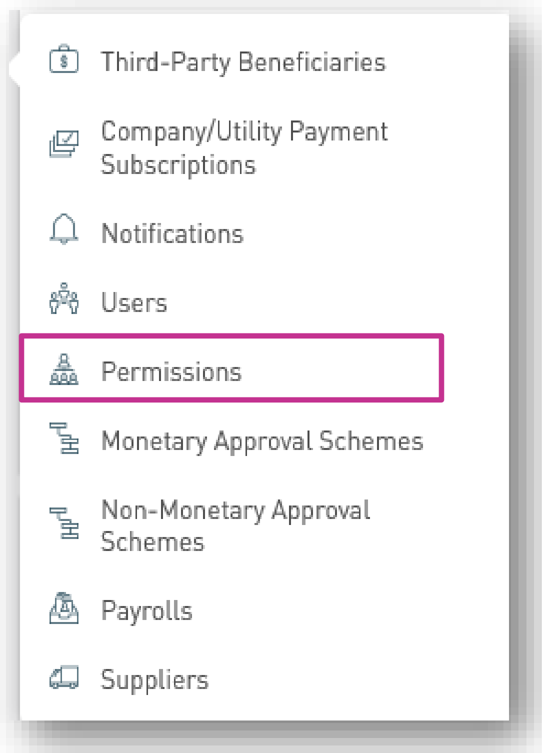
Permissions Administration

The Permissions Page contains a master list of all the Business Site's users' permissions.

To access this page select the **Permissions** option under the the **Manage** section of either menu.



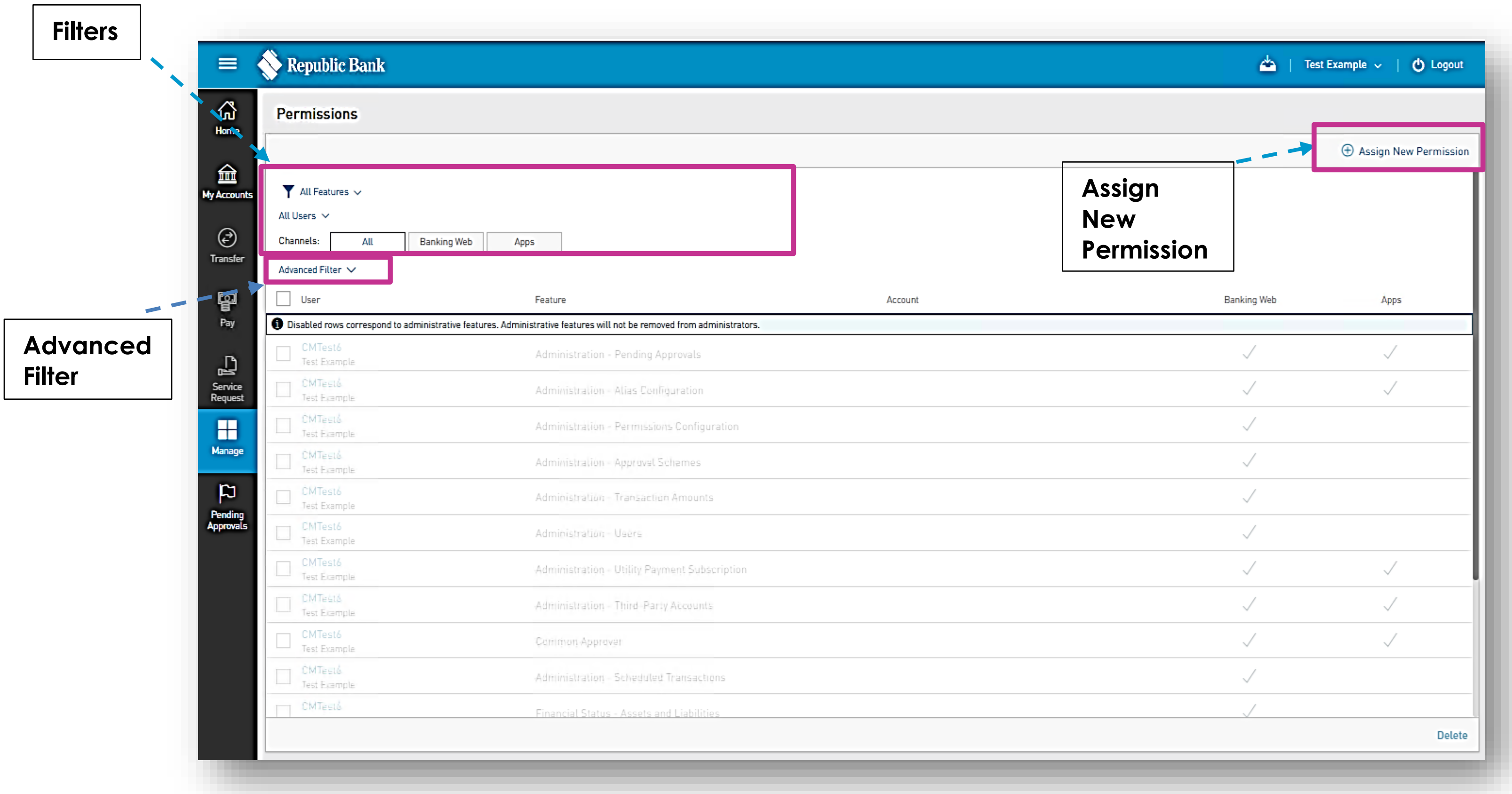
OR



This action will redirect the user to the Permissions Page.

Only the users assigned the relevant permissions will be able to access to the Permissions Configuration. (Refer to Appendix for list of Permissions)

Permissions Page

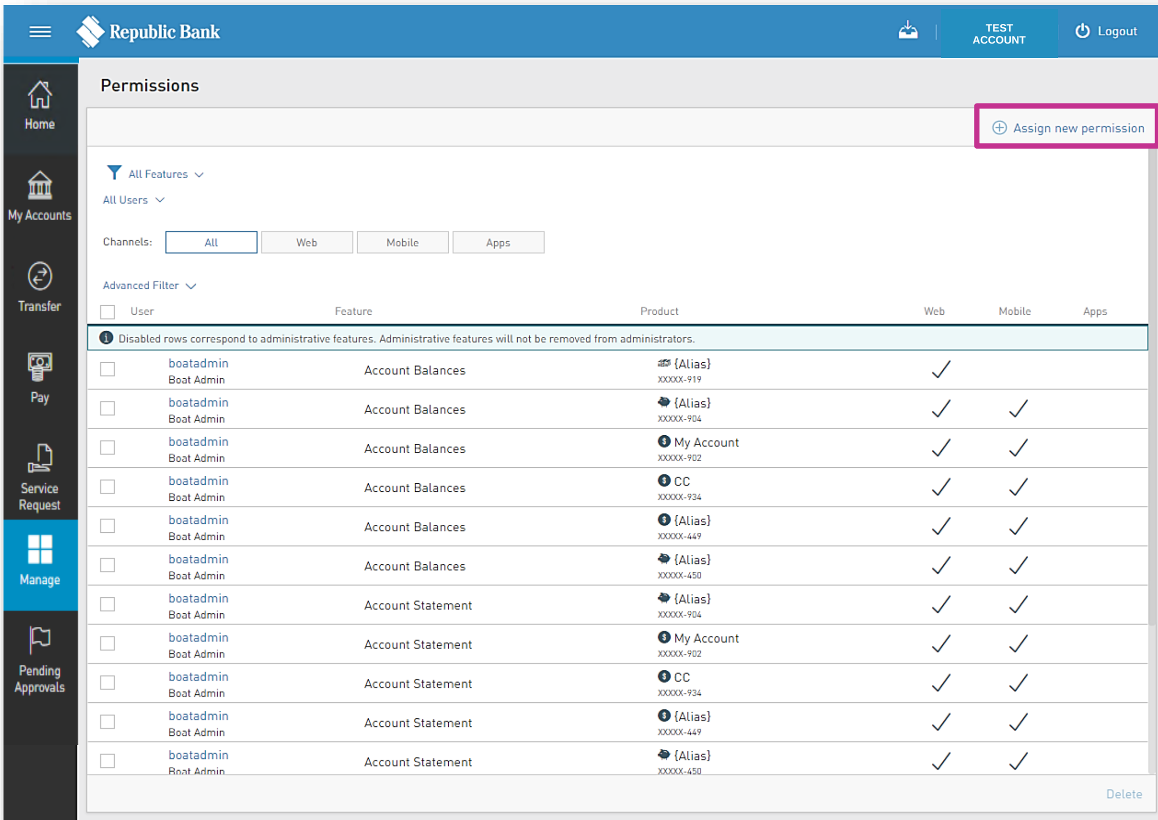


The Permissions Page displays the list with all the Site's permissions and their assigned users. The list contains the following details:

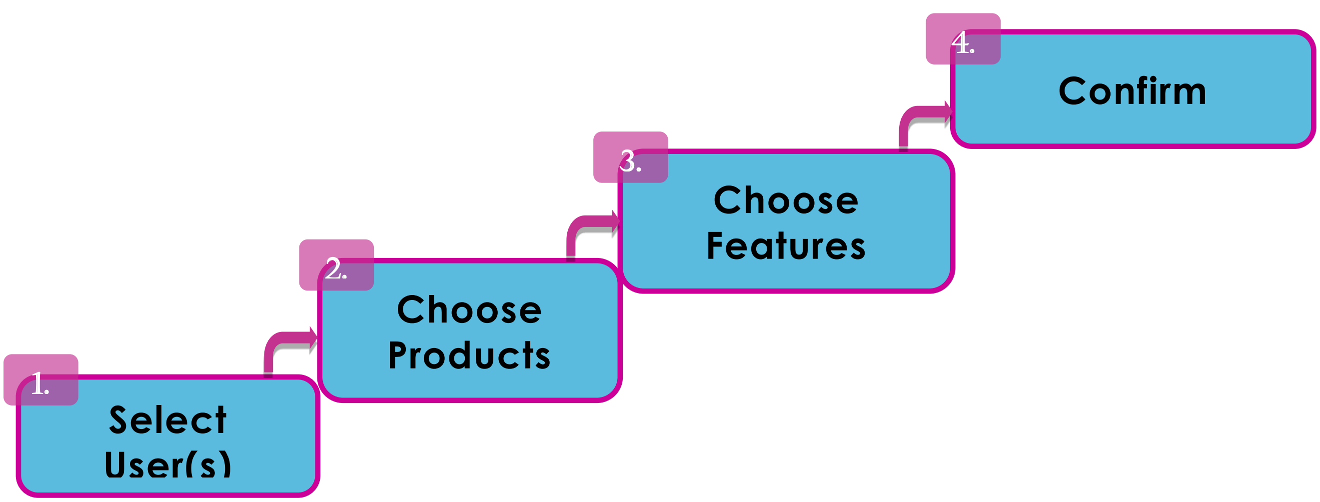
- User (username, and full name)
- Permission
- Product (where applicable)

How to assign permissions?

To assign permissions, go the the Permissions Page and click on the ⊕ Assign New Permission link:



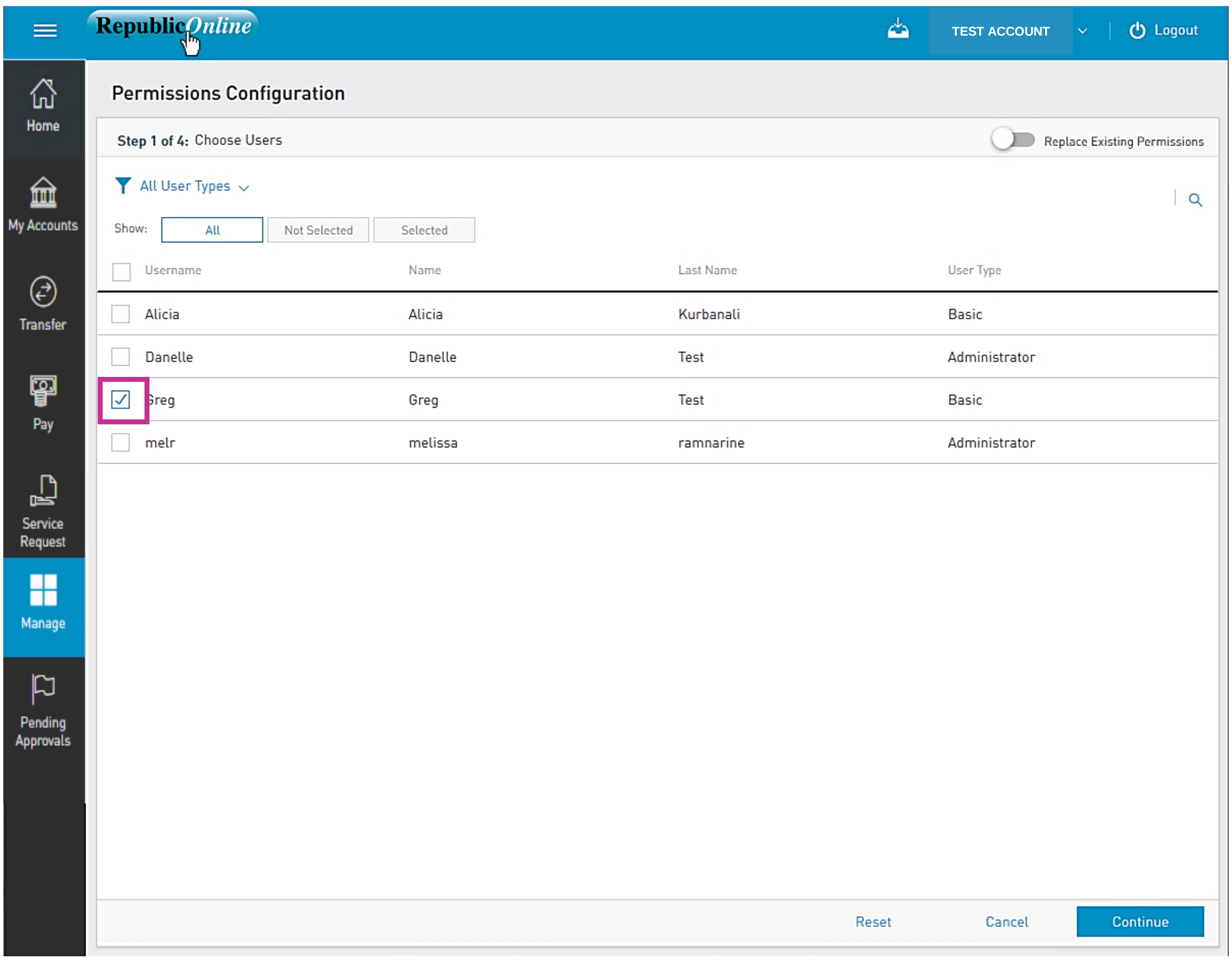
The process entails 4 steps as follows:

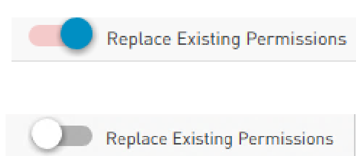


Step 1: Choose User

The master list of all the Site users will be displayed here. Select the radio button next to the name of the user you wish to assign permissions to.

Multiple users may be selected in this step, if they all require the same permissions.

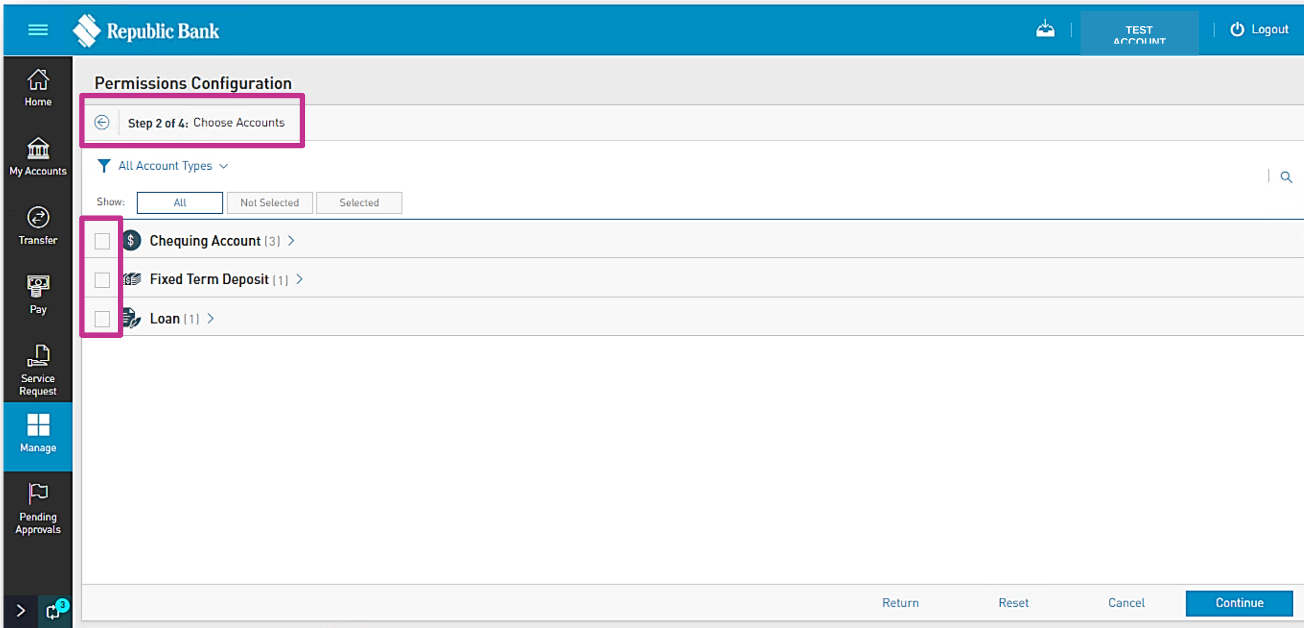




- **Enable toggle if the user's current permissions are to be removed/replaced.**
- **Leave toggle off if the user needs to retain their existing permissions.**

Step 2: Choose Accounts

This screen displays a master list of all available accounts for which permissions may be assigned. Here the products are categorised by type and may be filtered if required.



Expand the category to select the relevant product.

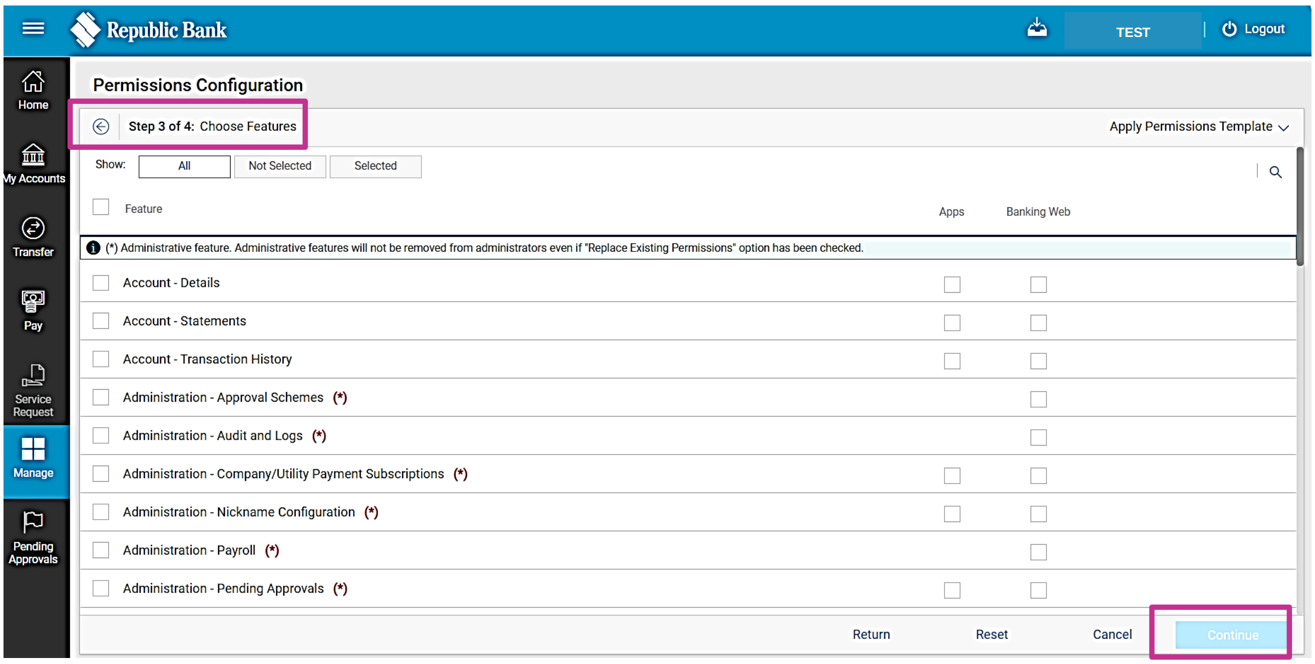
This step may be skipped if the user does not require permissions related to particular products (i.e. if the user is being assigned Administrative or General permissions.

Step 3: Choose Features

Features refer the relevant rights or access that the user may be granted.

This screen displays a master list of all available features that may be assigned. If a product was selected in the previous step, the list will contain all available features related to the selected product.

If no product was selected, then only administrative Features available on this Site will be listed (as shown below).

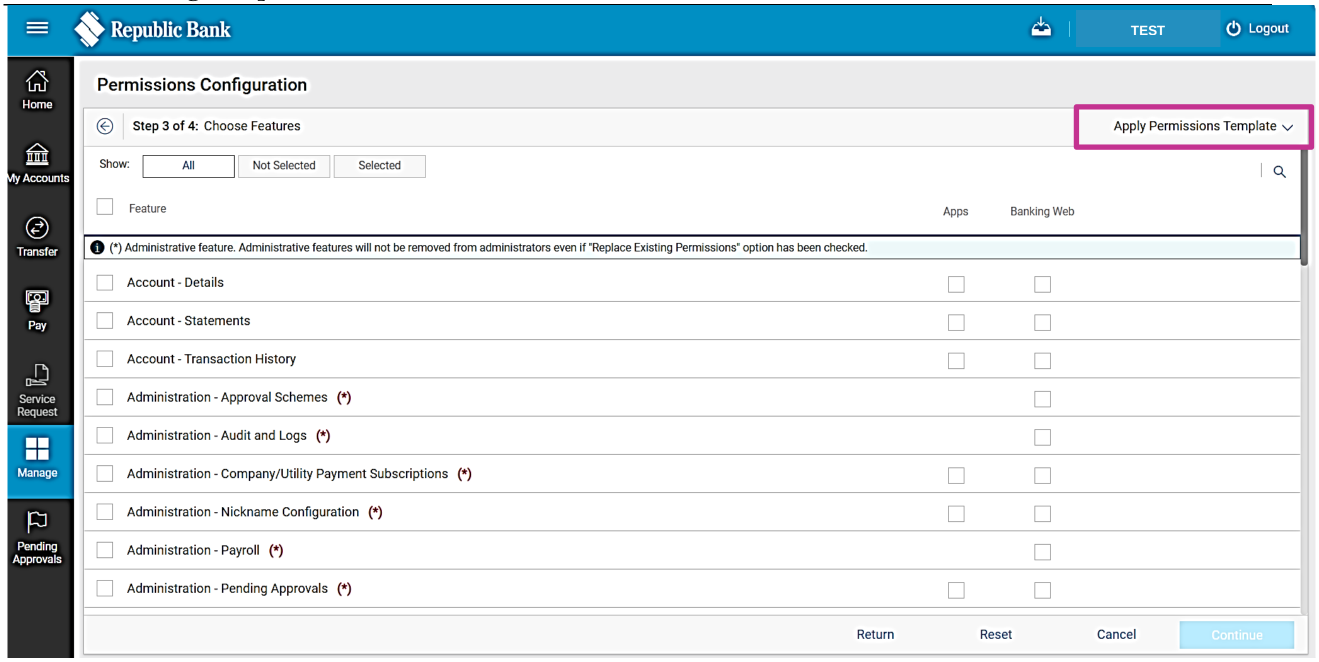


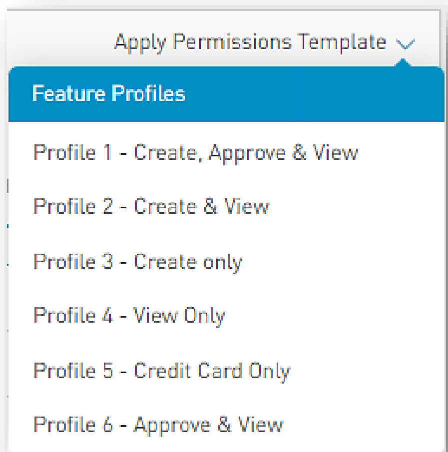
(*) Denotes the administrative features.

- Select required feature and channel by clicking on the relevant radio button(s) and select Continue to proceeed to step 4.

OR

To make it easier, we have created Permission templates:



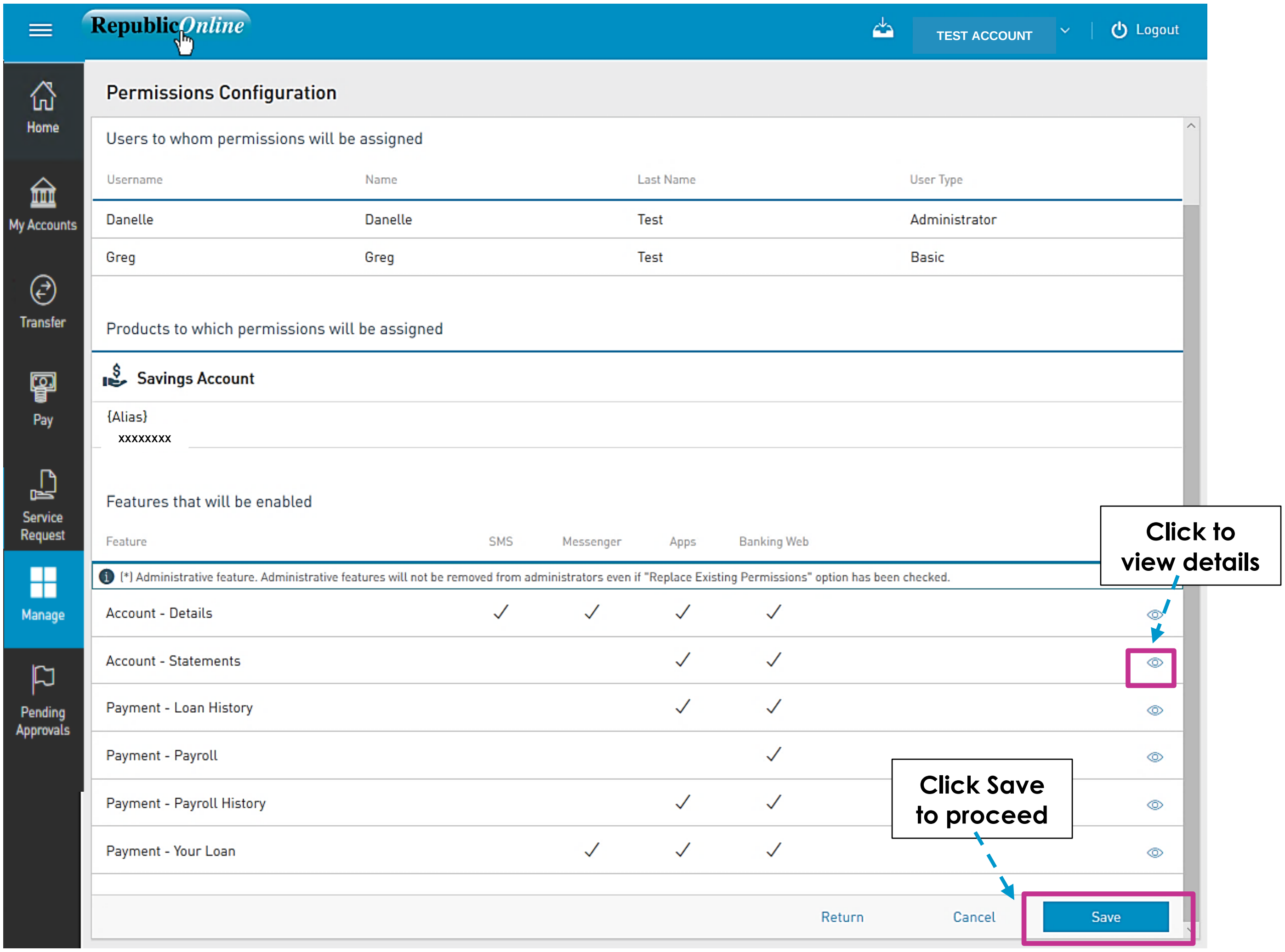


There are six (6) profiles which are associated with the main functions of internet banking users. Once a template is selected, the corresponding features will be selected from the list below.

- Select the required Permissions Template (or Profile) from the list provided the and select **Continue** to proceeed to step 4.

Permissions may also be restricted by channels whereby a user may be granted permissions on one channel only. E.g. Permissions to approve transactions on Web only. Please see Appendix E for description of Permission Templates.

Step 4: Confirm



This step allows the user to review/validate the information entered in the previous step, before submitting the changes.

Once the information has been verified select **Save** to proceed.

To go back to the previous step to edit transaction select **Return**

To cancel transaction request select **Cancel**

Approval Schemes

Approval Schemes (Overview)

Approval schemes outline which users have the authorisation to approve transactions on a Business Site. Schemes comprise the scope, as well as the users assigned to the scope and their authorisation privileges.

Approval Schemes are categorised as follows:

1. **Non-Monetary Schemes**

These schemes comprise: (1) A function or permission
(2) The Users authorised to approve the process
(3) The Approval Percentages.

2. **Monetary Schemes**

These schemes comprise: (1) A function or permission
(2) The Users authorised to approve the process
(3) The Approval Percentages.
(4) Transaction Limits

Key Elements of Approval Schemes

- Scope (Permissions + Users)
- Approval Percentages
- Approval Limits (Monetary Approval Schemes only)

Scope (Feature and Account)

Republic*Online* has an established list of permissions, that govern every potential action or transaction on the system. The Company's Administrator is responsible for creating the users and assigning them the relevant permissions. In the same way, users who are tasked with the responsibility of approving processes or transactions, must also be granted the permission to approve.

Users who are required to approve must be granted the following permissions

- ***Common Approver*: this permission enables the approval rights**
- ***Administration-Pending Approvals*: this permission**

Approval Percentages

All approval schemes contain approval percentages. These define the percentage of approval that the assigned users have access to approve, for the particular functionality or transaction.

Example:

Edit User Profile: User A – 50%

User B – 50%

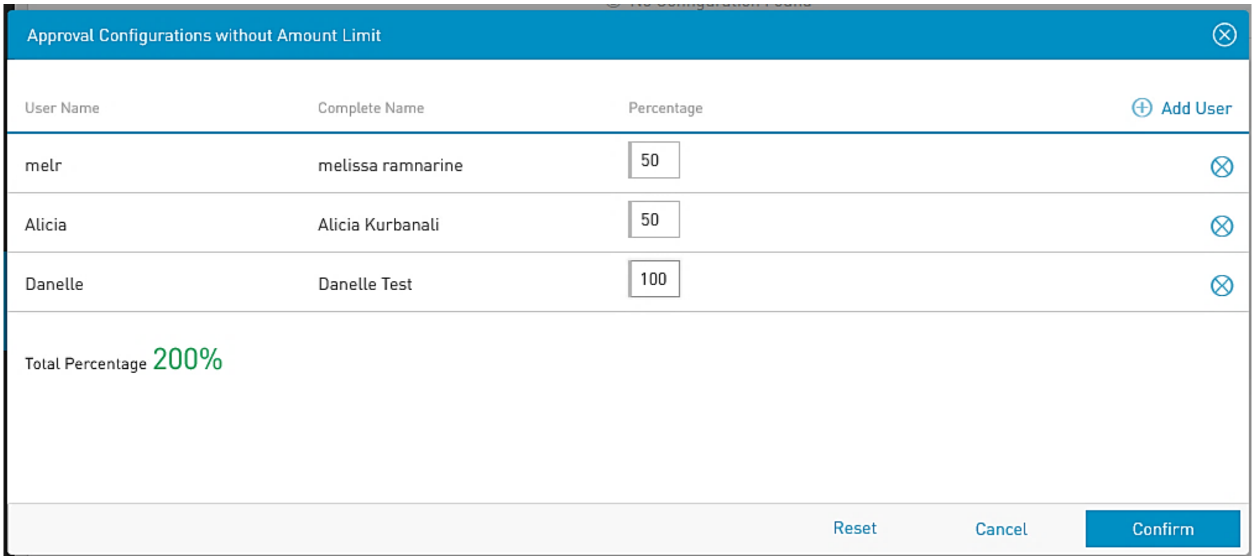
User C – 100%

In this scenario, the process can be approved by either *User* **A**, **B** or **C**. *User* **C** has 100% approval and can therefore approve alone. However, *Users* ***A*** and ***B*** are assigned 50% approval. This means that if *User* ***A*** approves the transaction, it will only be 50% approved. In this case, the request will remain "Pending Approval" until *User* **B** or **C** approves it.

All transactions require 100% approval. In this example, *Users* **A** and **B** may approve together or, they may each approve with *User* **C**. The requirement is for a minimum of 100% but, the system does <u>not</u> prevent users if their combined approval percentage exceeds 100%.

All approval schemes must reach 100% for the scheme to be complete.

Example:



Approval Limits

When creating Monetary Approval Schemes, the Administrator has two options;

- He/she may create the scheme "Without Amount Limit", whereby all users assigned to the scheme may authorise transactions up to any amount

OR

- The scheme may be created where the assigned approvers may only approve up to a pre-set limit

Example 1:

Scheme X: Transfer of funds from Corporate Account 1

Limit: $50,000

User A – 50% User B – 50% User C – 100%

In this example, the users have authority to approve the transfer of funds from Account 1 up to $50,000. If the transfer exceeds this limit, these three users would not be able to approve it.

One user may be assigned to multiple schemes with varying configurations and limits.

Example 2:

Scheme Y: Transfer of funds from Corporate Account 2

Limit: -

User A – 50% User B – 50% User C – 100%

In this case, we see that the same users have the authority to approve the transfer of funds from Account 2 up to any amount, as a limit was not defined in this scenario.

One account may be assigned to multiple schemes with varying configurations and limits.

Example 3:

Scheme Z: Transfer of funds from Corporate Account 1

Limit: -

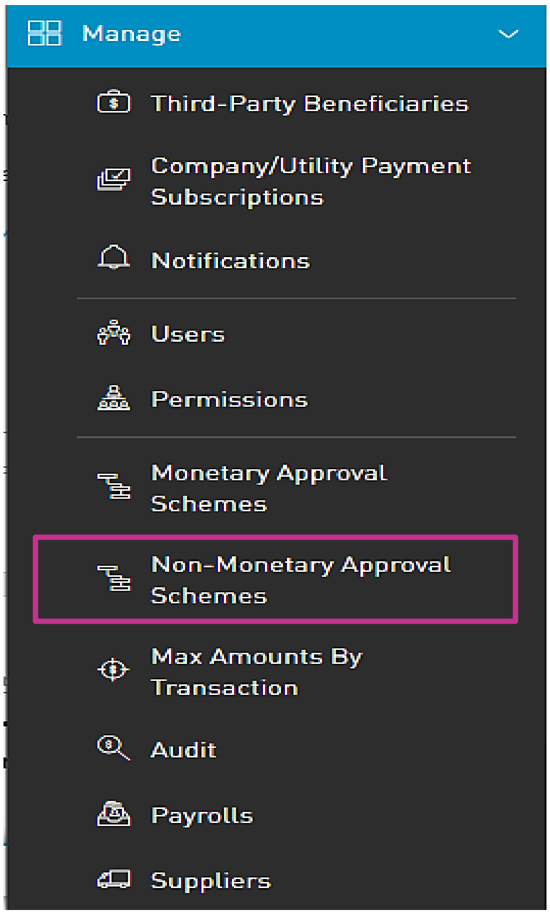
User A – 25% User B – 25% User C – 50% User D – 100%

This scenario is an example of how the same users may belong to multiple schemes involving the same account. In example 1, Users **A** and **B** could authorise up to 50% of transfers from Account 1, up to $50,000. In Scheme 3, no limit was set. Therefore, if there are any fund transfers form Corporate Account 1 exceeding $50,000, the same users may authorise, but their approval percentages in this case, are different.

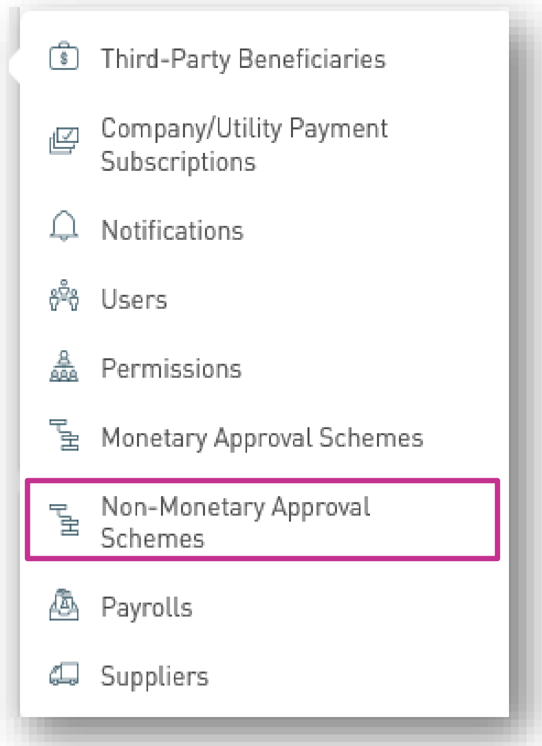
	Scheme X	***Scheme Z***
User A	50% approval up to $50,000	25% approval; unlimited
User B	50% approval up to $50,000	25% approval; unlimited
User C	100% approval up to $50,000	50% approval; unlimited

How to create a Non-Monetary Approval Scheme?

To access this page select the **Non-Monetary Approval Schemes** option under the **Manage** section of either menu.



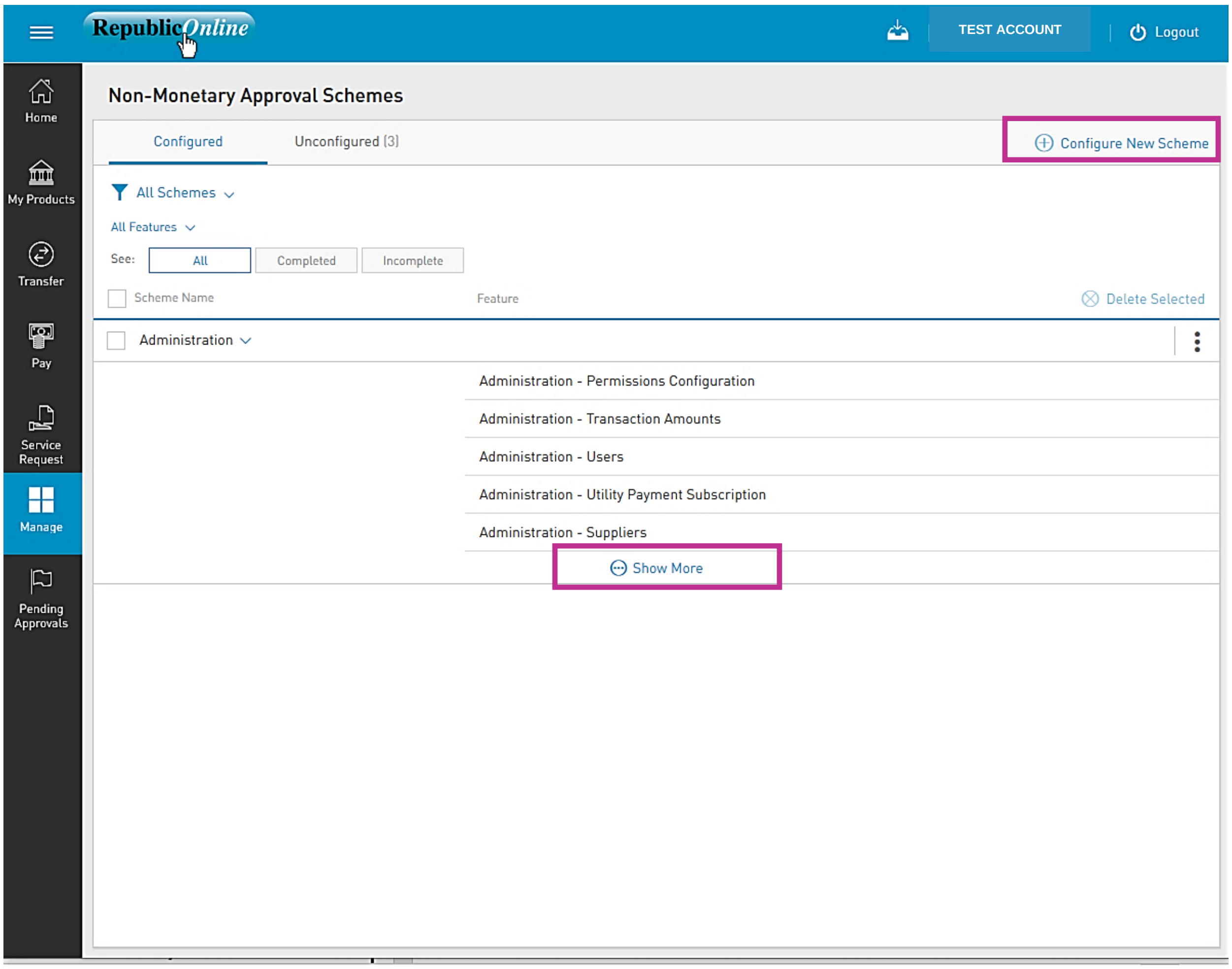
OR



Only the users assigned the relevant permissions will be able to access the Non-Monetary Approval Schemes feature. (Refer to Appendix for list of Permissions)

The Non- Monetary Approval Schemes Page.

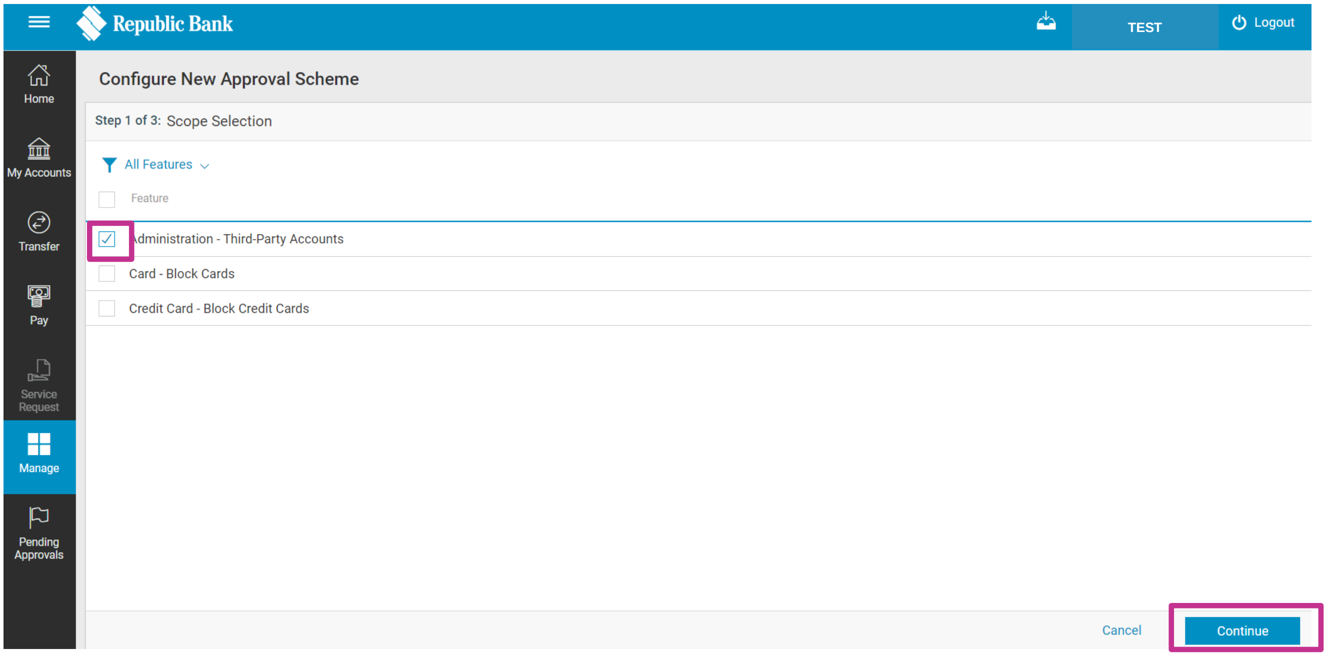
This page displays all existing Non-Monetary Approval Schemes.



Select the 

link to create a new approval scheme.

Step 1: Select Feature (Scope of Approval Scheme)

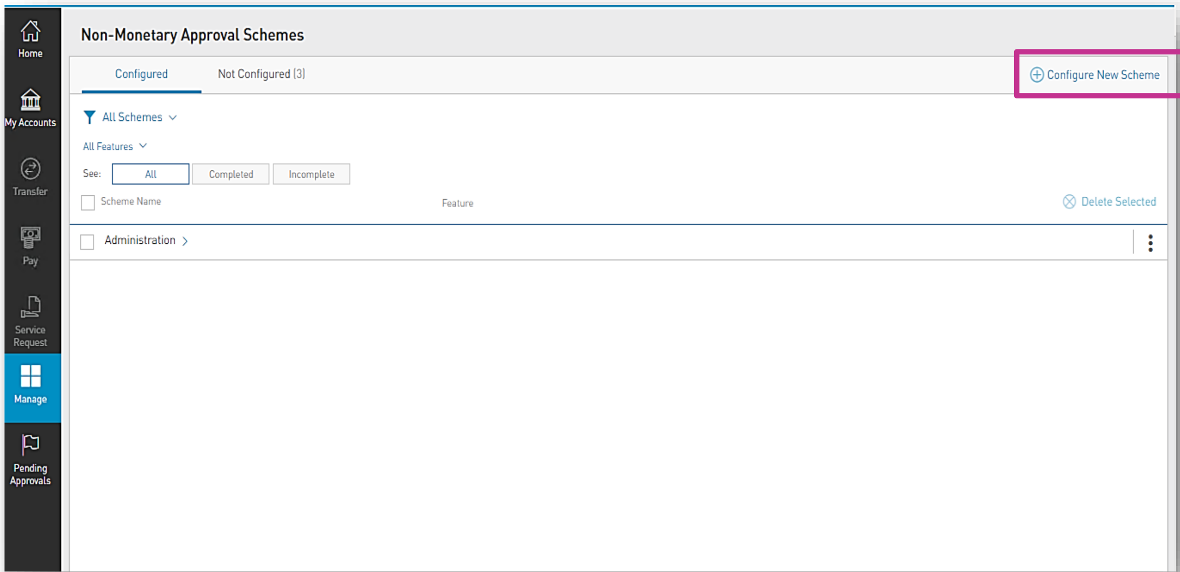


Select the required feature by ticking the radio button.

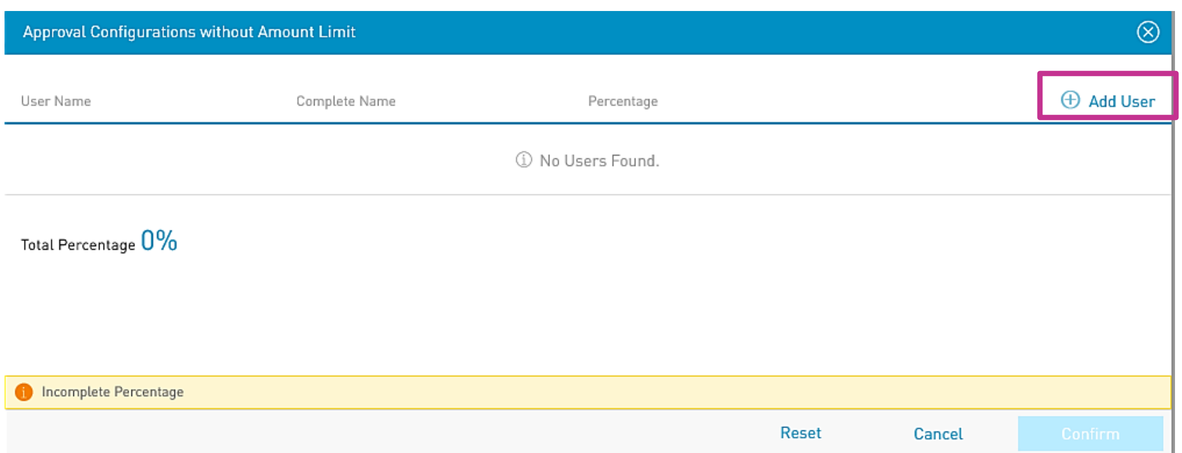
Select Continue to proceed or Cancel to cancel the request if required.

Step 2: Configure New Approval Scheme

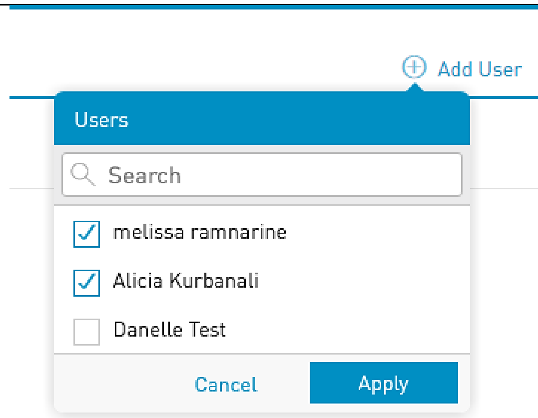
- Click on the Configure New Scheme link to configure the Approval Scheme.



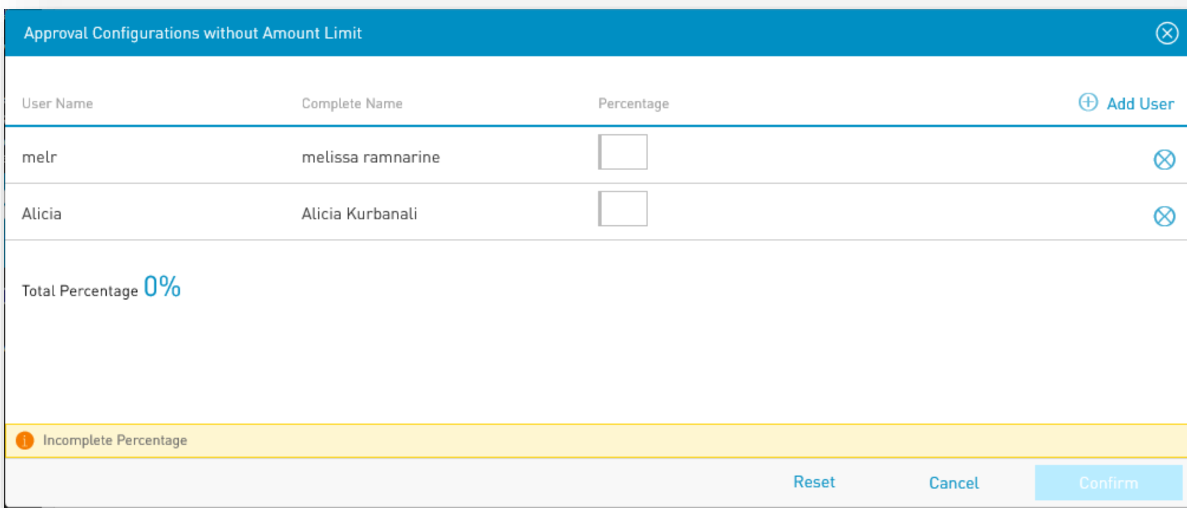
- Click on the Add User link to add users to the scheme.



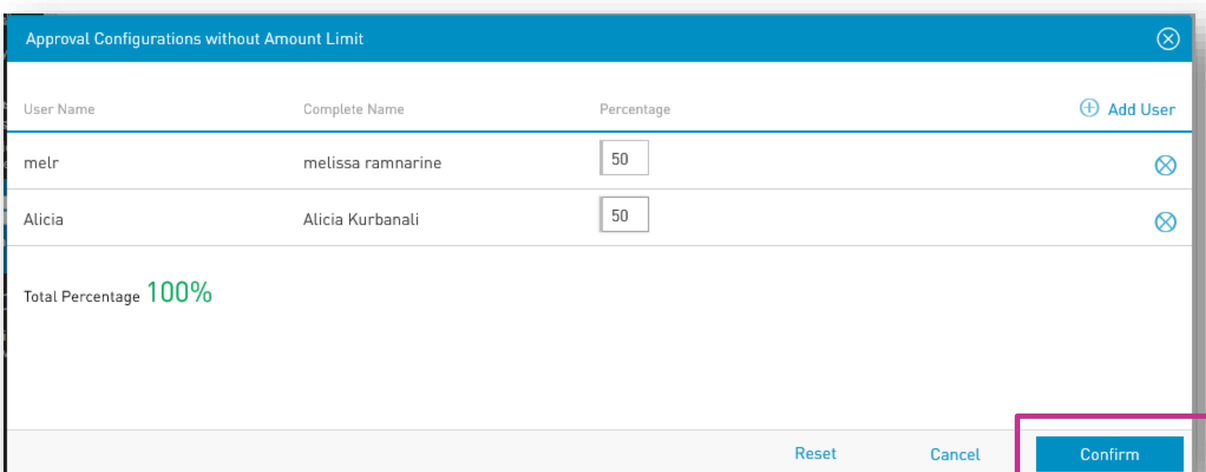
- Select the users to be added by clicking on the radio buttons.



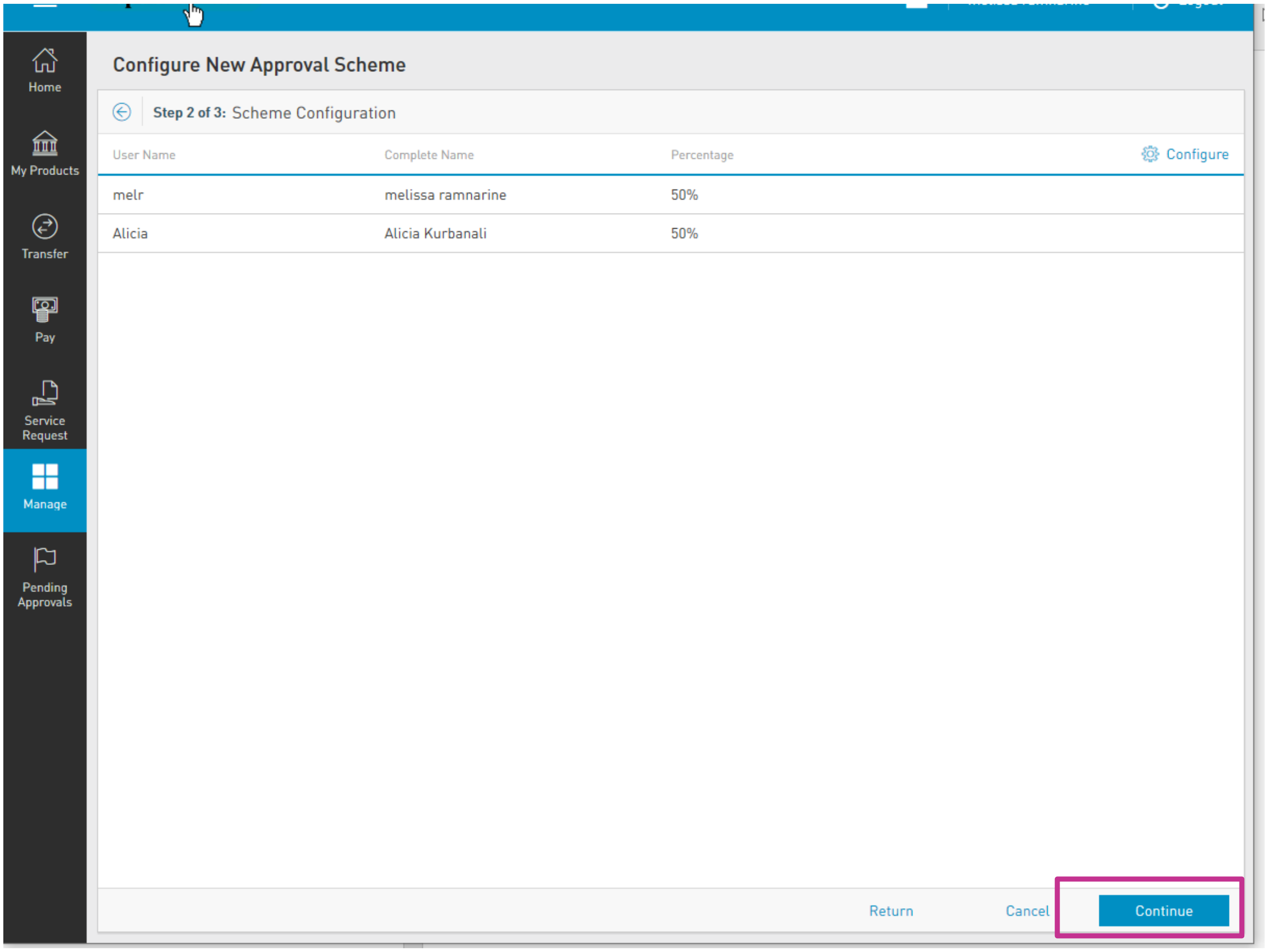
- Input the approval percentages required.



- Click on **Confirm** to proceed.



This completes the configuration process of the non-monetary approval scheme. The user will be redirected to the Scheme Configuration screen.

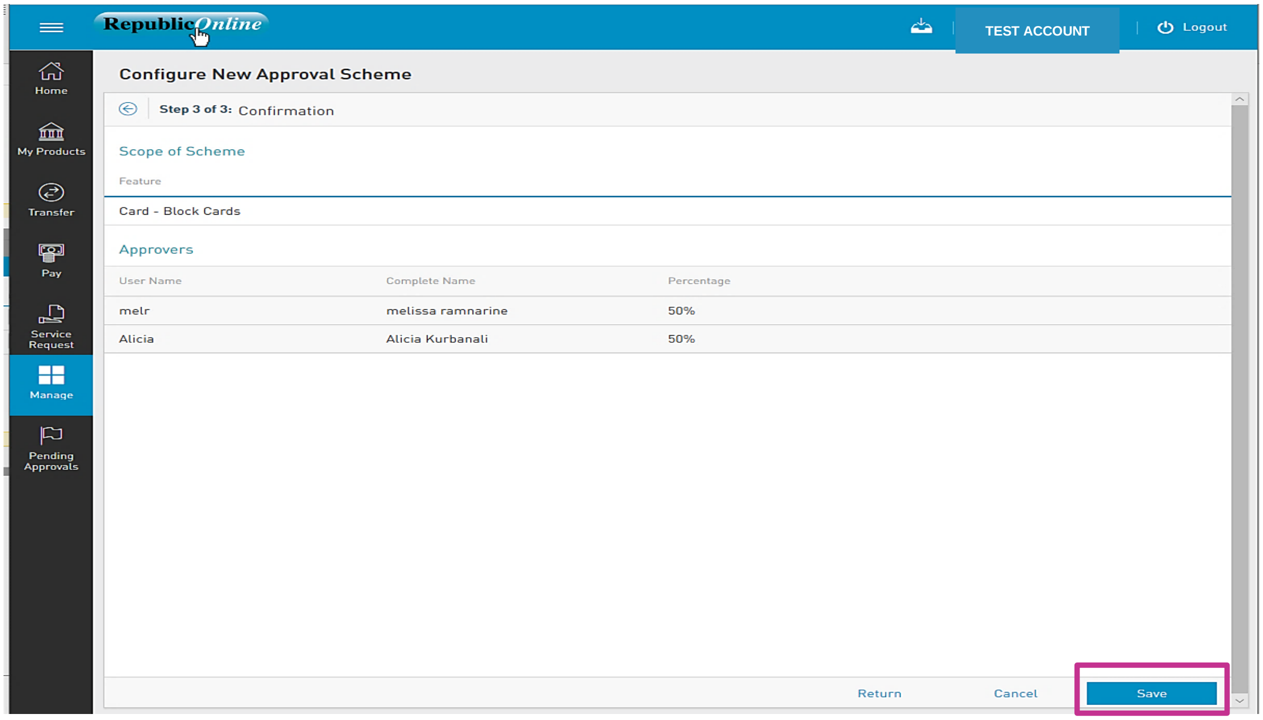


The available actions are:

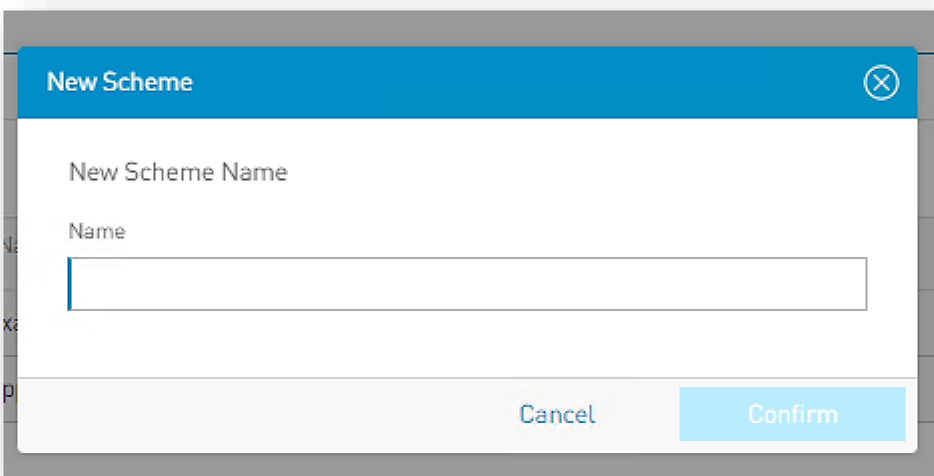
- **Continue: to confirm the date and proceed to the next step.**
- **Cancel: to cancel application.**
- **or Return: to return to the previous step**

Step 3: Confirm New Approval Scheme

- Click **Save** to proceed.

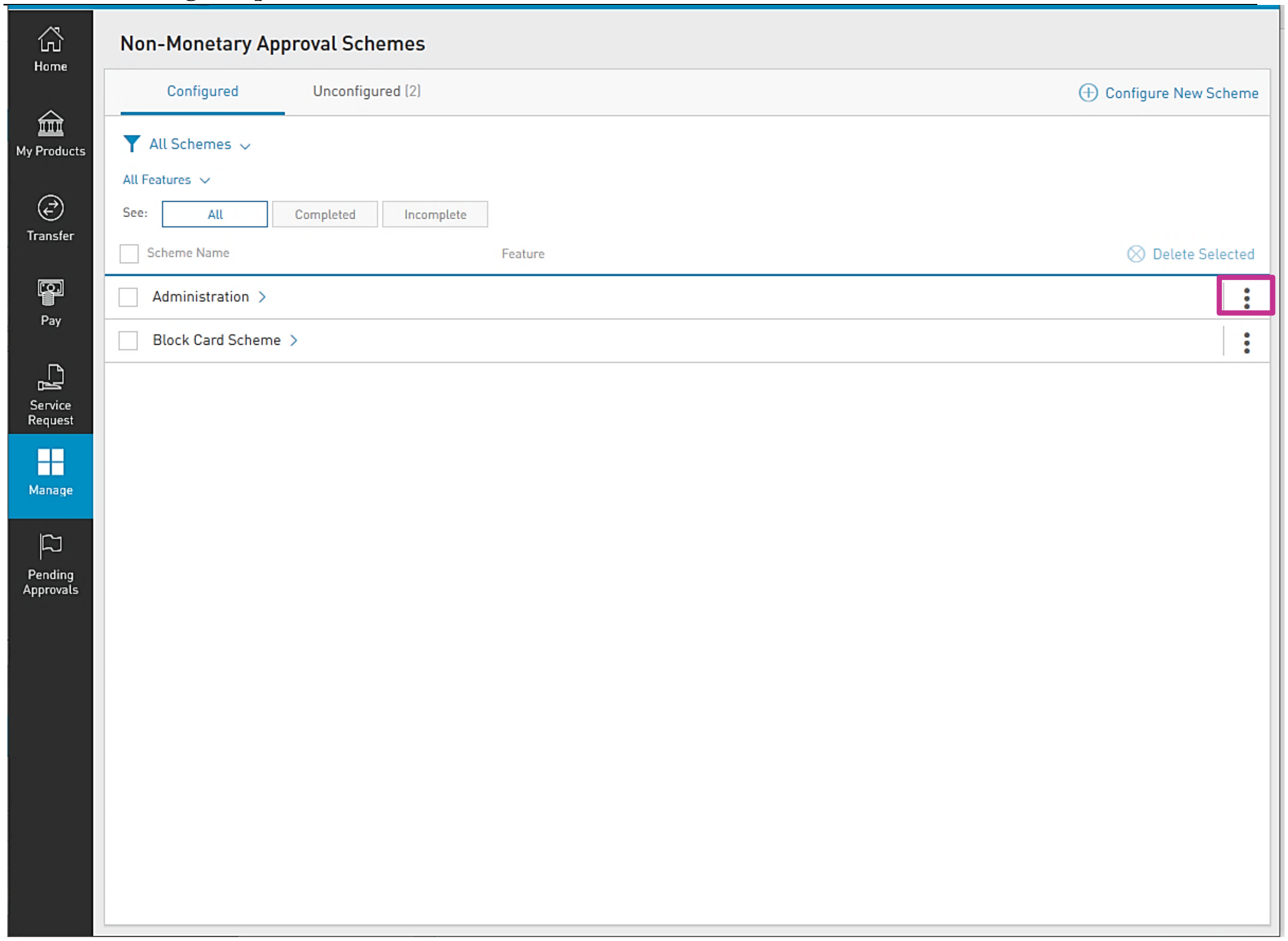


- Enter a name for the new scheme in the space provided.

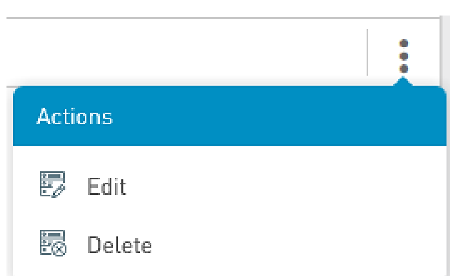


This step completes the process for creating a New Non-Monetary Approval Scheme.

Once the scheme is saved the user will be redirected to the Non-Monetary Approval Schemes page where the new scheme will be listed.

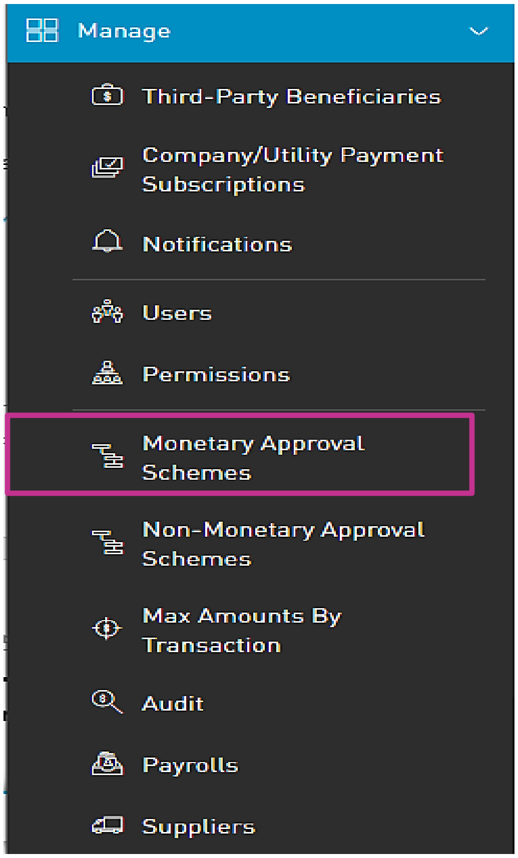


From the page the user may also edit and delete selected approval schemes via the contextual menu of the relevelant scheme.

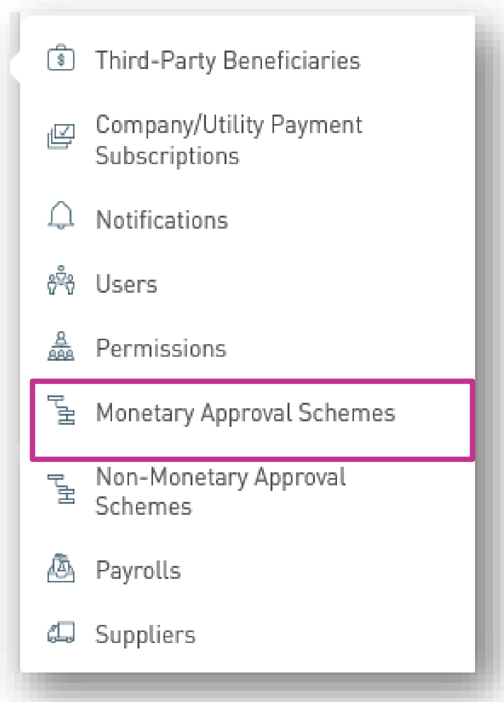


How to create a Monetary Approval Scheme?

To access this page select the **Monetary Approval Schemes** option under the **Manage** section of either menu.



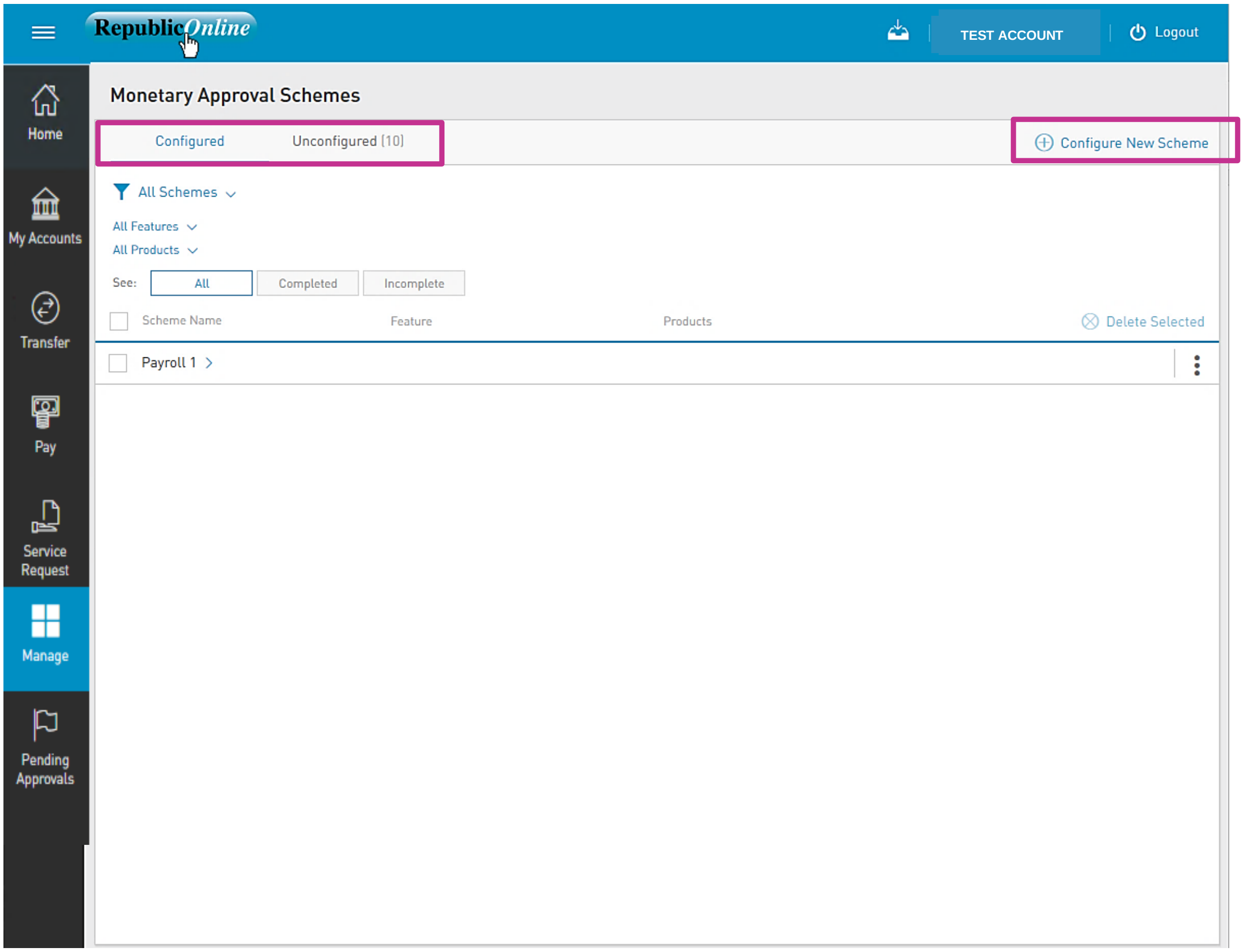
OR



Only the users assigned the relevant permissions will be able to access to the Non-Monetary Approval Schemes feature. (Refer to Appendix for full list of Permissions)

The Monetary Approval Schemes Page

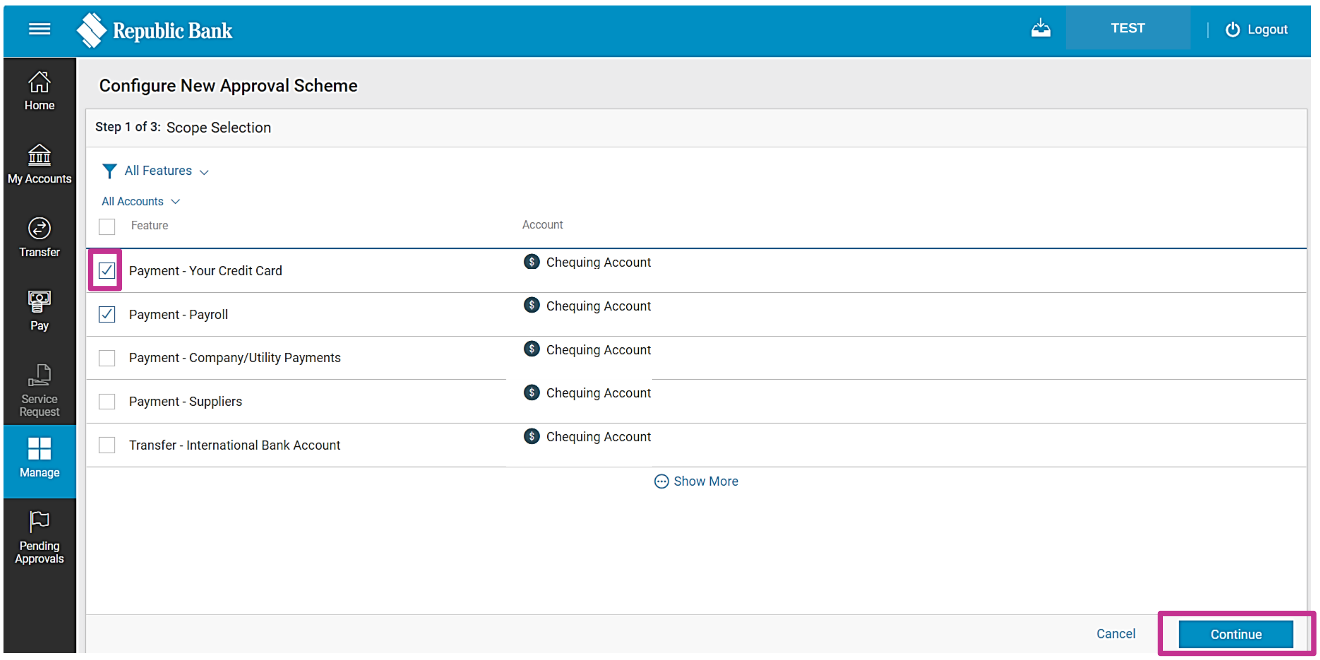
This page displays all existing Monetary Approval Schemes.



Pay attention to the Configured and Unconfigured details shown at the top of the page, as all Schemes must be configured (i.e. Approvers must be established) for users to perform those transactions.

Step 1: Select Scope

Feature + Product = Scope



Select the required feature by ticking the radio button.

Select Continue to proceed or Cancel to cancel the request if required.

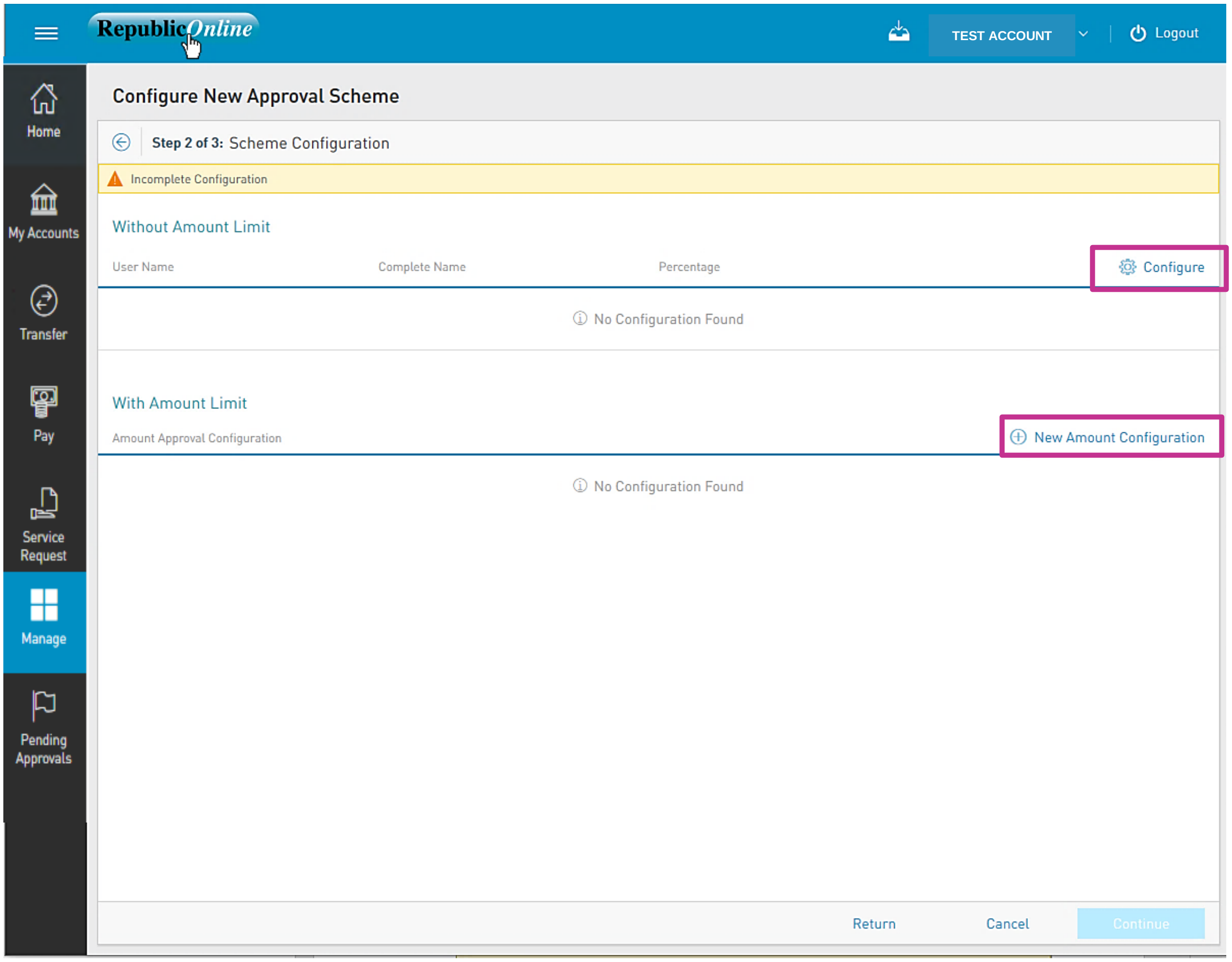
The product attached to the scope will serve as the debit account in the scheme.

Step 2: Configure New Approval Scheme

Here there are two options:

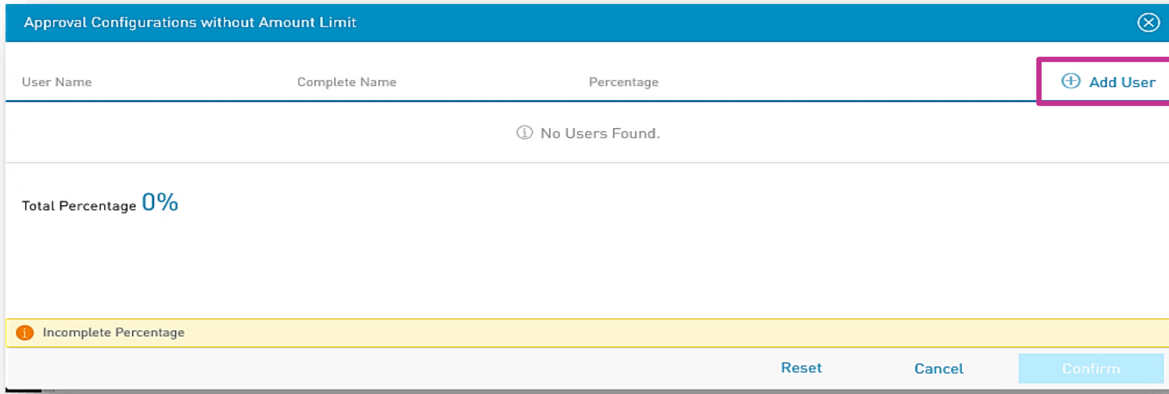
- Click on the Configure link to configure a new approval scheme without an amount limit.

- Click on the New Amount Configuration link to configure a new scheme with an amount limit.

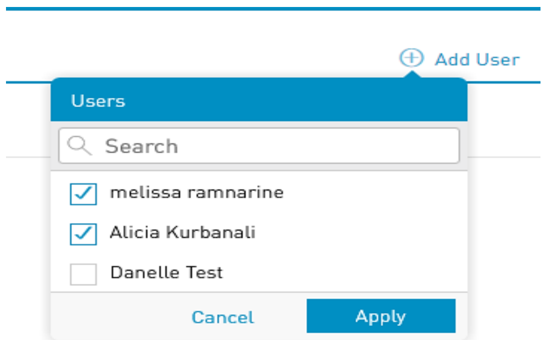


Without Amount Limit

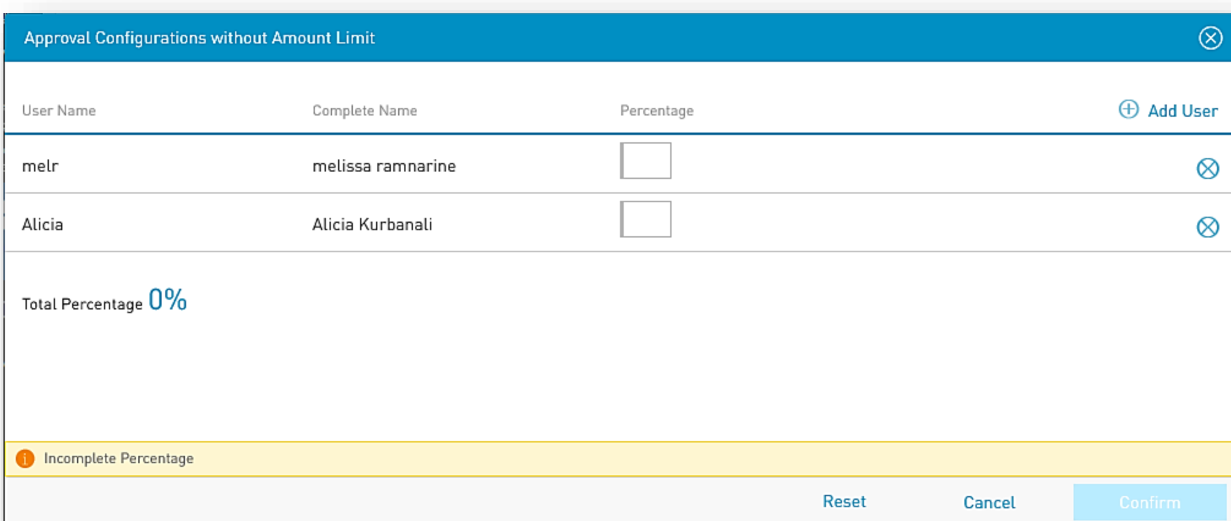
- Click on the Add User link to add users to the scheme.



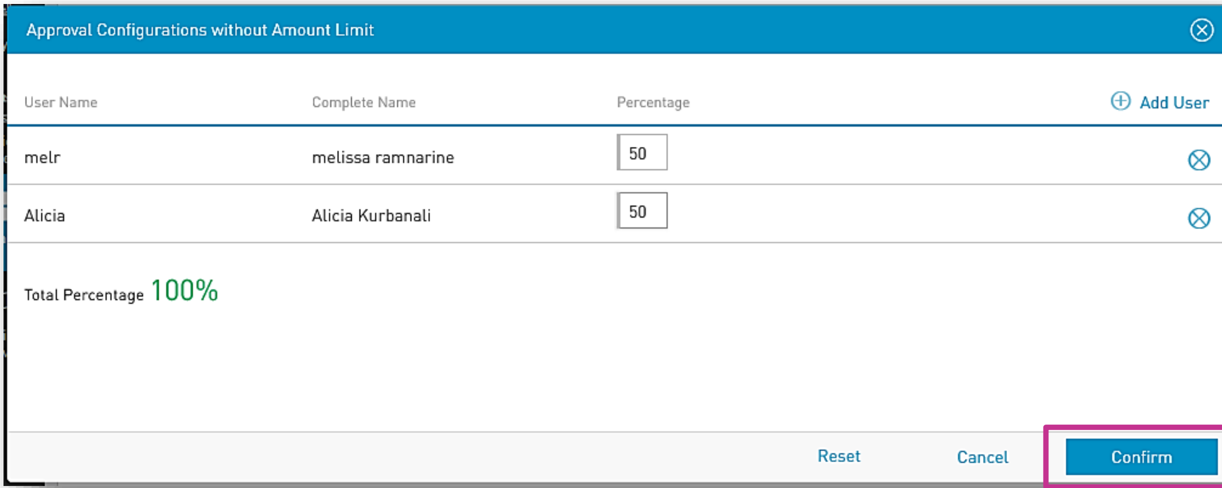
- Select the users to be added by clicking on the radio buttons.



- Input the approval percentages required.



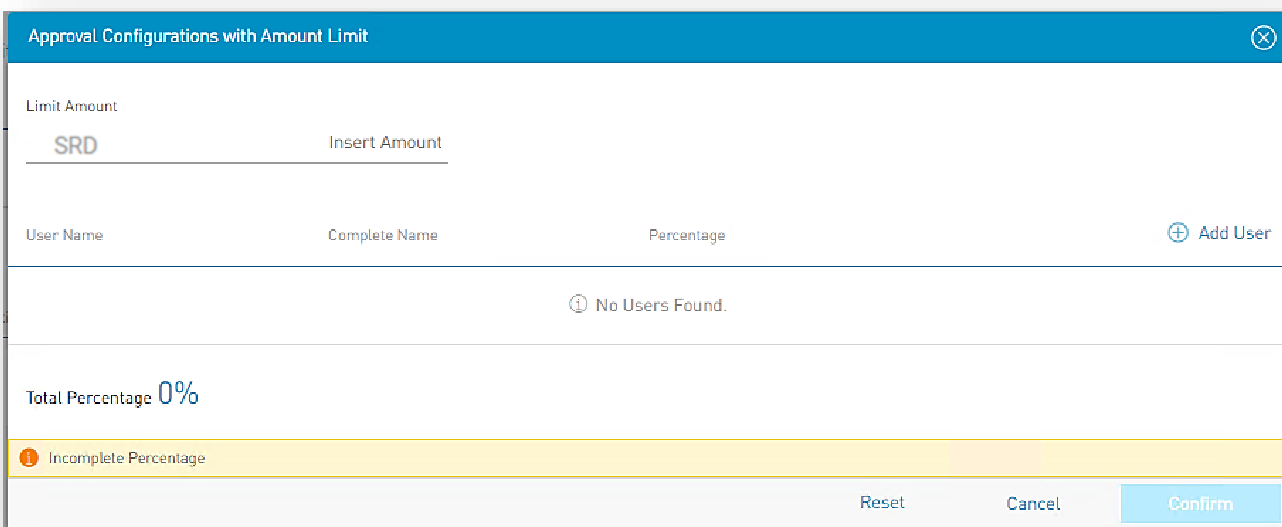
- Click on **Confirm** to proceed.



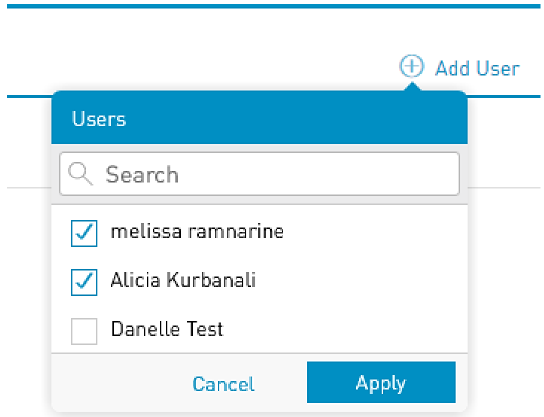
This completes the configuration process of the monetary approval scheme with no amount limit. The user will be redirected to the Scheme Configuration screen.

With Amount Limit

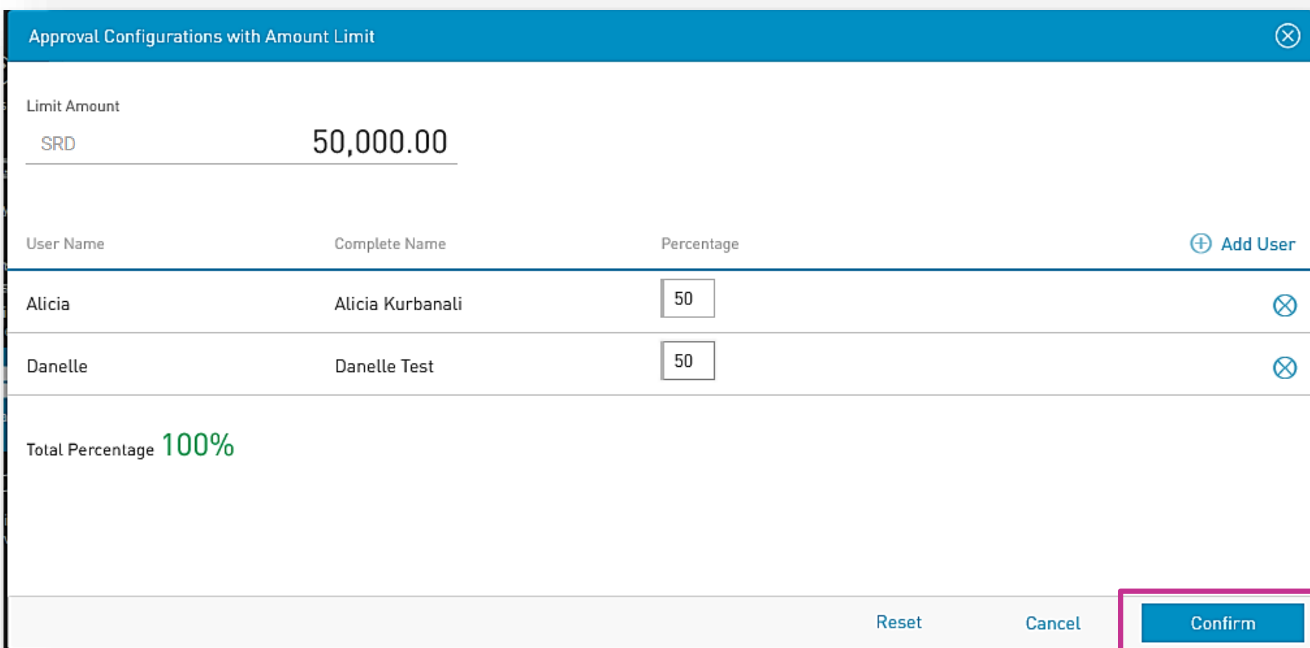
- Insert Amount Limit in the space provided.
- Click on the ⊕ Add User link to add users to the scheme.



Select the users to be added by clicking on the radio buttons.

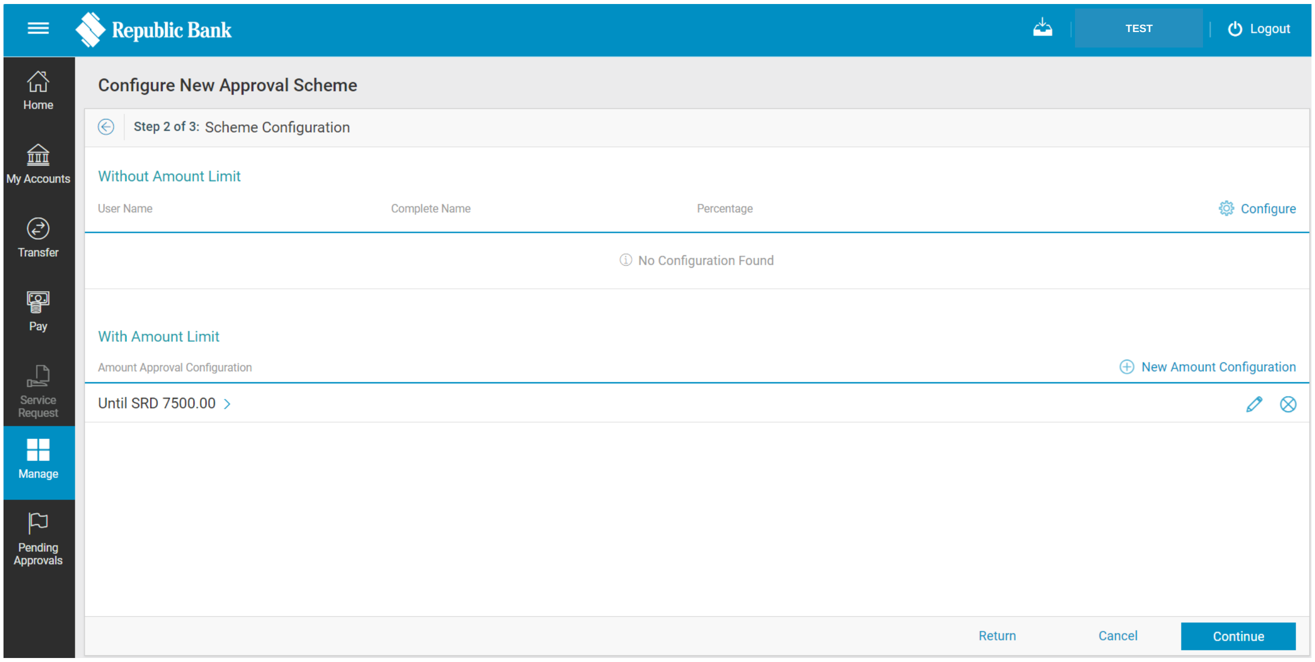


- Input the approval percentages required.



- Click on **Confirm** to proceed.

This completes the configuration process of the monetary approval scheme with an amount limit. The user will be redirected to the Scheme Configuration screen.

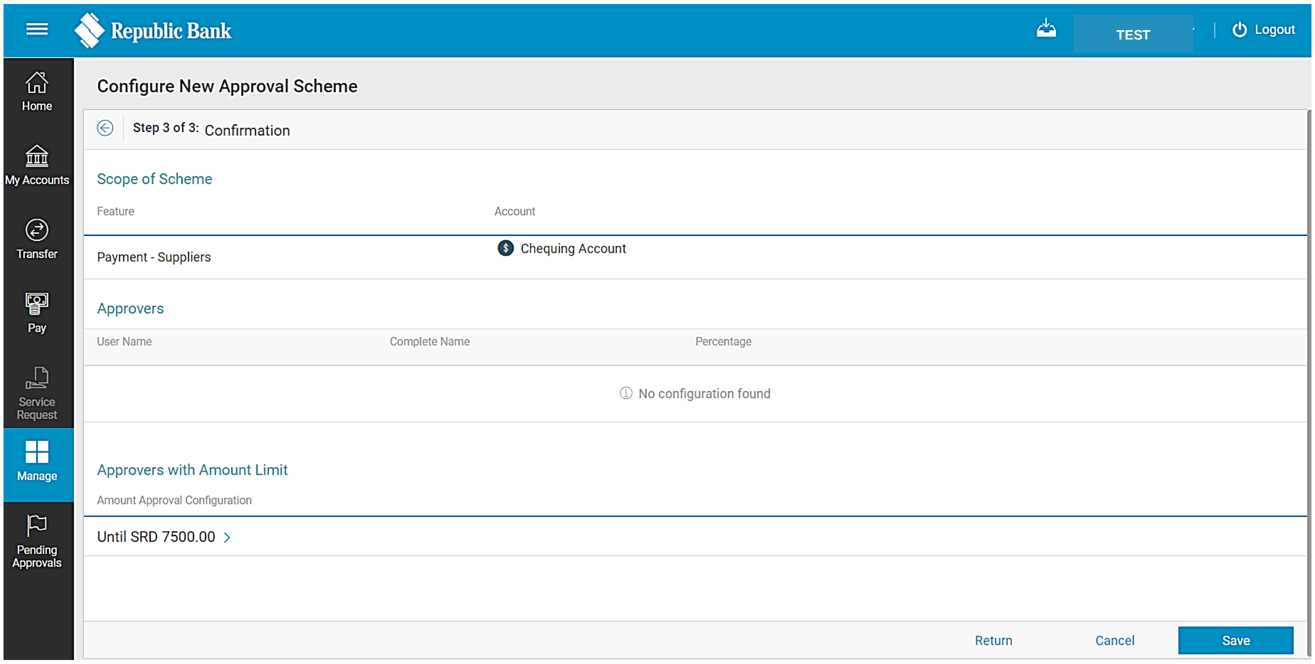


The available actions are:

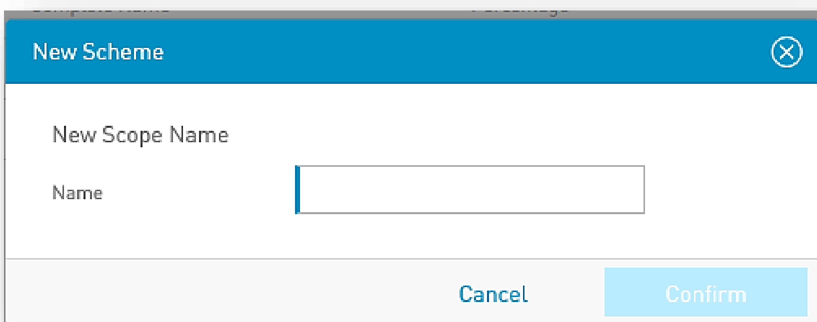
1. **Continue : to confirm the date and proceed to the next step.**
2. **Cancel : to cancel application.**
3. **or Return : to return to the previous step**

Step 3: Confirm New Approval Scheme

- Click **Save** to proceed.

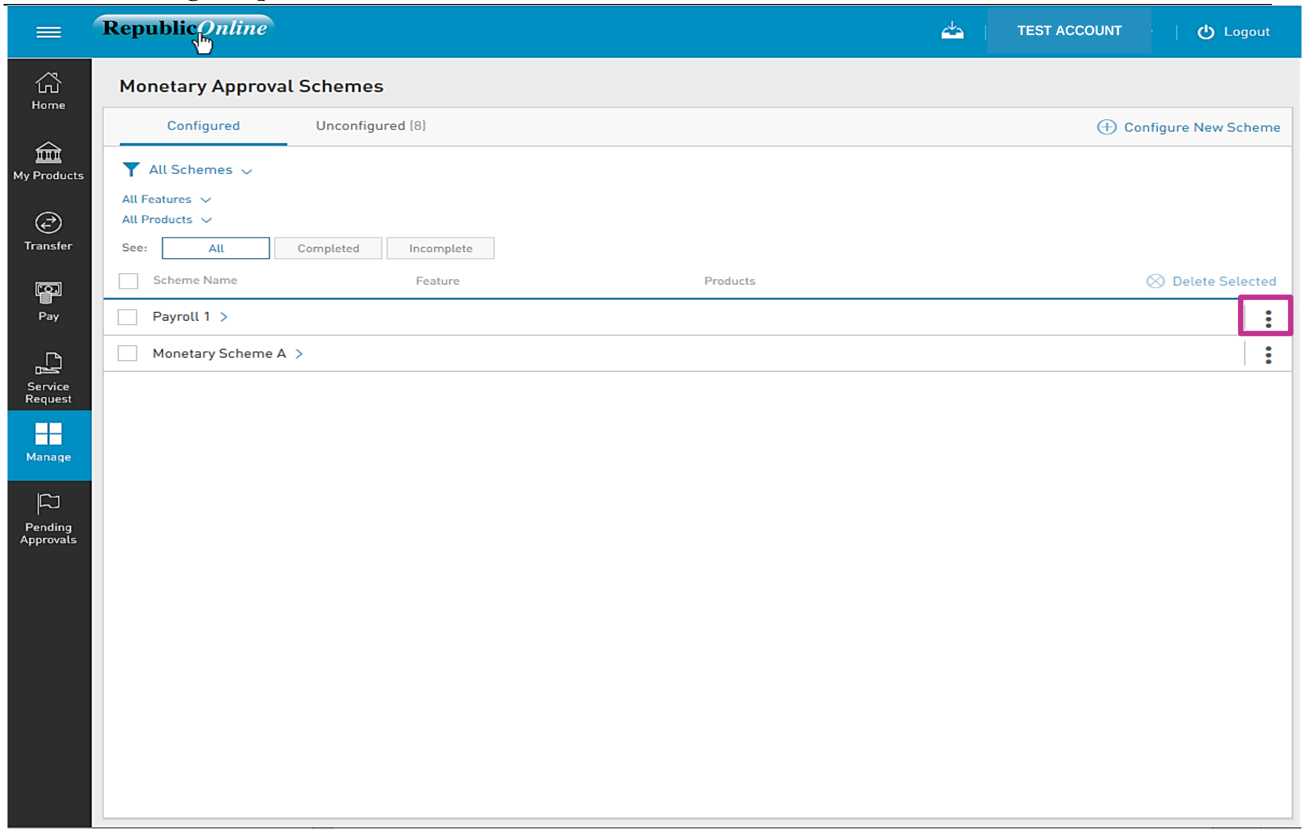


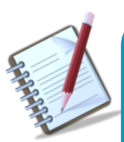
- Enter a name for the new scheme in the space provided.



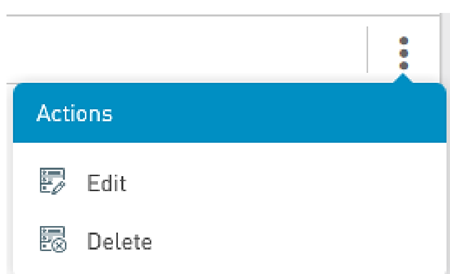
This step completes the process for creating a New Monetary Approval Scheme.

Once the scheme is saved the user will be redirected to the Monetary Approval Schemes page where the new scheme will be listed.



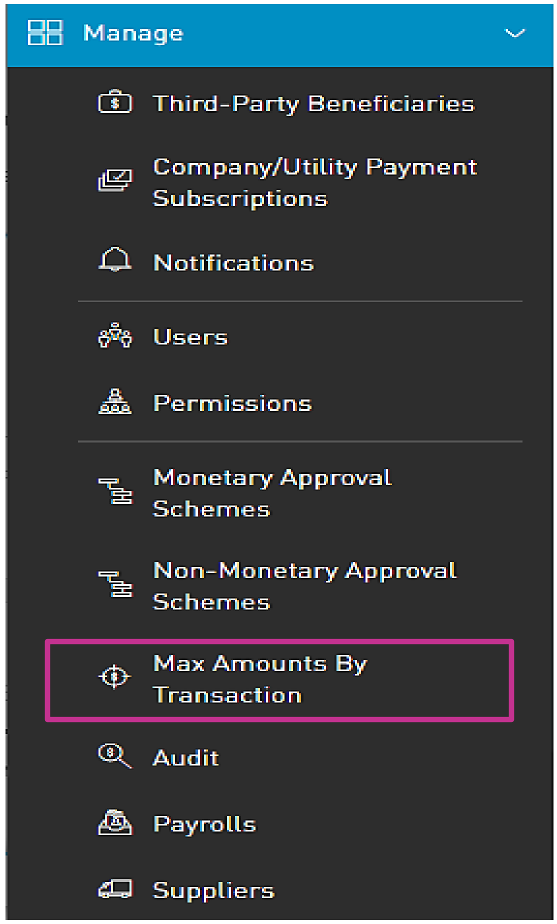


From the page the user may also edit and delete selected approval schemes via the contextual menu of the relevelant scheme.



Max Amount By Transaction

To access this Transaction Limits feature select the **Max Amounts by Transaction** option under the the **Manage** section of the **Main** menu.

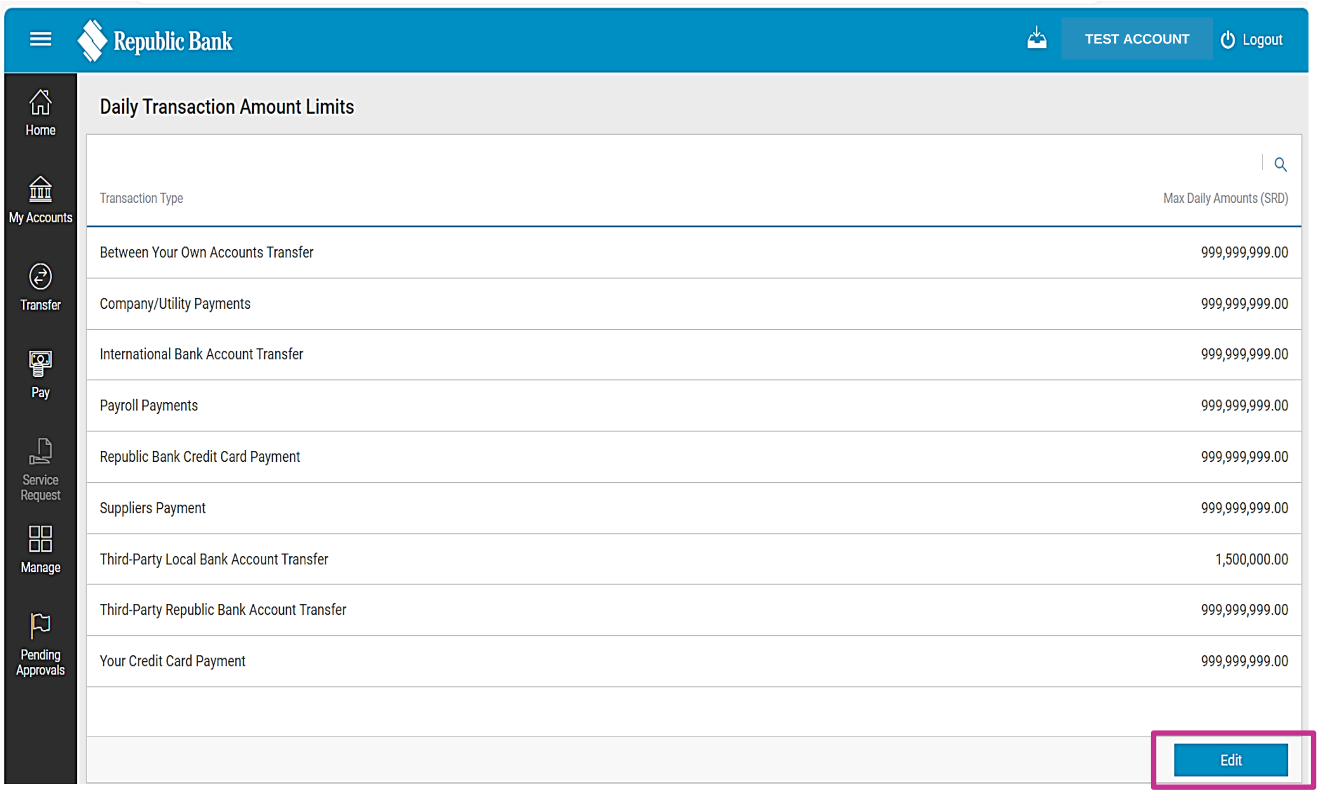


Only the users assigned the relevant permissions will be able to access to the Transaction Limits feature. (Refer to Appendix for list of Permissions)

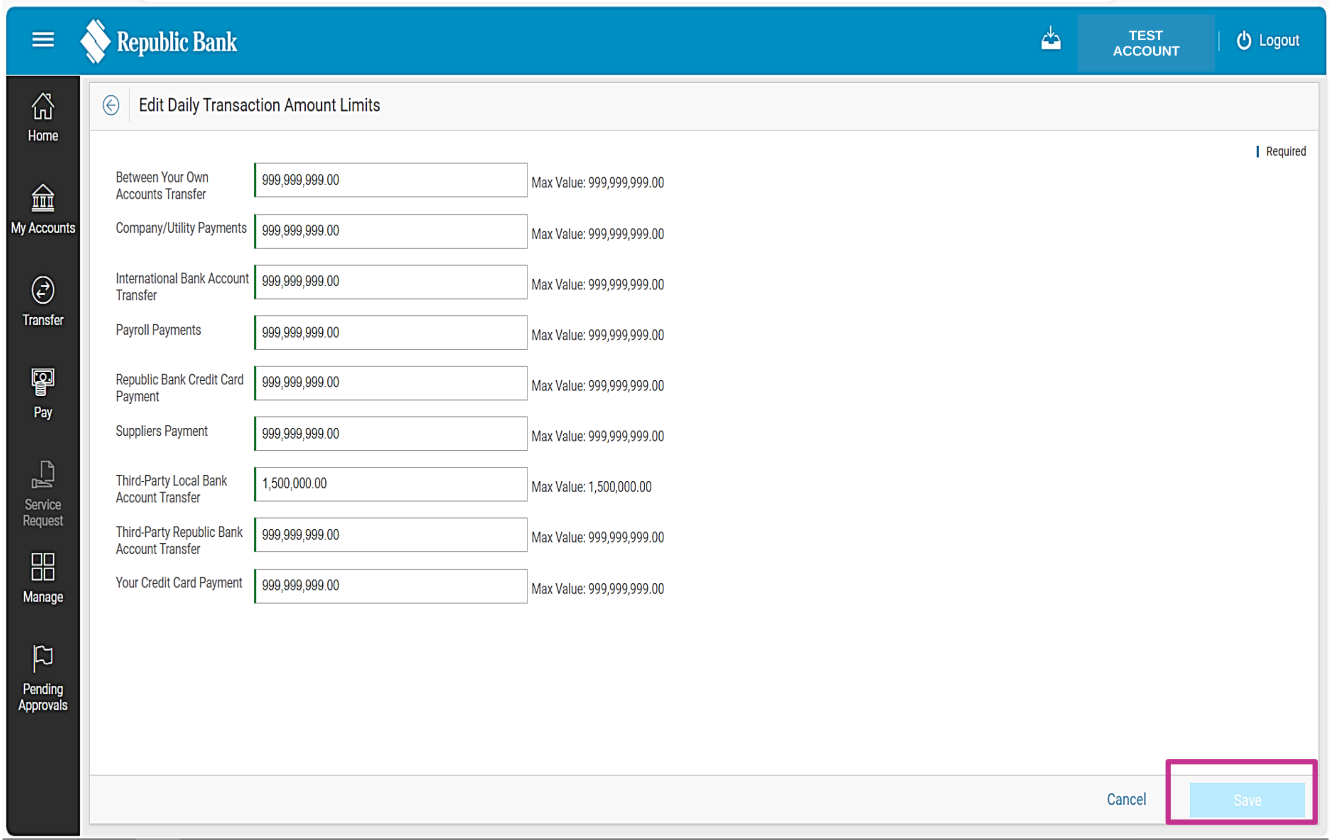
Daily Transaction Amount Limits Page

This page displays the master list of the daily transaction limits for the Business Site.

- To Edit this list, click on the **Edit** button at the bottom of the page.



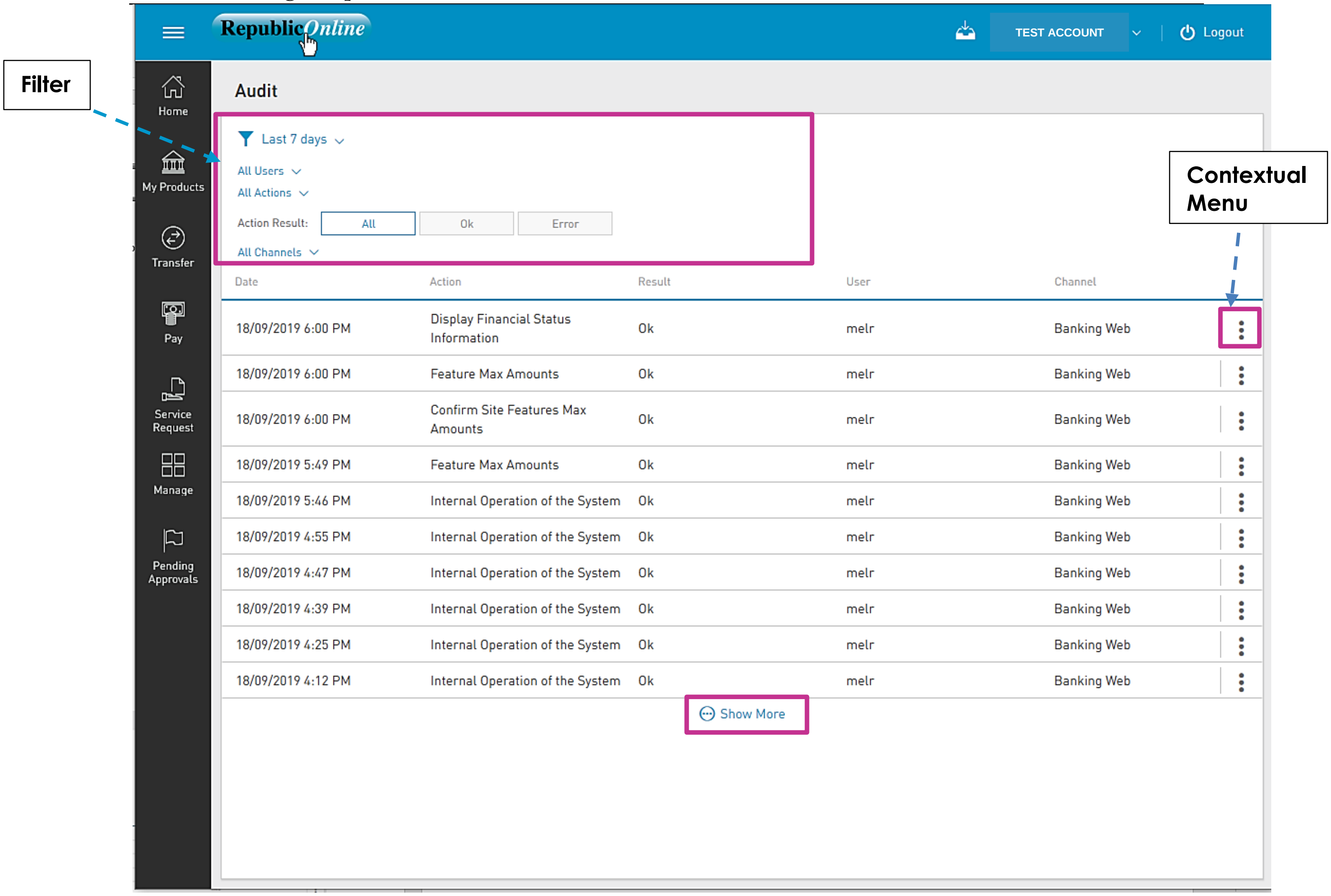
- Edit the amount in the relevant fields and click **Save** to proceed.



How to audit the business' online transactions?

Through the Audit feature, users can access the site's audit logs in a tabular format.

Only the users assigned the administrative permissions will have access to the Audit feature.



For each action or transaction, the following data is shown:

- Date
- Action
- Results
- User
- Channel

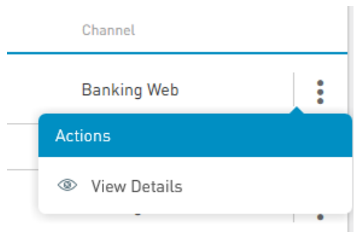
Filters

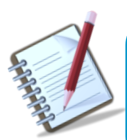
- **Last 7 Days**: enables filtering of logs by time period. Click the to change option.
- **All Users**: enables filtering of log by users. Click the to change option.

- **All Actions:** enables filtering by logs by specific actions. Click the to change option.
- **Action Result**: enables filtering by status of action. (All/OK/Error)
- **All Channels**: enables filtering by channel. Click the to change option.

Contextual Menu

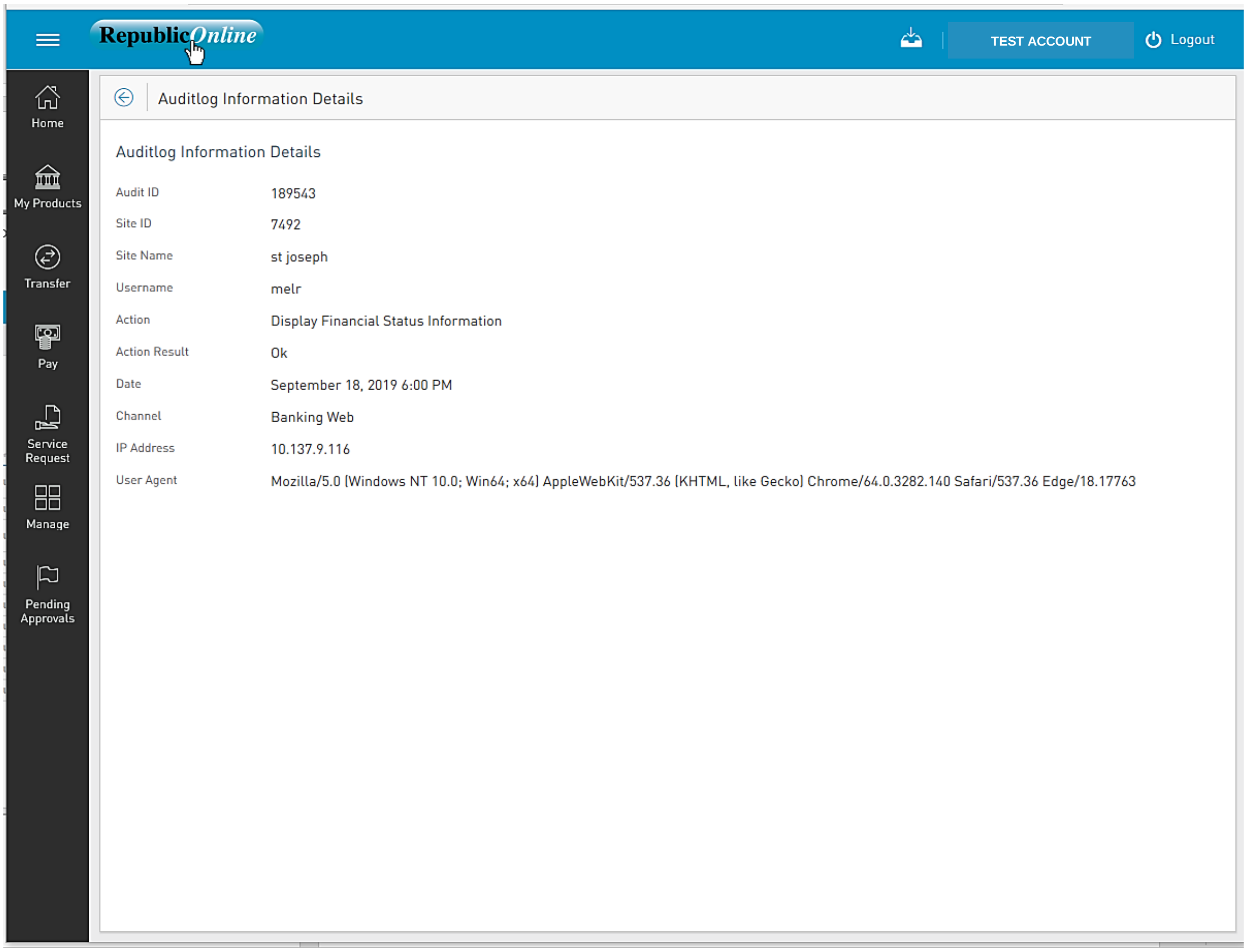
The menu on each log offers the View detail option only





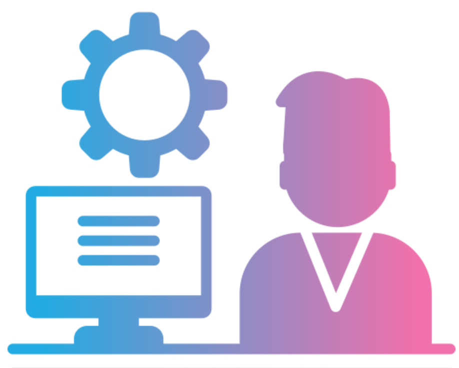
The only action available for the Audit is the view detail access. No site user has permission to amend any detail on the audit log.

Auditlog Information Details Screen



For each different action the details displayed will vary. The general data shown is as follows:

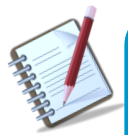
- Audit ID
- Site ID
- Site Name
- Username
- Action
- Action Result
- Date
- Channel
- IP Address
- User Agent



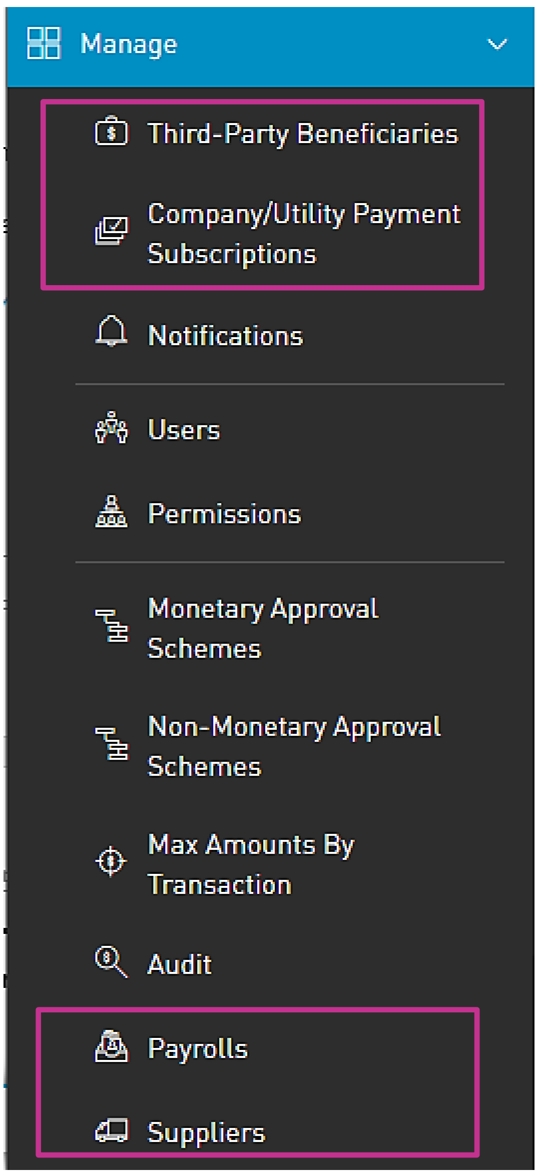
Manage

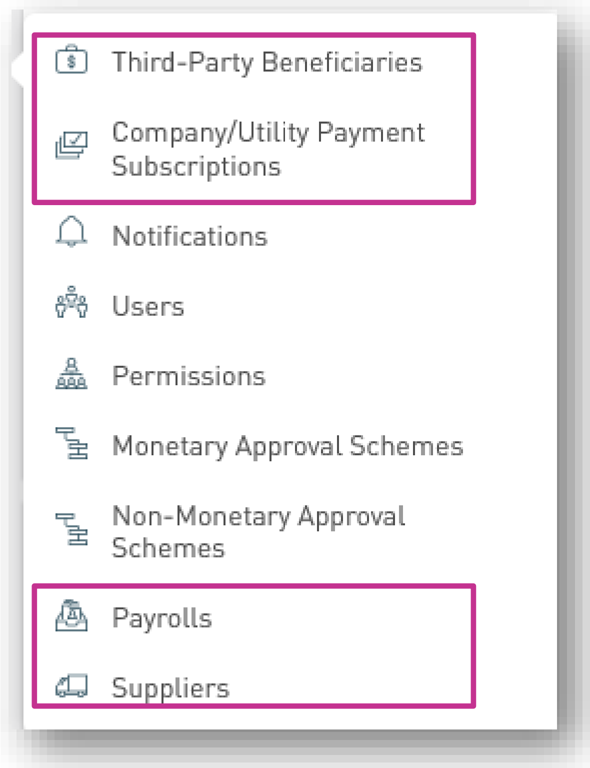
Manage - Overview

This section of the application is where users access the administrative functions. This option is available from both the **Quick** and **Main Menu**.



The fundamental administrative functions were explained in previous section of this book. This section will expound on the other administrative features that are related to products and monetary functions.





OR

Third-Party Beneficiaries

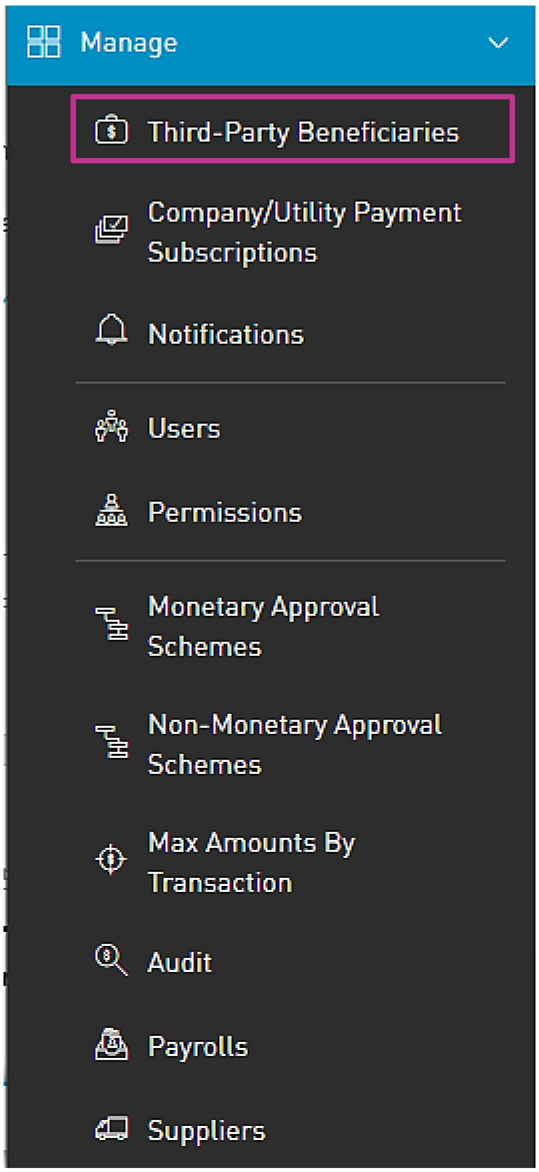
Customers will be allowed to make payments to the following third-party products:

- Republic Bank Chequing Account
- Republic Bank Savings Account
- Republic Bank Credit Card
- Local Bank Deposit Account
- International Bank Deposit Account

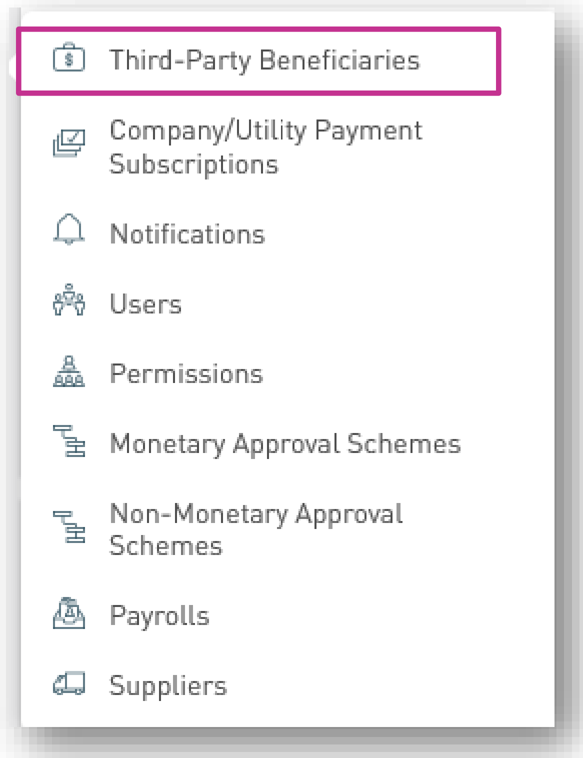
For Corporate Republic*Online* customers, all beneficiaries must be registered.

How to Register Third-Party Beneficiaries

To register third-party beneficiaries, select the **Third-Party Beneficiaries** option under the **Manage** tab of either the **Main** or **Quick Menu.**

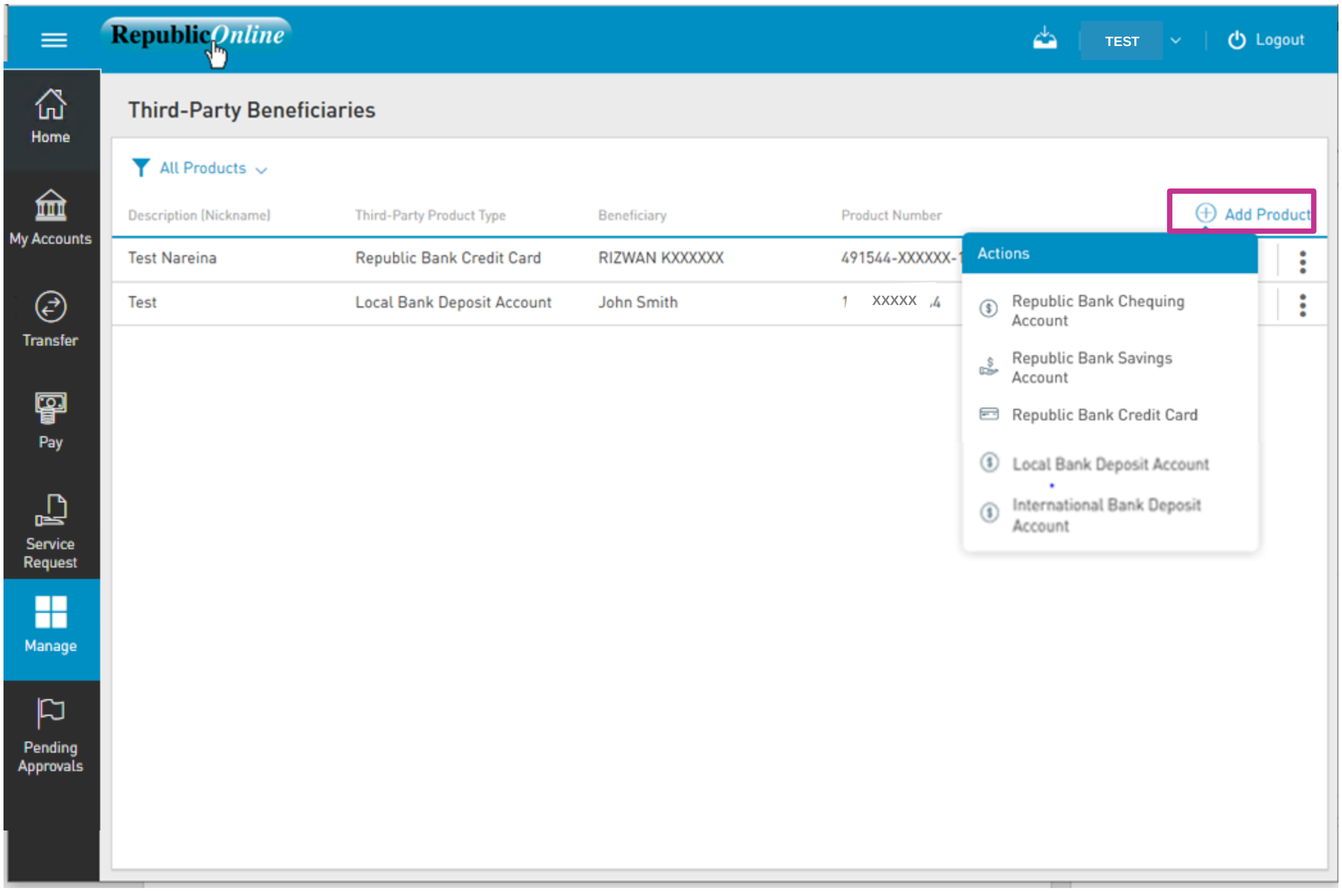


OR



This option will direct the user to the the **Third-Party Beneficiaries** page.

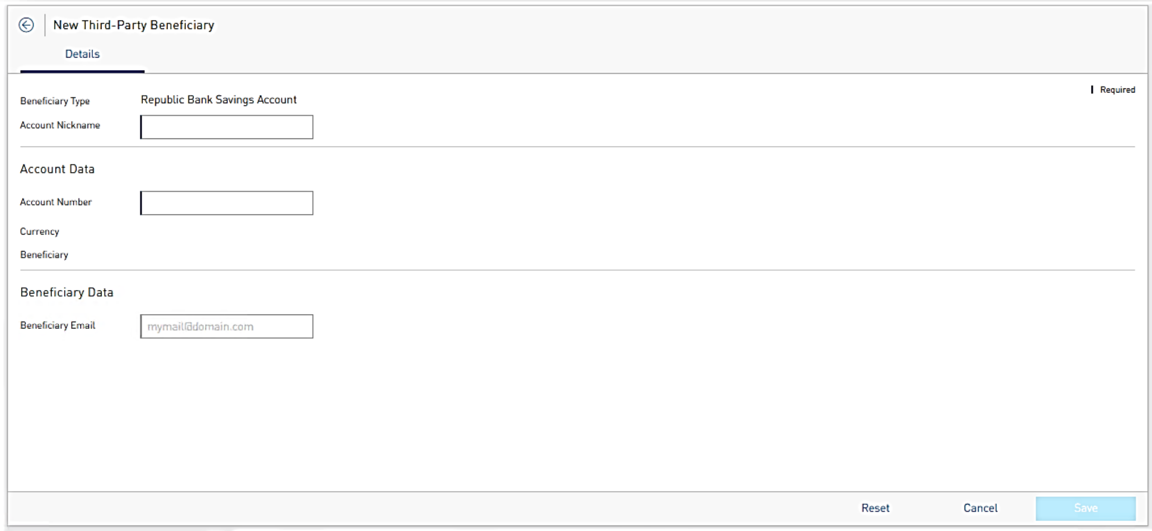
- Select the "Add Product" icon
- Select the relevant type of beneficiary account from the list provided



For Republic Bank Beneficiaries (Republic Bank Chequing account, Savings account, or Credit Card) the following information will be requested:

- Product Nickname(Required)
- Account data - number (Required)
- Beneficiary Email – This field is not mandatory. However, if the user requires the beneficiary to be notified when payments are made, then the beneficiary's email address can be included here. If no data is input in this field, the system will automatically send the notification to the default email address, which is the user's registered email address.

Example:

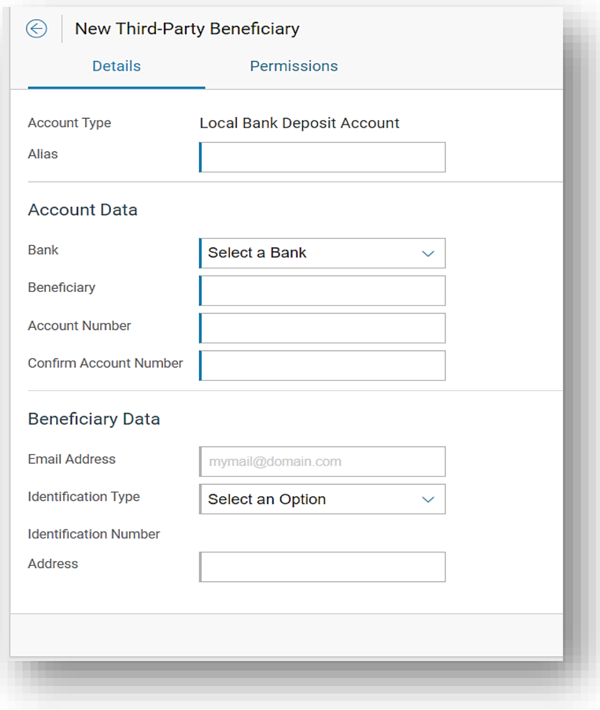


For external beneficiaries, which include the local bank deposit account and International Bank Deposit account, the user will be required to input the product data as well as the external bank information.

Local Bank Deposit Account:

The following information will be requested for a Deposit account in a local bank:

- Alias (Required)
- Account data:
    - Bank (Required)
    - Beneficiary name (Required)
    - Account Number (Required)
- Beneficiary data:
    - Email address
    - Identification type
    - Identification number
    - Address



International Bank Deposit Account:

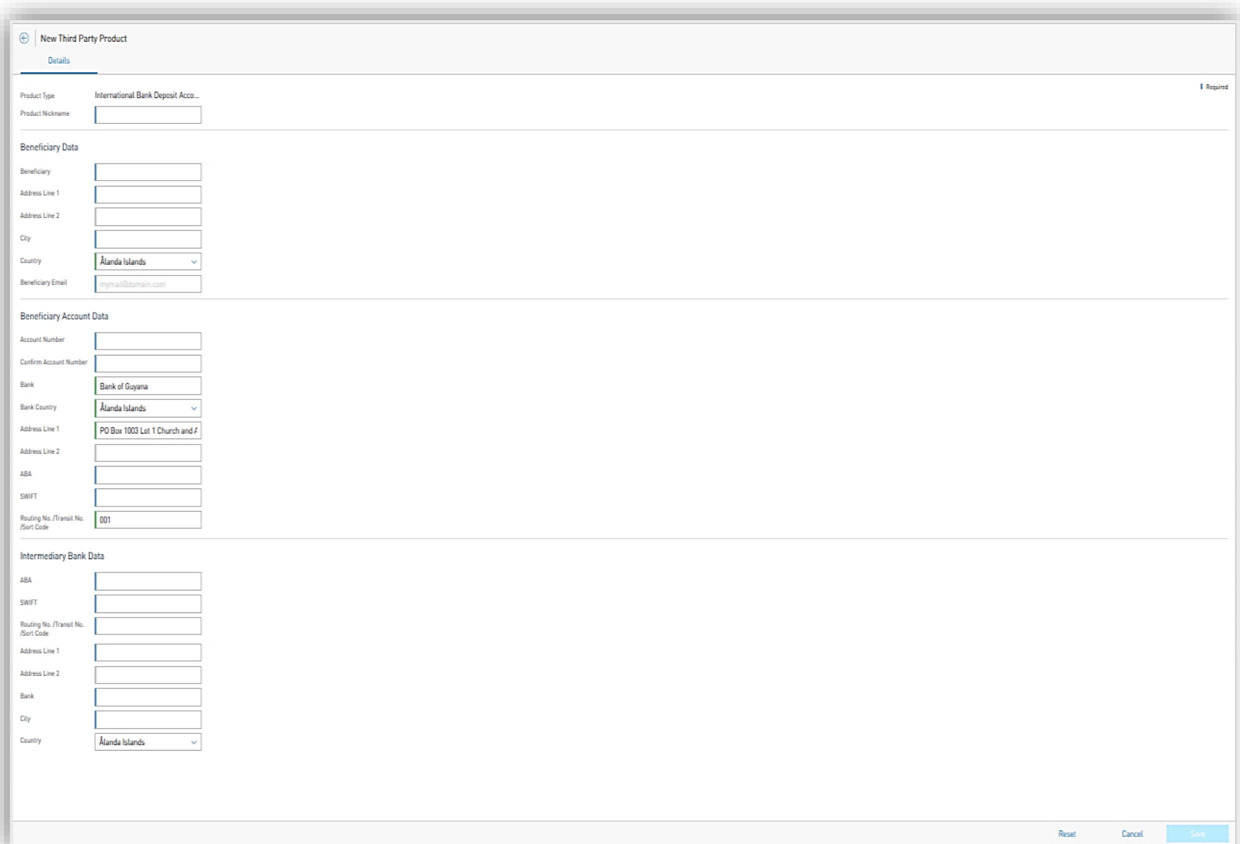
The following information will be requested for a Deposit account in an international bank:

- Product Nickname(Required)
- Beneficiary data:
  - Beneficiary (Required)
  - Address (Required)
  - City (Required)
  - Country (Required)
- Beneficiary Account Data:
  - Account Number (Required)
  - Bank
  - Bank Country
  - Address
  - ABA (Required)

- Swift (Required)
- Routing No./ Transit No./Sort Code

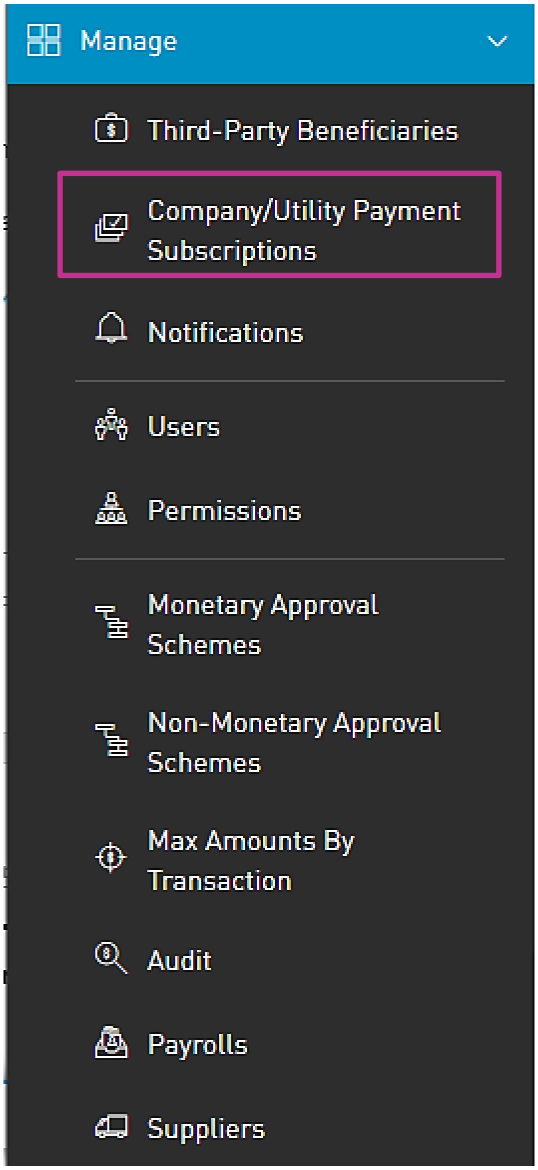
● Intermediary Bank Data:

- ABA (Required)
- Swift (Required)
- Routing No./ Transit No./Sort Code (Required)
- Address (Required)
- Bank (Required)
- City (Required)
- Country (Required)

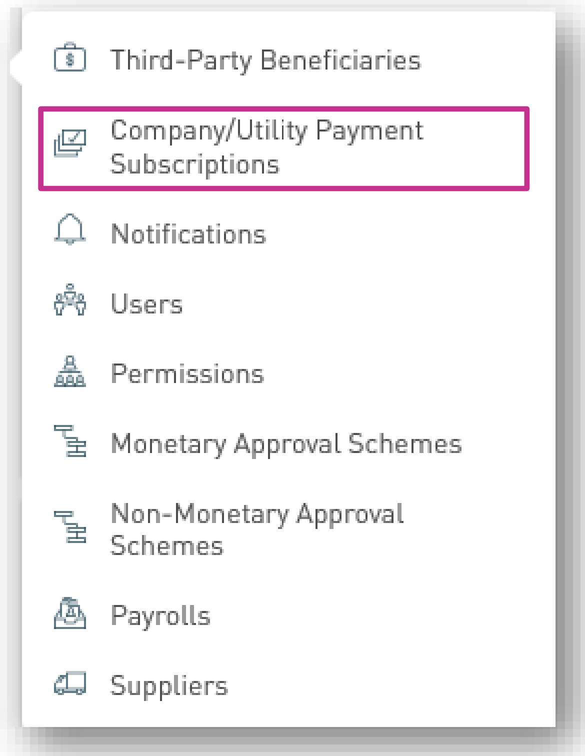


How to Register Company/Utility Payment Subscriptions?

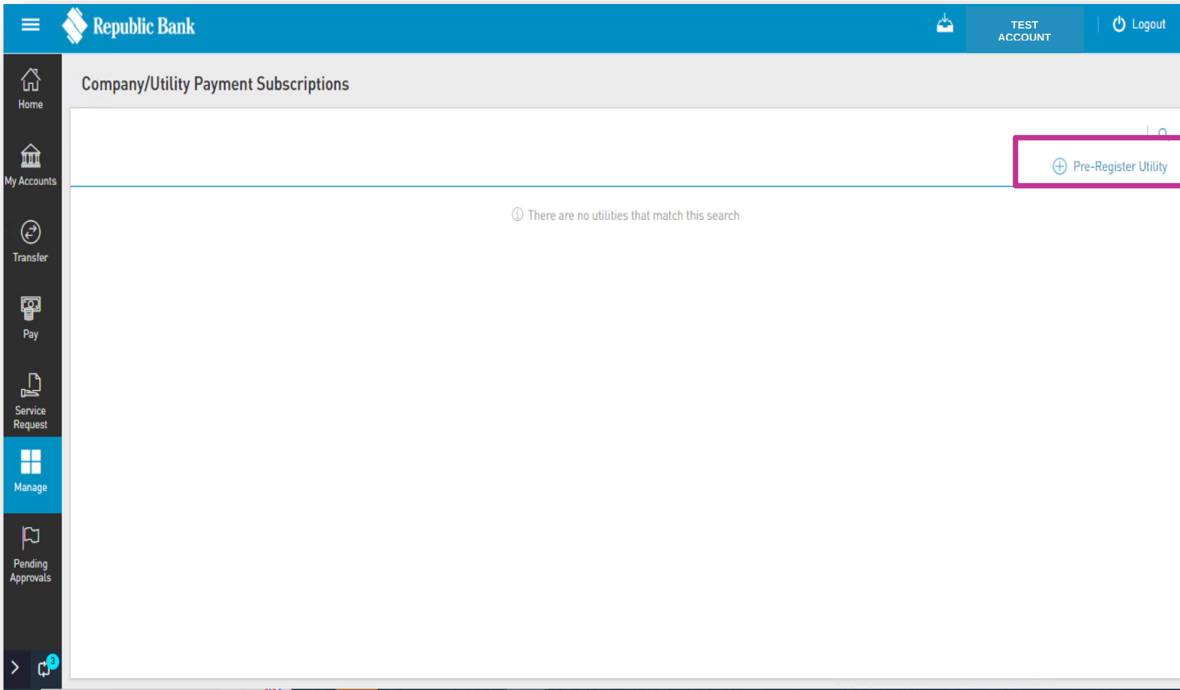
To register third-party beneficiaries, select the **Company/Utility Payment Subscriptions** option under the **Manage** tab of either the **Main** or **Quick Menu.**



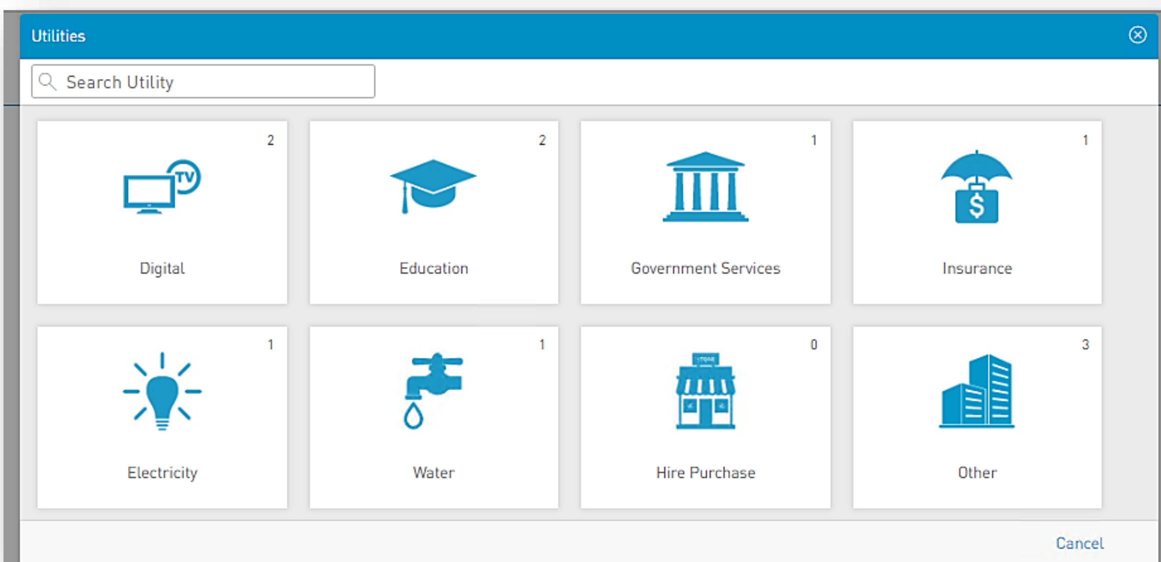
OR



This option will direct the user to the the **Company/Utility Payment Subscriptions** page.

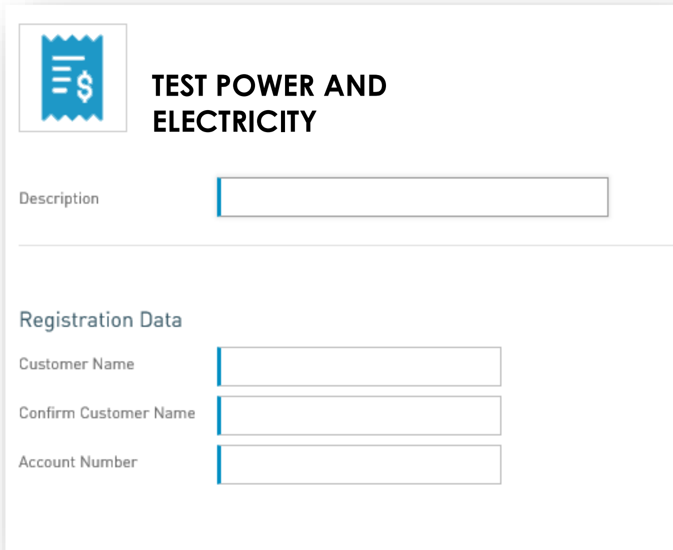


1. Select a category from the list provided.
2. Select the relevant utility



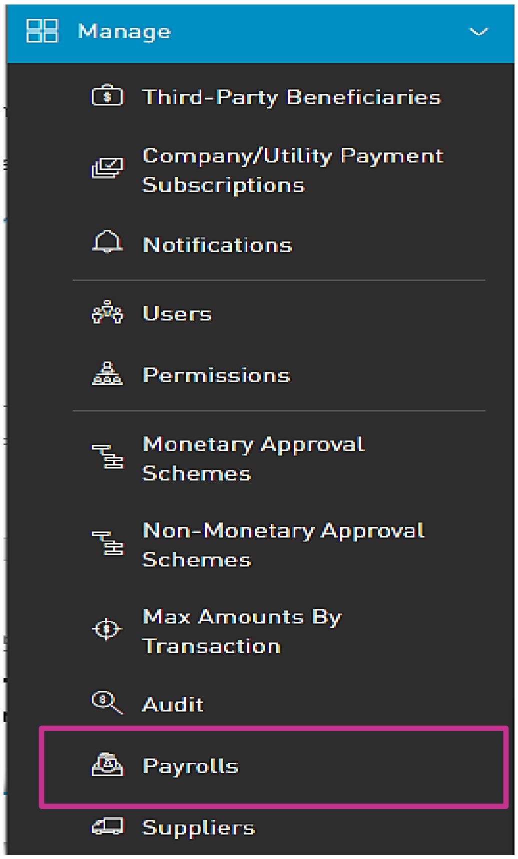
3. Insert required data and select **CONFIRM** to save the Company/Utility information.

Example:

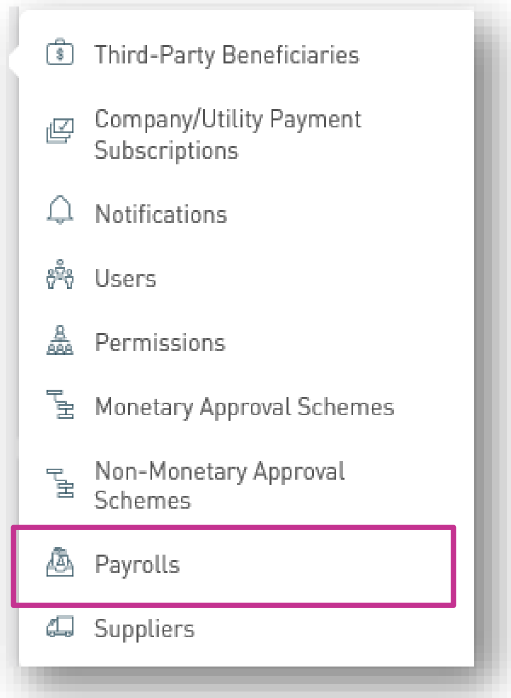


Payroll Administration

Payrolls can be created or amended via the Payroll Admininstration Page. To access this page select the **Payroll** option under the the **Manage** section of either menu.

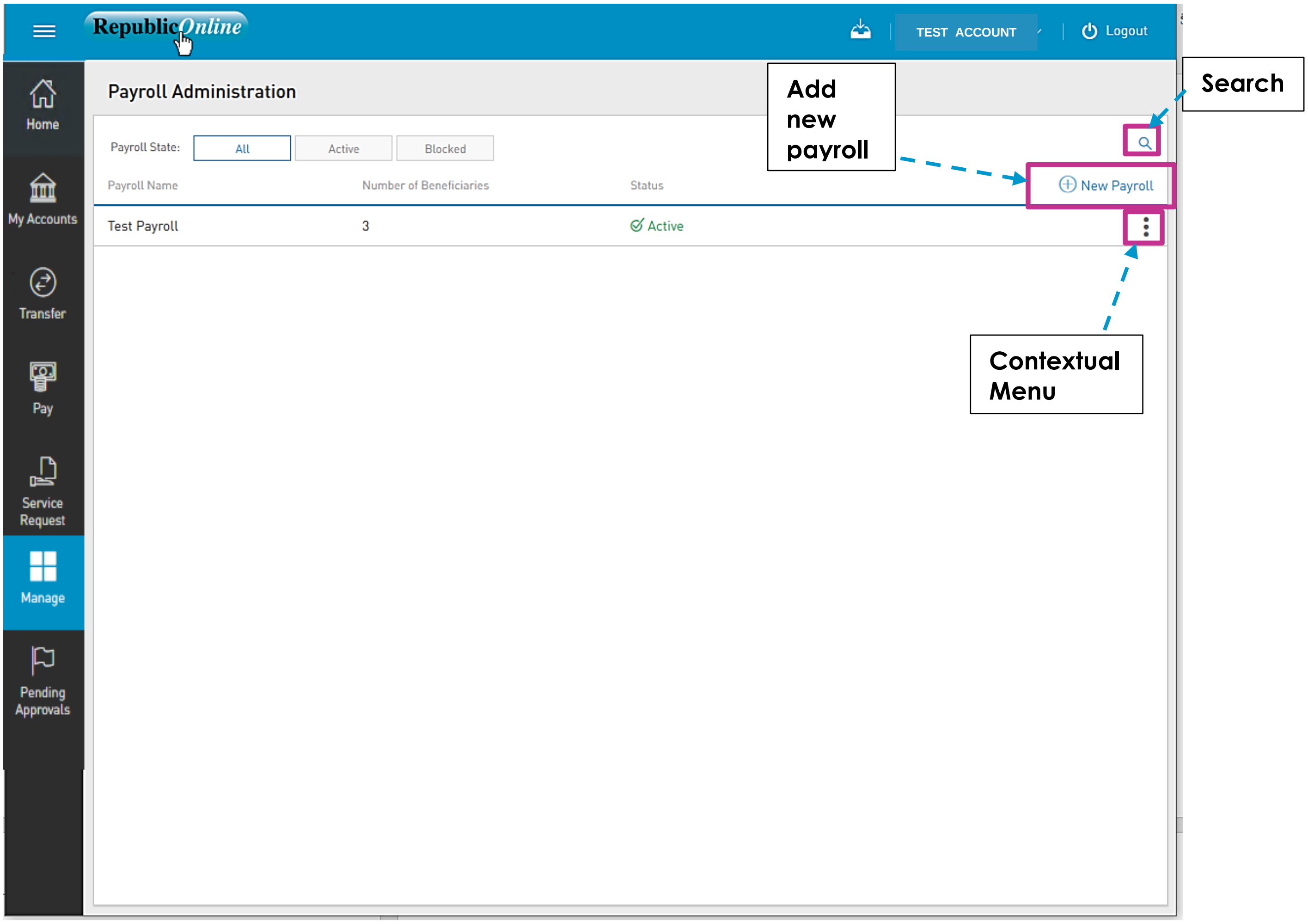


OR



Only the users assigned the relevant permissions to do payroll administration will have access to this page. (Refer to Appendix for full list of permissions)

Payroll Administration Page

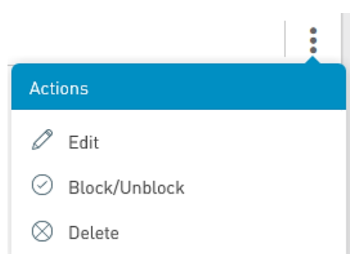


This page contains a master list of all the Site's existing payrolls.

Contextual Menu

The menu on each payroll list offers the following actions:

- Edit
- Block/Unblock
- Delete



How to create a new payroll?

To create a new payroll, click on the ⊕ New Payroll link.

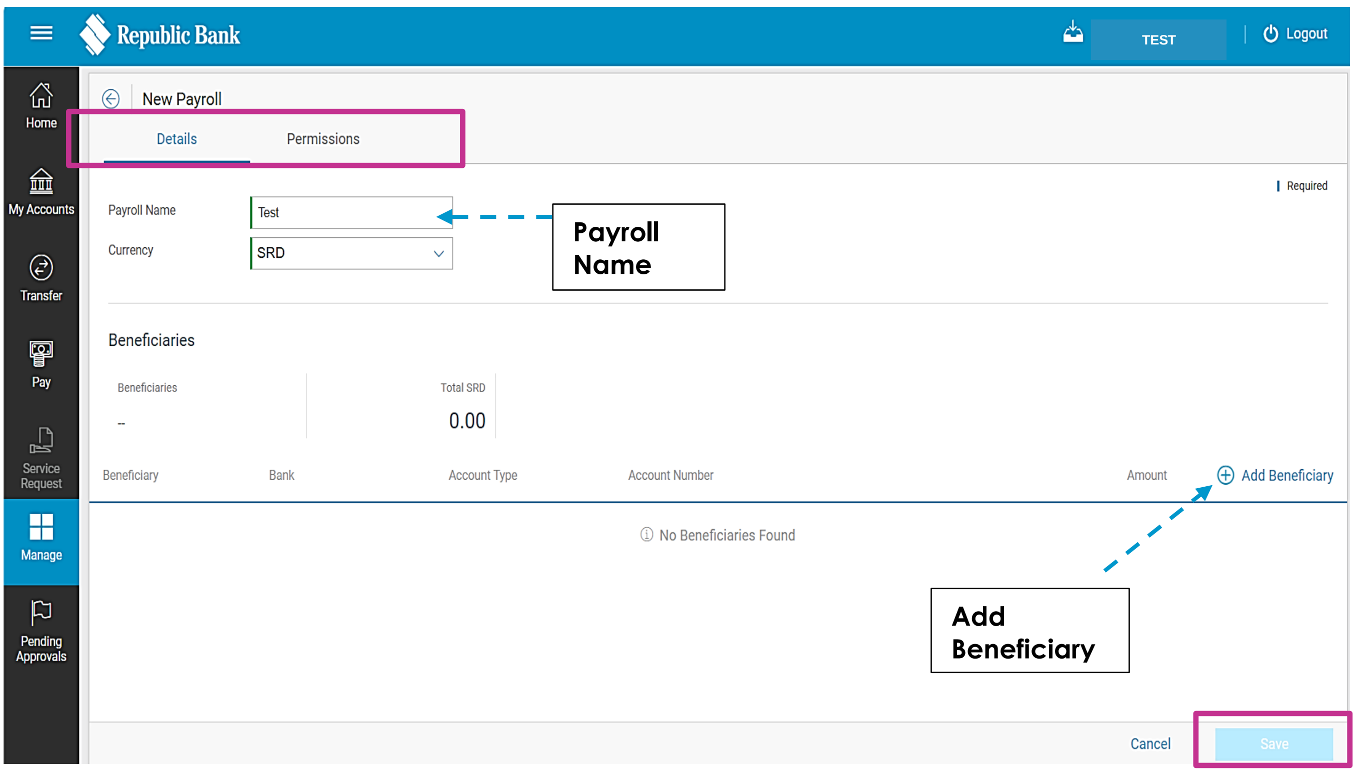
There are two (2) Main steps in creating a payroll:

- **Details**

  The Details includes adding the beneficiary information to the payroll list

- **Permissions**

  The Permissions entails adding users who are required to access the payroll (e.g. To pay the payroll)

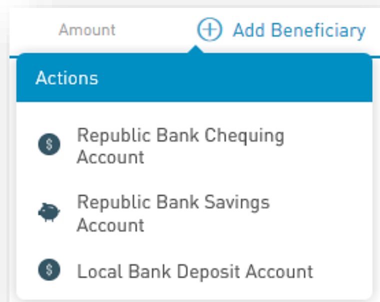


1. Details

- Insert a name for the new payroll list in the space provided.

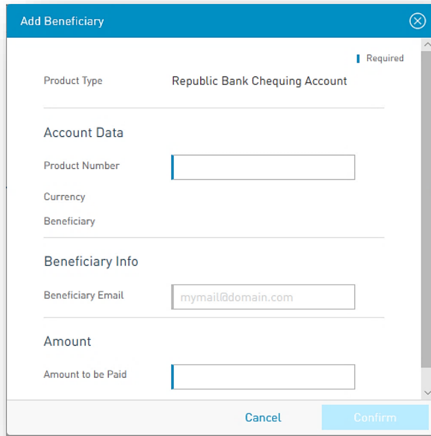
- Click on the ⊕ Add Beneficiary link to add beneficiaries to the list.

- Select Beneficiary Type. The options are:
    - Republic Bank Chequing Account
    - Republic Bank Savings Account
    - Local Bank Deposit Account



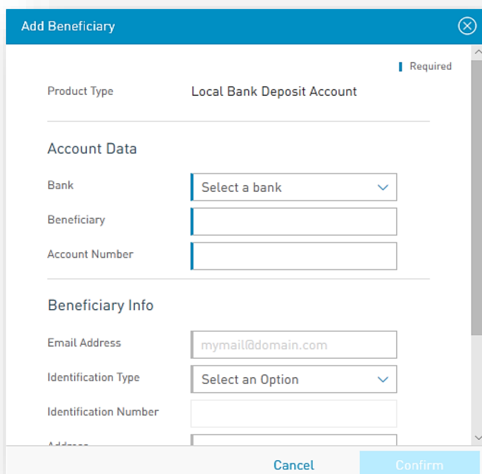
- Insert Beneficiary Details as follows:

- Account Data: Product Number
    - Currency
    - Beneficiary
- Beneficiary Info: Email
    - Id Type/Id Number (Optional)
    - Address (Optional)
- Amount to be paid.



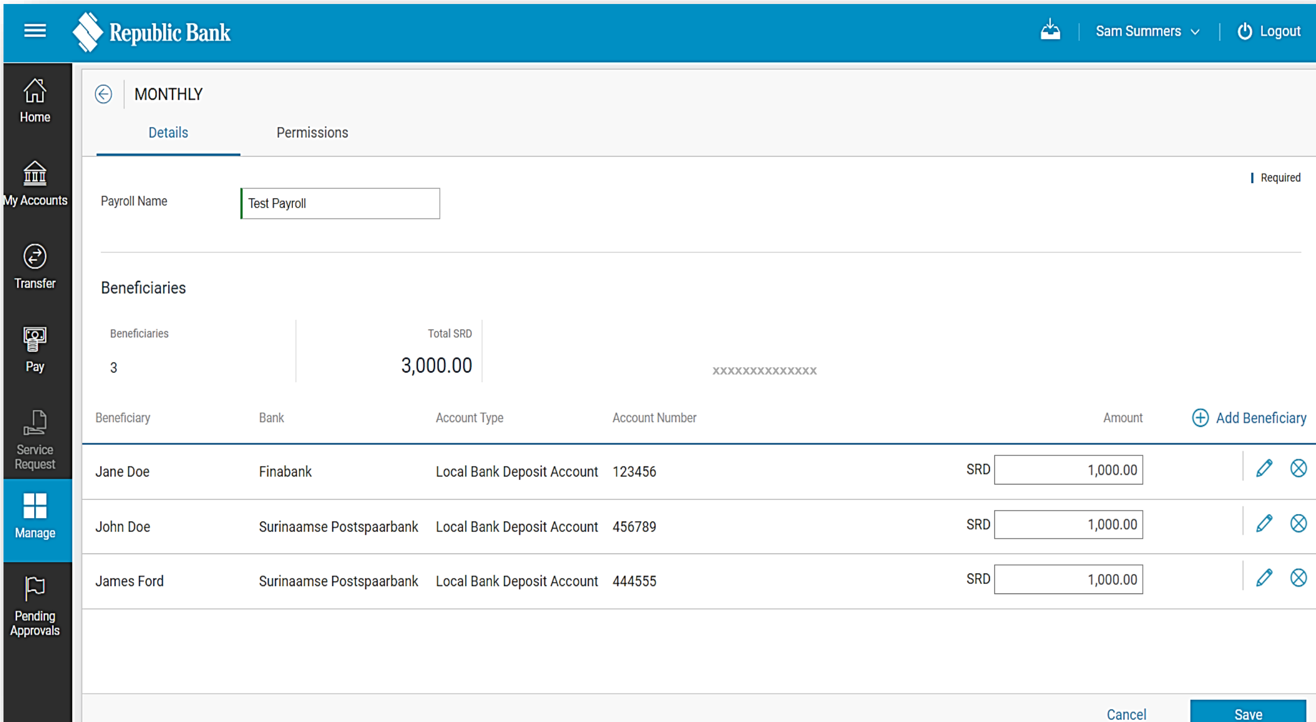
Republic Chequing Account

> **For Republic Bank Beneficiary accounts, the product number will be validated, and the system will auto-populate the currency and beneficiary name, once the account is valid and active.**



Local Bank Account

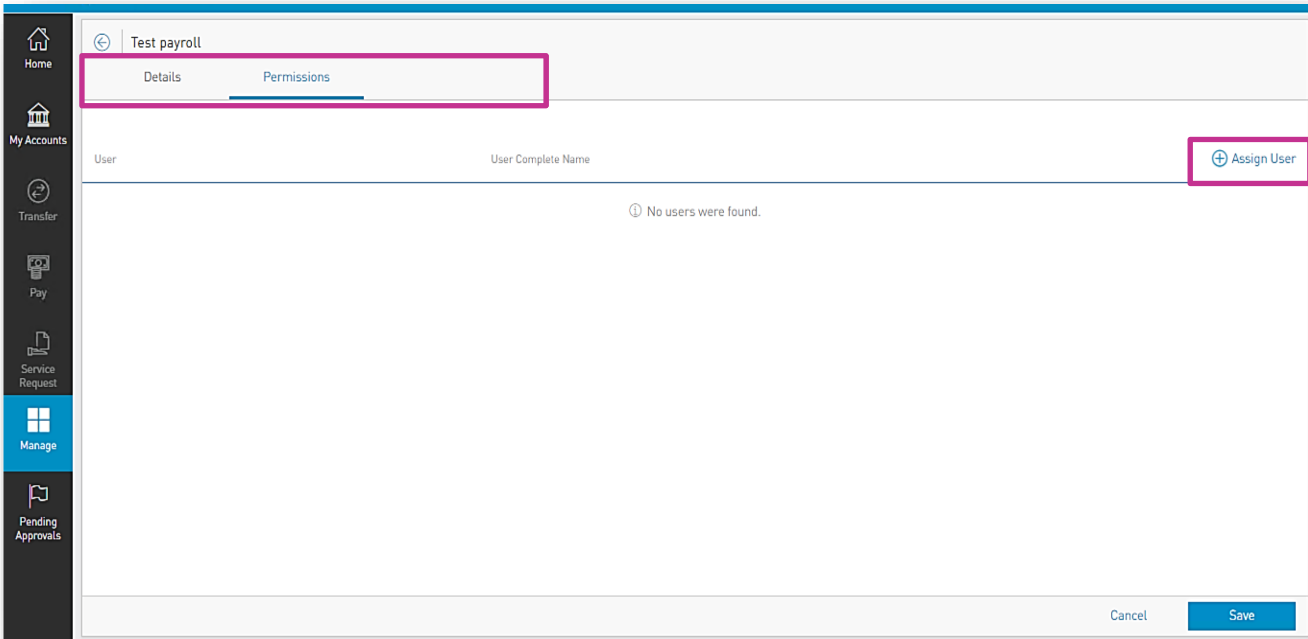
> **For Local Bank Beneficiary accounts, the Bank, Beneficiary and account number are required. There are additional fields included for the beneficiary, but these are not mandatory. This information is included to aid the bank in identifying them, if required.**



2. Permissions.

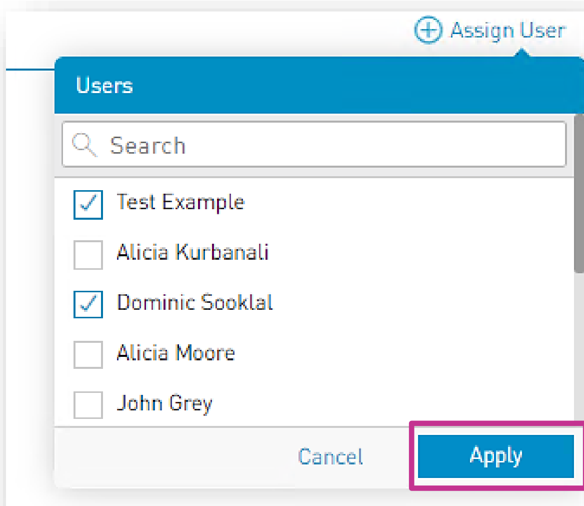
When the user has finished inputting the Details of the payroll list, he/she must then assign permissions to users who are required to access this payroll.

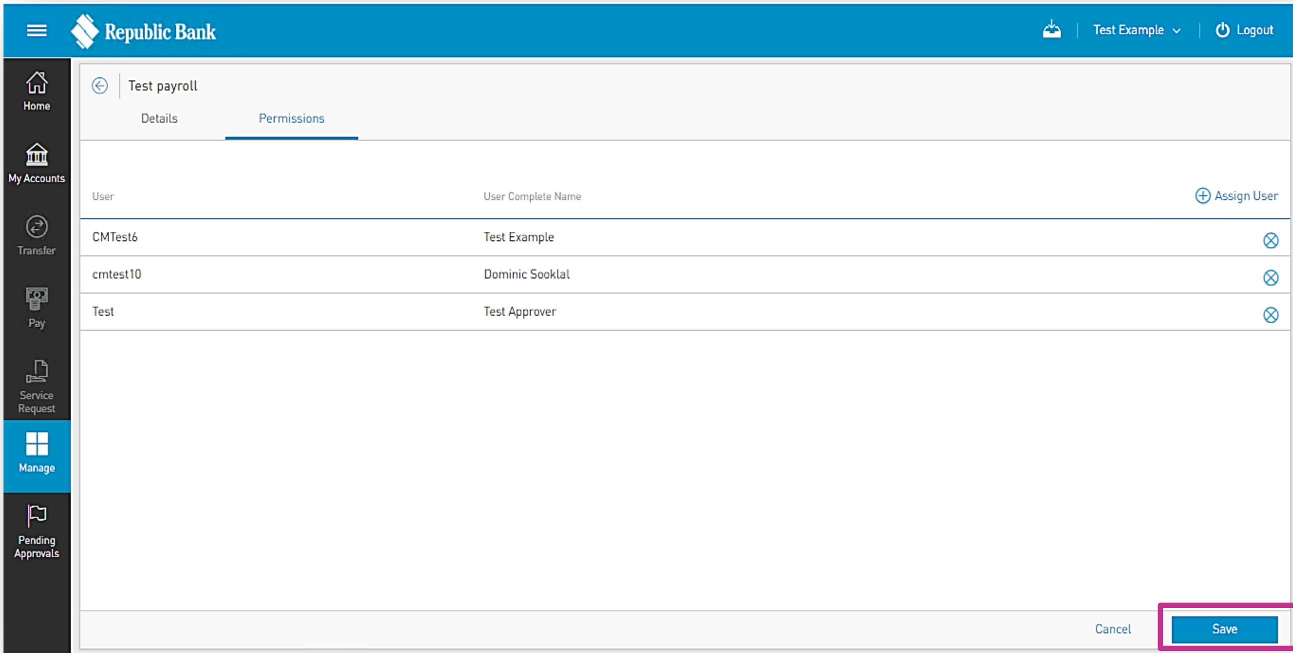
- Click on the Permissions tab at the top of the screen.



- Click the ⊕ Assign User link to select users.

- Select the user(s) from the list by ticking the radio button(s) and click Apply.





Once the information is verified, click 

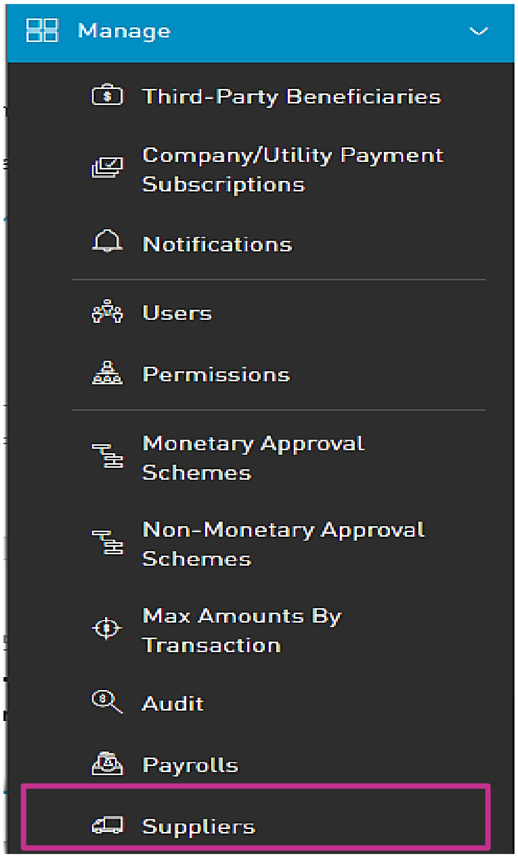
.

This completes the process for adding a new payroll. The user will be redirected to the Payroll Administration Page.

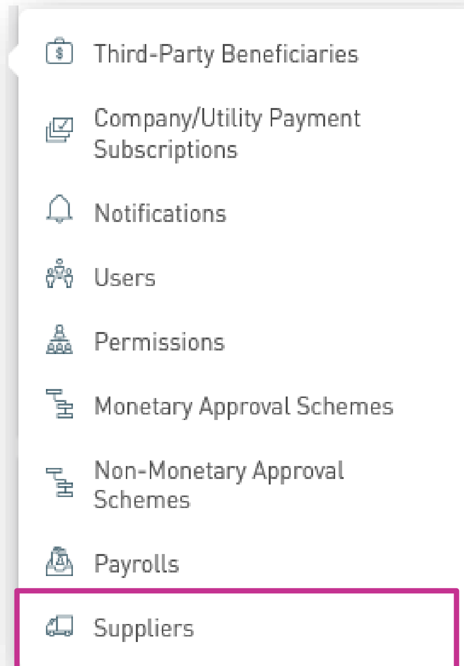
Payrolls registered here will be used in the Manual Payroll payments.

Suppliers Administration

Supplier lists can be created or amended via the Suppliers Admininstration Page. To access this page select the **Suppliers** option under the the **Manage** section of either menu.

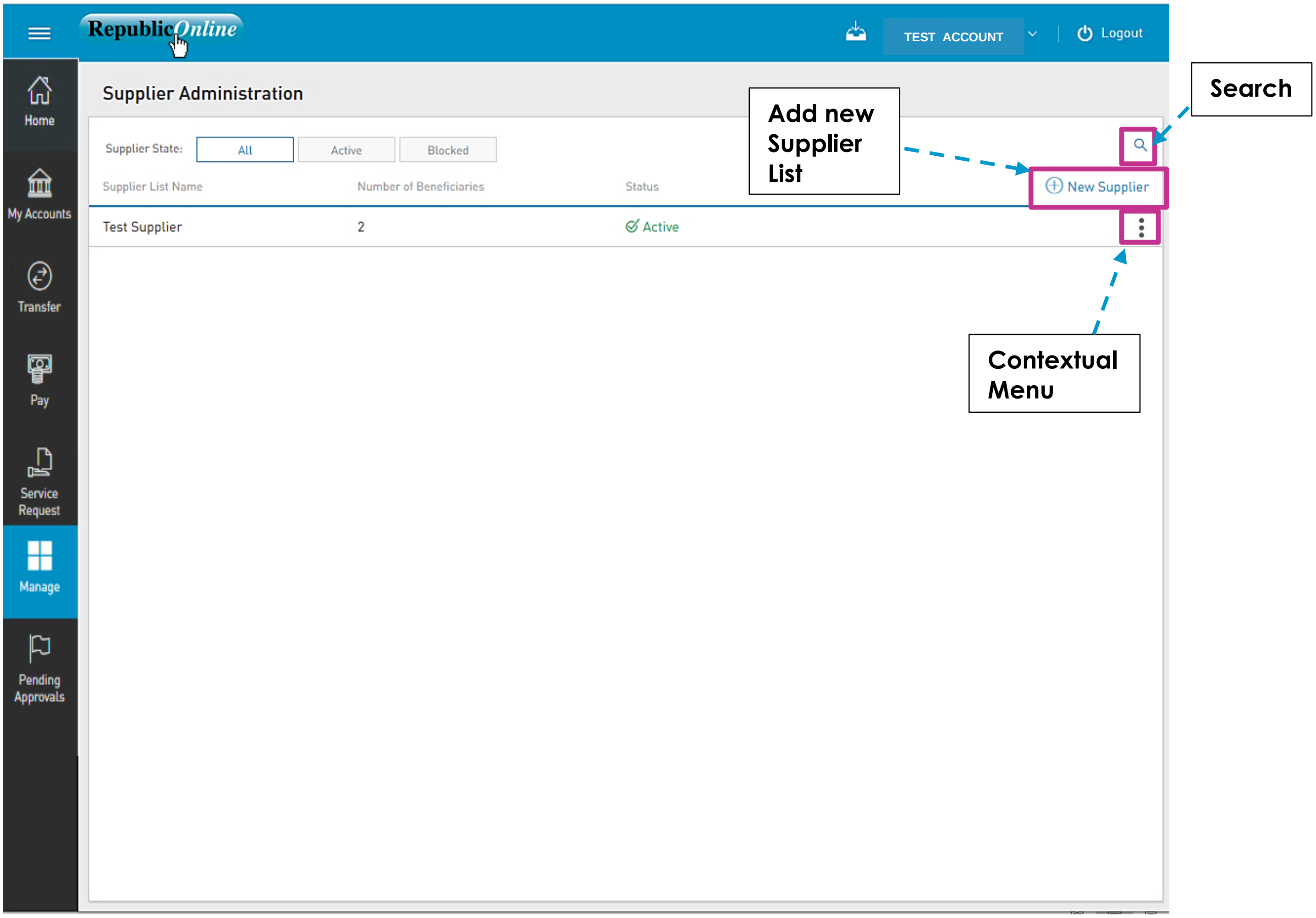


OR



Only user with the permissions to do supplier administration will have access to this page. (Refer to Appendix for full list of permissions)

Supplier Administration Page

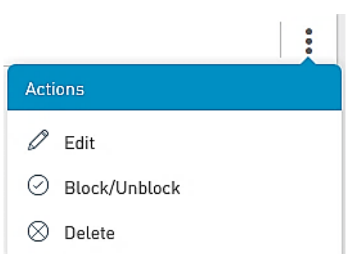


This page contains a master list of all the Site's existing supplier lists.

Contextual Menu

The menu on each payroll list offers the following actions:

1. Edit
2. Block/Unblock
3. Delete



How to create a new Supplier List?

To create a new supplier list, click on the ⊕ New Supplier link.

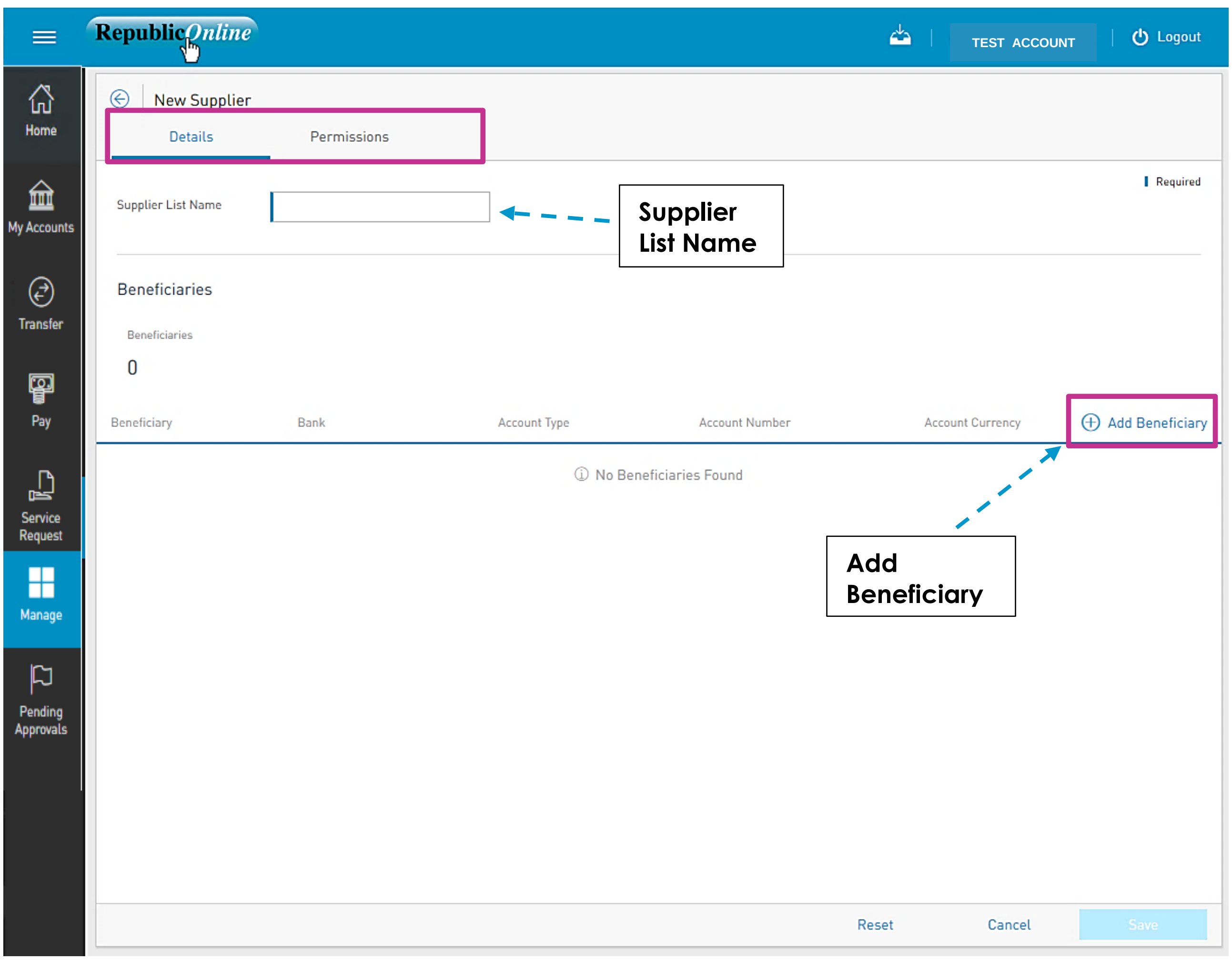
There are two (2) Main steps in creating a supplier list:

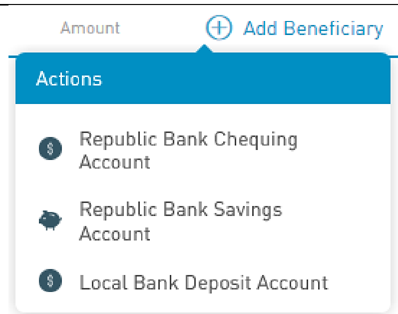
- **Details**

  The Details includes adding the beneficiary information to the payroll list

- **Permissions**

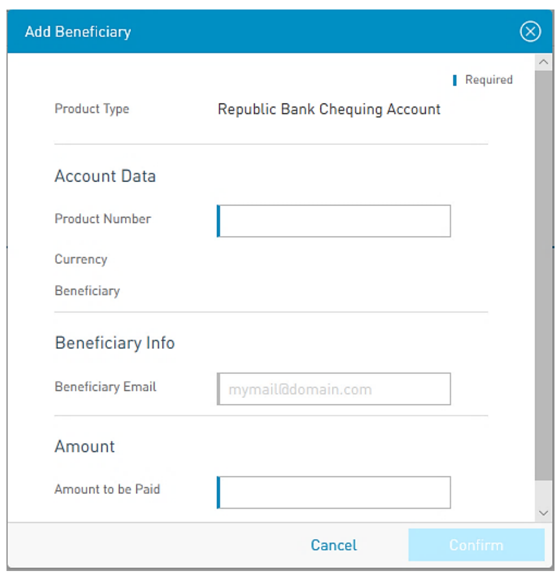
  The Permissions entails adding users who are required to access the payroll (e.g. To pay the payroll)





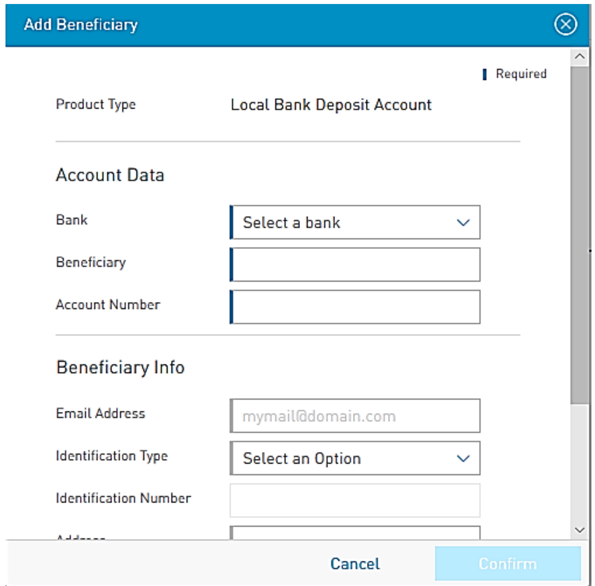
- Insert Beneficiary Details as follows:

- Account Data: Product Number
  - Currency
  - Beneficiary
- Beneficiary Info: Email
  - Id Type/Id Number (Optional)
  - Address (Optional)
- Amount to be paid.



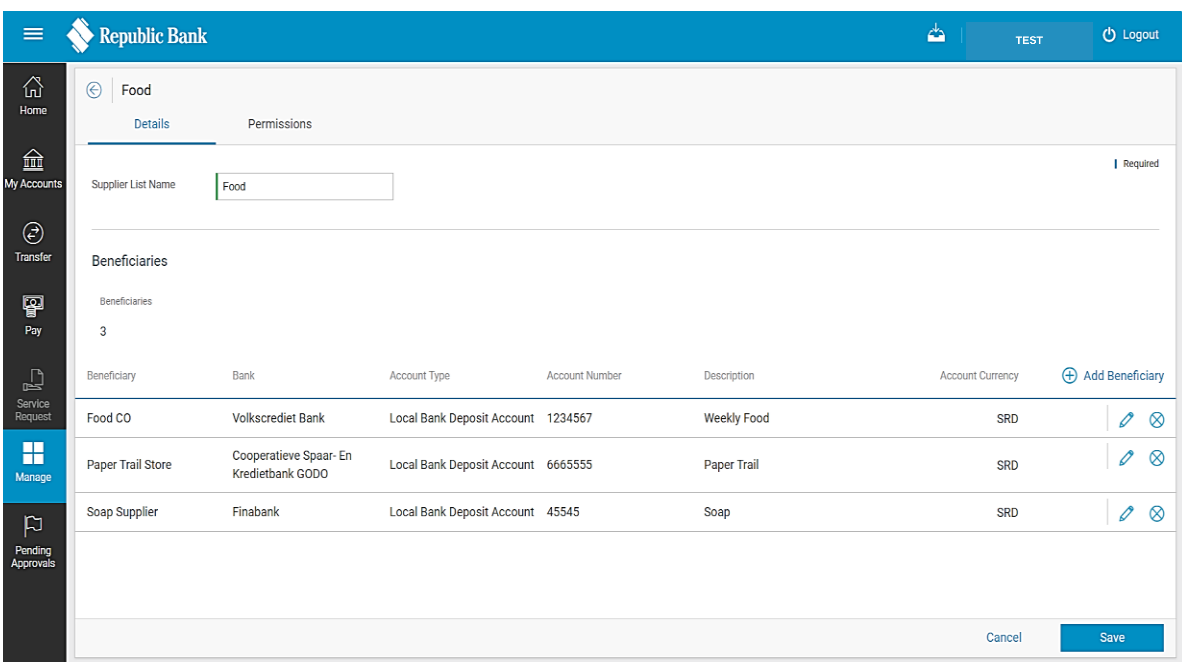
Republic Chequing Account

For Republic Bank Beneficiary accounts, the product number will be validated, and the system will auto-populate the currency and beneficiary name, once the account is valid and active.



Local Bank Account

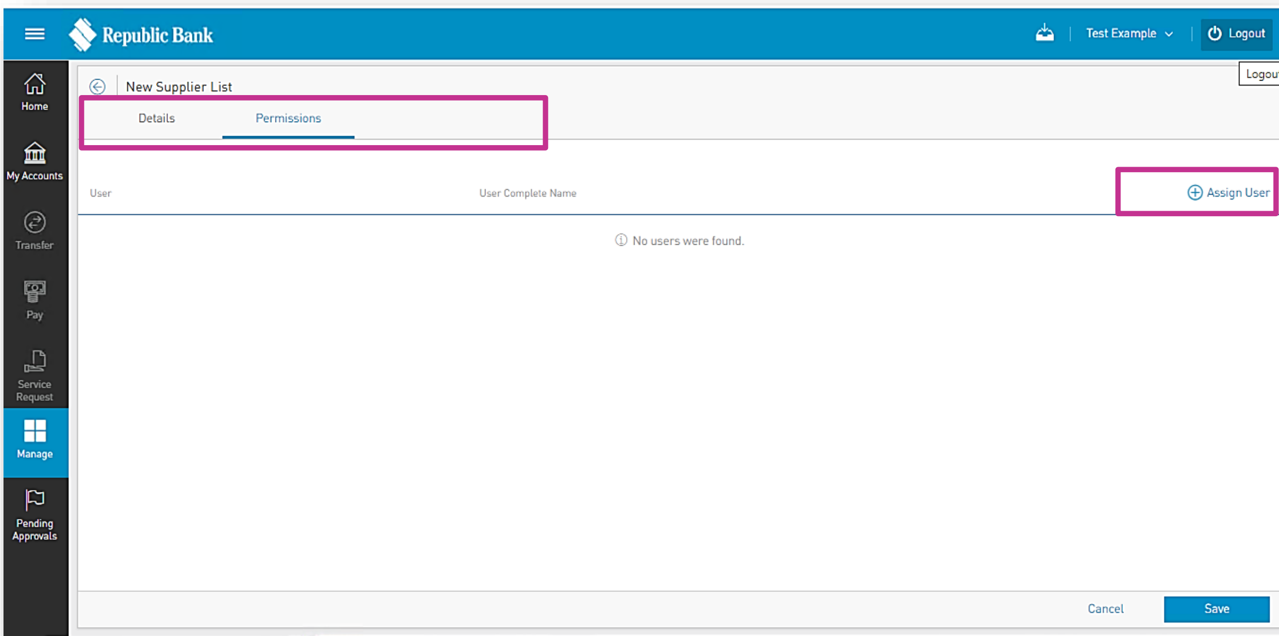
For Local Bank Beneficiary accounts, the Bank, Beneficiary and account number are required. There are additional fields included for the beneficiary, but these are not mandatory. This information is included to aid the bank in identifying them.



Permissions

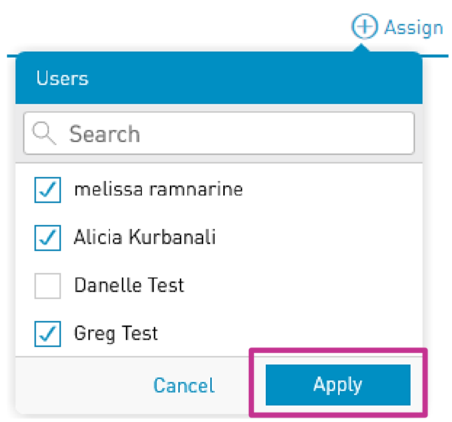
When the user has finished inputting the Details of the supplier list, he/she must then assign permissions to users who are required to access this payroll.

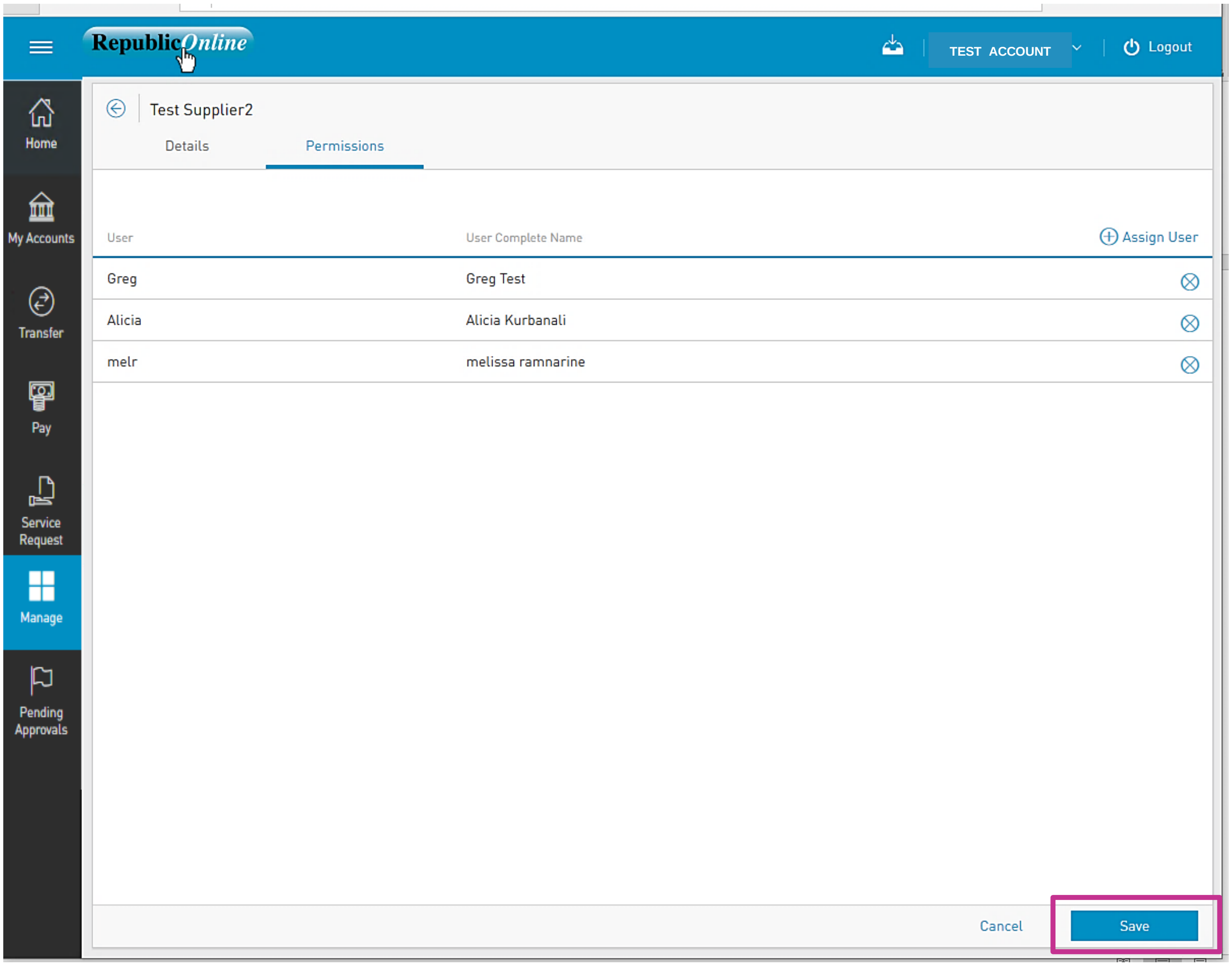
- Click on the Permissions tab at the top of the screen



- Click the ⊕ Assign User link to select users.

- Select the user(s) from the list by ticking the radio button(s) and click Apply.





Once the information is verified, click Save.

This completes the process for adding a new supplier list. The user will be redirected to the Supplier Administration Page.

Supplier Lists registered here will be used in the Manual Supplier payments.

Appendix

Appendix A - Key Terms to Note

In addition to the many new features of the upgraded Republic*Online* application, there is also some new jargon that users should become familiar with.

Here are some key terms and expressions that apply to the new RepublicOnline:

Term	*Meaning*
Second-Factor Authentication Device	This refers to the device used as the second layer or security to protect a user's internet banking account. In this case, we utilise a mobile device to obtain the second layer of authentication. These include, OTP, Sync and SMS Code.
OTP (One-Time Password)	The *OTP* is an automatically generated code, that may only be used for one login session. Republic*Online* OTPs will be generated by the system and are to be retrieved on the second factor authentication device.
Sync	The *Sync* refers to a process whereby a code is generated by the website and the user either scans or manually inputs the code into the mobile app to synchronise the two devices.
Business Site	This term is used to describe the user's Republic*Online* workspace, where they can access their products, balances, transactions, features and so on.
Business Site Administrator	The Business Site Administrator, is the designated official responsible for the management of the Business' Site. This includes the administration of the Business Site's products, users, permissions, limits and settings.

Permissions	Permissions are the rights or access privileges that are granted to a RepublicOnline user. These permissions determine the access that a user will have to the various functionalities and transactions.
Scope	A Scope refers to a Product and the associated functionality. The system will automatically generate all scopes for all the products associated with a Site. E.g. 1. Chequing Account A + Transfer to International Account 2. Savings Account B + Pay Utility
Approval Schemes	*Approval schemes* outline which users have the authorisation to approve transactions on a Business Site. Schemes comprise the scope, as well as the users assigned to the scope and their authorisation privileges. These may be monetary or non-monetary and are configured by the Business Site Administrator.

Appendix B - Administrative Permissions List

Permission Name	Description	Permission Type
Administration – Pending Approvals	Allows a user to access the pending approvals page. This permission needs to be given with **Common Approver**	**Administrative**
Administration – Permissions Configuration	Allows users to view and maintain the permissions assigned in a site (this permission does not allow user to approve creation of permissions)	**Administrative**
Administration – Alias Configuration	Allows a user to configure the alias or nickname of a product	**Administrative**
Administration – Approval Schemes	Allows users to view and maintain the approval schemes defined in a site	**Administrative**
Administration – Transaction Amounts	Allows users to view and maintain the daily amount of site (this permission does not allow user to approve modification of limits)	**Administrative**
Administration – Users	Allows users to view and manage users of a site (this permission does not allow user to approve creation or edition of users)	**Administrative**
Administration – Utility Payment Subscription	Allows the user to administer subscriptions to utility payments	**Administrative**
Administration - Payroll	Allows users to administer (view, add, amend etc.) the payrolls of a site	**Administrative**
Administration - Suppliers	Allows users to administer (view, add, amend etc.) the suppliers of a site	**Administrative**
Administration – Audit and Logs	Allows the user to access the audit log	**Administrative**
Administration – Third-Party Products	Allows users to administer (view, add, amend etc.) the beneficiaries of a site	**Administrative**
Administration - Scheduled Transactions	Allows the user to administer (view, add, amend etc.) the scheduled transactions created in a site. The user needs to at least have **one transaction permission** over a **product**.	**Administrative**

Appendix C - Product Permissions List

Permission Name	Description	Permission Type
Account – Details	Allows users to view the detail of a saving or checking account	**Product** (Chequing or Saving)
Account – Statements	Allows users to view the statements of a saving or a checking account	**Product** (Chequing or Saving)
Account – Transaction History	Allow users to view the account transaction history for checking and saving accounts	**Product** (Chequing or Saving)
Card – Block Cards	Allows users to block or unblock a card (debit or credit)	**Product** (Credit Card, Chequing or Saving)
Card – Block Cards	Allows users to block a credit card	**Product** (Credit Card)
Credit Card - Current Transactions	Allows users to view the current movements of a credit card	**Product** (Credit Card)
Credit Card – Details	Allows users to view the details of a credit card	**Product** (Credit Card)
Credit Card – Statements	Allows users to view the statement of a credit card	**Product** (Credit Card)
Credit Card - Pending Transactions	Allows users to view the pending movements of a credit card	**Product** (Credit Card)
Fixed Term Deposit – Details	Allows users to view the detail of a fixed term deposit	Account (Certificate of Deposit)
Loan – Details	Allows users to view the detail of a loan	**Product** (Credit Card)
Loan – Payment Details	Allows users to view the payment details of a loan	**Product** (Chequing or Saving)
Investment – Details	Allows users to view investment information	**Product** (Investment)
Payment – Your Credit Card	Allows the user to create credit card payments debiting from a saving or checking account selected in the previous step	**Product** (Chequing or Saving)
Payment – Your Credit Card History	Allows users to view all credit card payments debited from a CA or SA	**Product** (Chequing or Saving)
Payment – Loan	Allows the user to create loan payments debiting from a saving or checking account	**Product** (Chequing or Saving)

Payment – Loan History	Allows users to view all loan payments debited from a CA or SA	**Product** (Chequing or Saving)
Payment – Payroll	Allows the user to create salary payments debiting from a checking or saving accounts	**Product** (Chequing or Saving)
Payment – Payroll History	Allows users to view all salary payments debited from a CA or SA	**Product** (Chequing or Saving)
Payment – Company/Utility Payments	Allows users to create utilities payments debiting from a CC, SA or CC	**Product** (Credit Card, Chequing or Saving)
Payment – Company/Utility Payments History	Allows users to view all utilities payments transfers debited from a CA, SA or CC on the online history	**Product** (Credit Card, Chequing or Saving)
Payment – Suppliers	Allows the user to create supplier payments debiting from a checking or saving accounts	**Product** (Chequing or Saving)
Payment – Suppliers History	Allows users to view all suppliers' payments debited from a CA or SA on the online history	**Product** (Chequing or Saving)
Payment - Republic Bank Credit Card	Allows the user to create payments to third party credit cards debiting from a checking or saving account on the online history	**Product** (Chequing or Saving)
Payment – Republic Bank Credit Card History	Allows users to view all third-party credit card payments debited from a CA or SA on the online history	**Product** (Chequing or Saving)
Payroll Payment – Display Payment Amounts	Allows users to view the amount that will be paid as part of a payroll payment on the online history	**Product** (Chequing or Saving)
Transfer - Between Your Own Accounts	Allows users to originate transfers between own accounts debiting from a saving or checking account	**Product** (Chequing or Saving)
Transfer - Between Your Own Accounts History	Allows users to view all own accounts transfers debited from a CA or SA on the online history	**Product** (Chequing or Saving)
Transfer - Third-Party Republic Bank Account	Allows users to originate transfers to a third-party account in Republic Bank debiting from a saving or checking account	**Product** (Chequing or Saving)
Transfer – Third-Party Republic Bank Account History	Allows users to view all transfers to third-party accounts in Republic Bank debited from a CA or SA on the online history	**Product** (Chequing or Saving)
Transfer - Third-Party Local Bank Account	Allows users to originate transfers to a third-party account in another bank in the country debiting from a saving or checking account	**Product** (Credit Card, Chequing or Saving)

Transfer – Third-Party Local Bank Account History	Allows users to view all transfers to third-party account to another bank in the country debited from a CA or SA on the online history	**Product** (Chequing or Saving)
Transfer - International Bank Account	Allows users to originate transfers to a third-party account in another country debiting from a saving or checking account	**Product** (Chequing or Saving)
Transfer – International Bank Account History	Allows users to view all transfers to third-party account to another country debited from a CA or SA on the online history	**Product** (Chequing or Saving)

Appendix D - General Permissions List

Permission Name	Description	Permission Type
Common Approver	Allows the user to be eligible to be part of an approval scheme. If a user will approve some transaction, this permission must be assigned. This permission needs to be given with **Administration – Pending Approvals**	**General**
Financial Status – Assets and Liabilities	Allows users to view this web part in the dashboard	**General**
Non Monetary Requests	Allows the user to create new service requests	**General**
Non Monetary Requests - Requests Status	Allows the user to review all the service request that were created in the site	**General**

Appendix E- Permission Templates

TEMPLATE NAME	PERMISSIONS ASSIGNED
Profile 1: Create, Approve & View	Account- Details
	Administration – Pending Approvals
	Administration – Alias Configuration
	Payment – Your Credit Card
	Payment – Credit Card History
	Payment – Loan History
	Payment – Your Loan
	Payment – Payroll History
	Payment - Payroll
	Administration – Utility Payment Subscription
	Payment – Utility History
	Payment – Company/Utility Payments
	Payment – Suppliers
	Payment – Suppliers History
	Transfer – International Bank Account
	Transfer – Third Party Accounts in Other Country History
	Transfer – Third Party Local Bank Account
	Transfer - Third Party Accounts in Country History
	Transfer - Third Party Republic Bank Account
	Transfer - Third Party Accounts in Bank History

	Transfer – Between Your Own Accounts
	Transfer – Own Accounts History
	Administration - Third Party Products
	Payment - Republic Bank Credit Card
	Common Approver
	Administration – Scheduled Transactions
	Financial Status – Assets and Liabilities
	Payment – Third-Party Credit Card History
	Account – Transaction History

TEMPLATE NAME	PERMISSIONS ASSIGNED
Profile 2: Create & View	Account- Details
	Payment – Your Credit Card
	Payment – Credit Card History
	Payment – Loan History
	Payment – Your Loan
	Payment – Payroll History
	Payment - Payroll
	Administration – Utility Payment Subscription
	Payment – Utility History
	Payment – Company/Utility Payments
	Payment – Suppliers
	Payment – Suppliers History
	Transfer – International Bank Account
	Transfer – Third Party Accounts in Other Country History
	Transfer – Third Party Local Bank Account
	Transfer - Third Party Accounts in Country History
	Transfer - Third Party Republic Bank Account
	Transfer - Third Party Accounts in Bank History
	Transfer – Between Your Own Accounts
	Transfer – Own Accounts History
	Administration - Third Party Products

	Payment - Republic Bank Credit Card
	Common Approver
	Administration – Scheduled Transactions
	Financial Status – Assets and Liabilities
	Payment – Third-Party Credit Card History
	Account – Transaction History

TEMPLATE NAME	PERMISSIONS ASSIGNED
Profile 3: Create Only	Payment – Your Credit Card
	Payment – Your Loan
	Payment - Payroll
	Administration – Utility Payment Subscription
	Payment – Company/Utility Payments
	Payment – Suppliers
	Transfer – International Bank Account
	Transfer – Third Party Local Bank Account
	Transfer - Third Party Republic Bank Account
	Transfer – Between Your Own Accounts
	Administration - Third Party Products
	Payment - Republic Bank Credit Card
	Administration – Scheduled Transactions

TEMPLATE NAME	PERMISSIONS ASSIGNED
Profile 4: View Only	Account- Details
	Payment – Credit Card History
	Payment – Loan History
	Payment – Utility History
	Transfer – Third Party Accounts in Other Country History
	Transfer - Third Party Accounts in Country History
	Transfer – Own Accounts History
	Payment – Third-Party Credit Card History
	Account – Transaction History

TEMPLATE NAME	PERMISSIONS ASSIGNED
Profile 5: Credit Card Only	Administration – Alias Configuration
	Payment – Credit Card History
	Administration – Utility Payment Subscription
	Transfer – Third Party Local Bank Account
	Transfer - Third Party Accounts in Country History
	Transfer - Third Party Republic Bank Account
	Transfer - Third Party Accounts in Bank History
	Payment – Third-Party Credit Card History
	Card- Blocked Cards

TEMPLATE NAME	PERMISSIONS ASSIGNED
Profile 6: Approve & View	Account- Details
	Administration – Pending Approvals
	Payment – Credit Card History
	Payment – Loan History
	Payment – Payroll History
	Payment – Utility History
	Payment – Suppliers History
	Transfer – Third Party Accounts in Other Country History
	Transfer - Third Party Accounts in Country History
	Transfer - Third Party Accounts in Bank History
	Transfer – Own Accounts History
	Common Approver
	Financial Status – Assets and Liabilities
	Payment – Third-Party Credit Card History
	Account – Transaction History