



**Installation of soft token application and
user guide for *Existing eBanking users***



Table of Contents

A. Installation of soft token application and registration guide for existing eBanking users (migration process)	3
B. Submission of authenticated requests using the Entrust IdentityGuard Mobile application	11
Appendix A: How to enable your “Face ID” authentication through the Entrust IdentityGuard Mobile application.....	15
Appendix B: Important Information	17



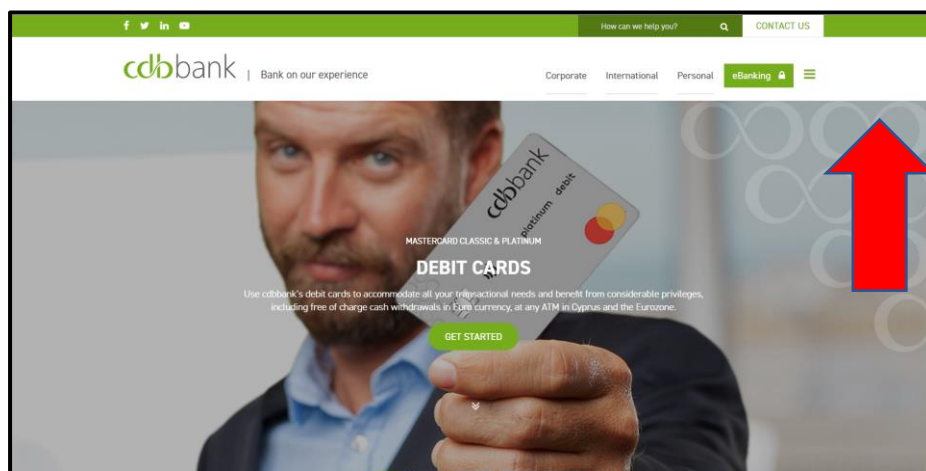
A. Installation of soft token application and registration guide for existing eBanking users (migration process)

This document explains step by step how to download and activate the Entrust IdentityGuard Mobile soft token application.

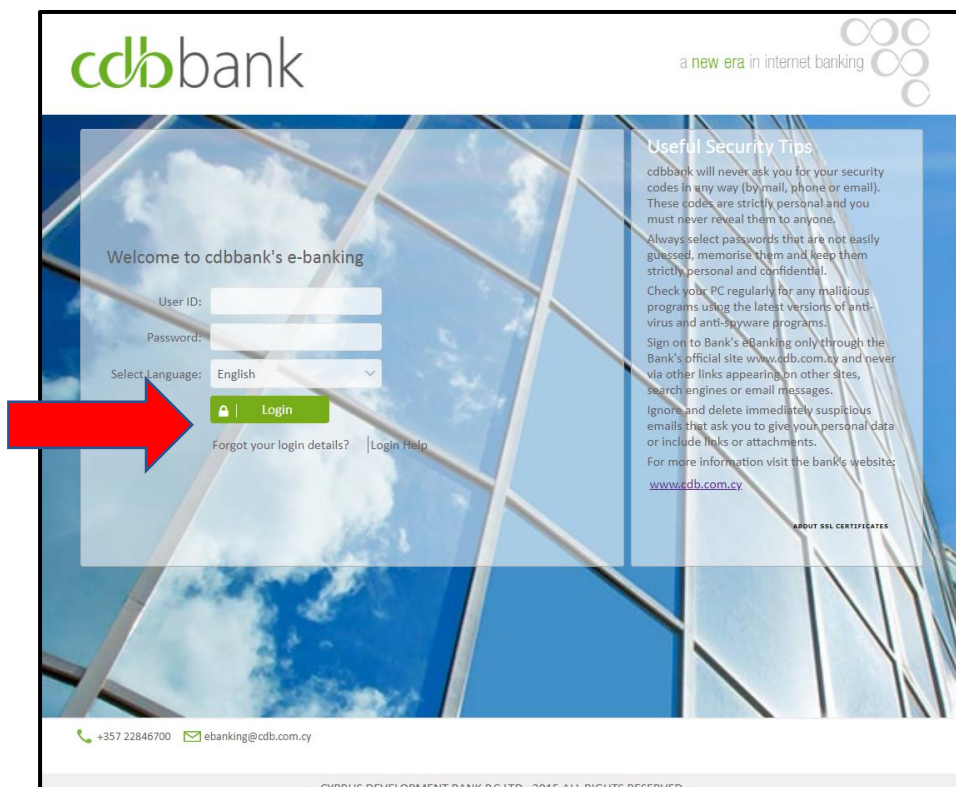
Step 1: Go to the bank’s website at www.cdb.com.cy and log-in using the



button, which is located in the upper right-hand corner.



Step 2: Enter your credentials (User ID and Password) and click on the “Login” button.





Step 3: Enter the One-Time-Password (OTP) which will be either generated from the old soft token application on your mobile device, or from your existing hard token. Users that do not currently have tokens will receive an SMS OTP.

- ✓ “Full access” users possessing a hard token:

The screenshot shows a form titled "One Time Password (OTP)". Below the title, it says "Please insert the One-Time-Password generated by your hard token device". There is a text input field with the placeholder "Insert OTP". At the bottom of the form, there are two buttons: "Logout" (grey) and "Submit" (green).

- ✓ “Full access” users possessing a mobile soft token:

The screenshot shows a form titled "Mobile OTP". Below the title, it says "Insert the One-Time-Password (OTP) generated by your soft (mobile) token below". There is a text input field with the placeholder "Insert OTP". At the bottom of the form, there are two buttons: "Logout" (grey) and "Submit" (green).

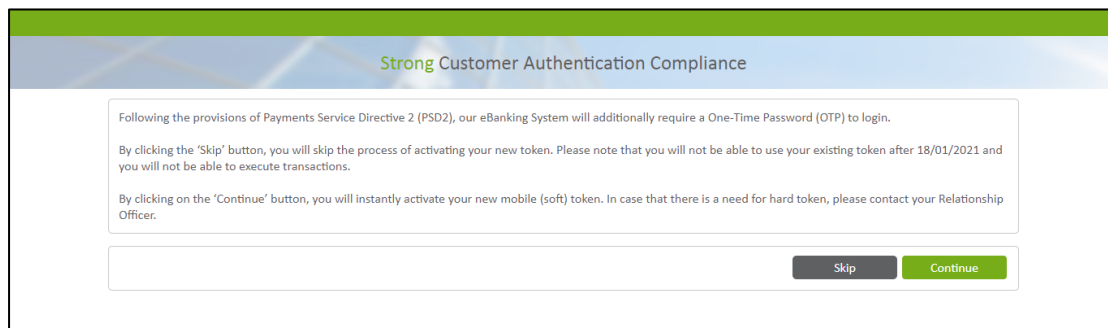
- ✓ Users who do not possess tokens, will receive an SMS OTP:

The screenshot shows a form titled "SMS OTP". Below the title, it says "Insert OTP". There is a text input field with the placeholder "Insert OTP". Below the input field is a green button labeled "Send OTP". At the bottom of the form, there are two buttons: "Logout" (grey) and "Submit" (green).

Note: The user will automatically be transferred to the ebanking homepage.



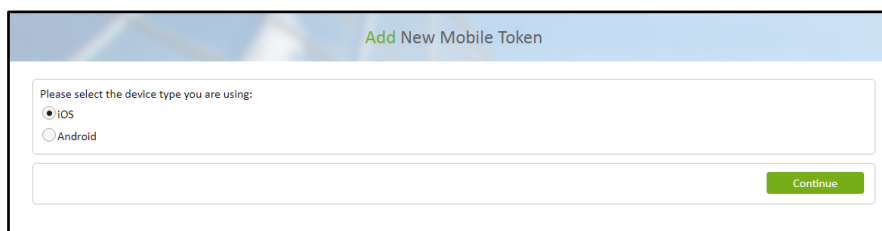
Step 4: Click on the “Continue” button, to initiate the procedure of activating your new mobile (soft) token. In cases where there is a need to continue with the use of a hard token, please contact your relationship officer to be guided accordingly.



Note: The “Skip” button can be used to postpone the soft token activation process.

Step 5: Enter the One-Time-Password (OTP) which will be either generated from the old soft token application on your mobile device, or from your existing hard token.

Step 6: Choose the type of device (i.e. iOS or Android) and then click on the “Continue” button.



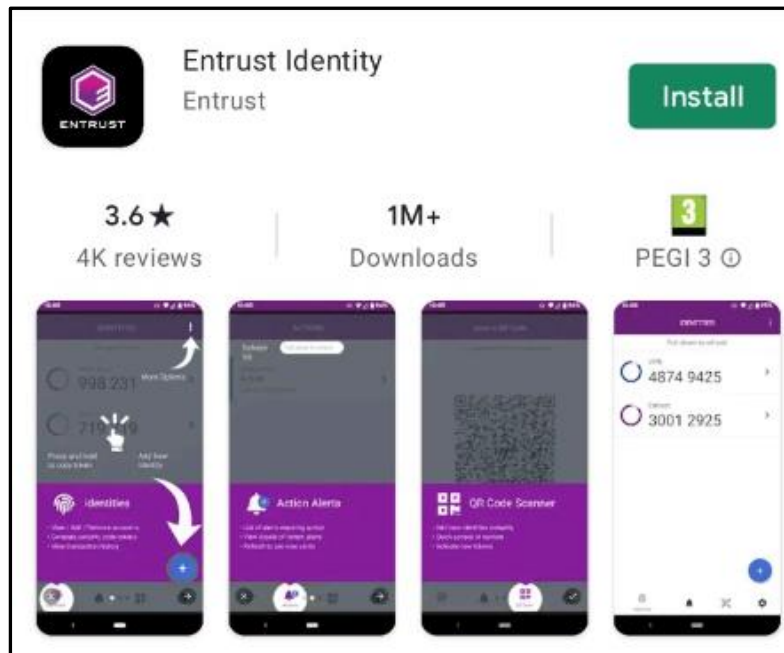
Step 7: “Add New Mobile Token” by following the two steps below:

7.1 Download the Entrust IdentityGuard Mobile application to your mobile device, by choosing any of the options of the below list:

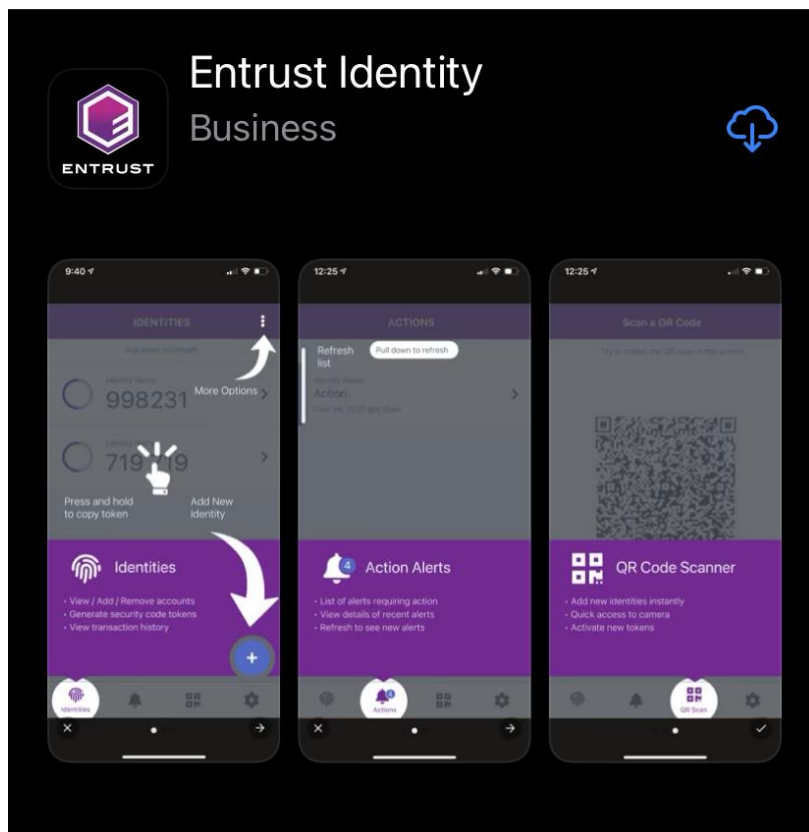
- ✓ switch on the camera on your mobile device, and then scan the QR code that appears on your eBanking screen, or
- ✓ use the link provided on your eBanking screen, or
- ✓ search the Entrust IdentityGuard Mobile application either on Apple Store or Google play as showed below:



✓ For Android Users:



✓ For iOS Users:





7.2 Insert “Alias” (i.e. friendly name) to name your device and click on the “Continue” button.

✓ **For Android users:**

✓ **For iOS users:**

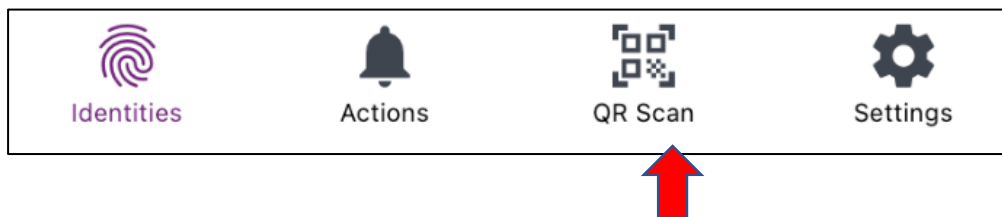
Note: If you want to go to the previous screen, click on the “Back” button.



Step 8: Enable the use of your new soft token, by following the steps below:

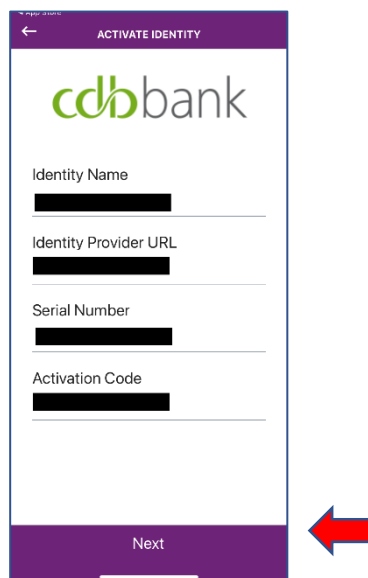
- 8.1. Open the Entrust IdentityGuard Mobile application on your mobile device
- 8.2. Use the QR Code that appears on your eBanking screen, to activate your soft token.

- ✓ Click on the QR code icon in the lower right corner of the Entrust IdentityGuard Mobile application, and then scan the QR code



- 8.3. Enter the password that appears on your eBanking screen, to the Entrust IdentityGuard Mobile application
- 8.4. Click on the “Next” button on the Entrust IdentityGuard Mobile application

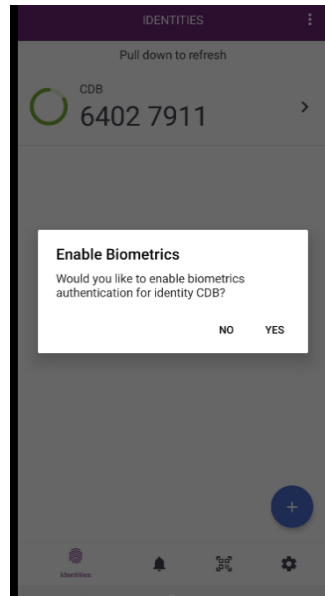
- ✓ The “Next” button is located in the bottom of the screen



- 8.5. Create a new PIN that you must use onwards to access the Entrust IdentityGuard Mobile application.



8.6 Click to the “Yes” button to enable biometrics authentication.

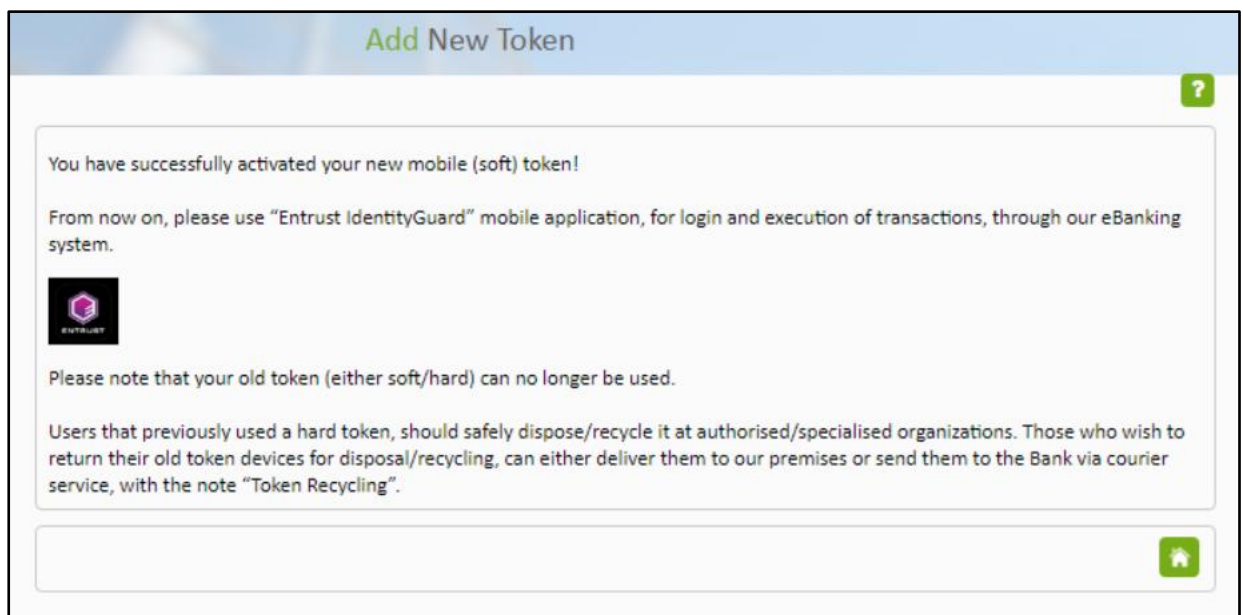


Kindly note that, you can also enable your “Face ID” authentication via the application settings once the activation process is completed, by following the instructions that are available in Appendix A.

8.7 Click on the “Homepage” button on your eBanking screen, to finalise the activation of your new soft token. Then,

8.7.1 If activation is **successful**, the below messages appear:

✓ **Your eBanking screen:**





8.7.2 If activation is **unsuccessful**, the below message appears:

✓ **Your eBanking screen:**

Add New Token

Soft Token has not been activated. Please retry to activate your token by following the below steps.

Scan the QR code above, to use the new soft token, by following the steps below:

1. Open Entrust IdentityGuard Mobile application on your device
2. Use the 'QR Code' to activate your soft token
 - o Click on the QR code icon in the lower right corner of the screen
3. Enter the password 36608293
4. Click on the "Next" button
5. Create a new PIN that you will be further using to access the application

To finalise the activation of the new Soft Token please press the 'Continue' button below.

Continue

Note: If the above message in red appeared on your screen, please make sure that you have installed and activated your mobile (soft) token.

Step 9: If the activation is successful, click on the "Homepage" button, to go to your eBanking homepage.

Add New Token

You have successfully activated your new mobile (soft) token!

From now on, please use "Entrust IdentityGuard" mobile application, for login and execution of transactions, through our eBanking system.

Please note that your old token (either soft/hard) can no longer be used.

Users that previously used a hard token, should safely dispose/recycle it at authorised/specialised organizations. Those who wish to return their old token devices for disposal/recycling, can either deliver them to our premises or send them to the Bank via courier service, with the note "Token Recycling".

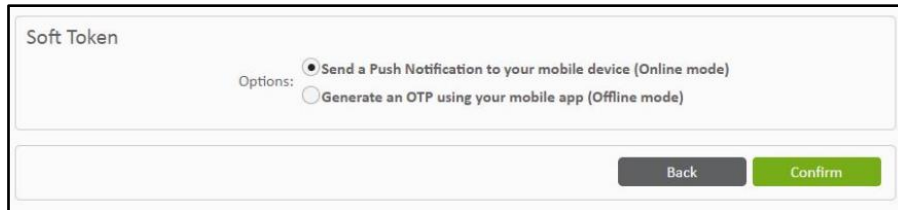
Home



B. Submission of authenticated requests using the Entrust IdentityGuard Mobile application

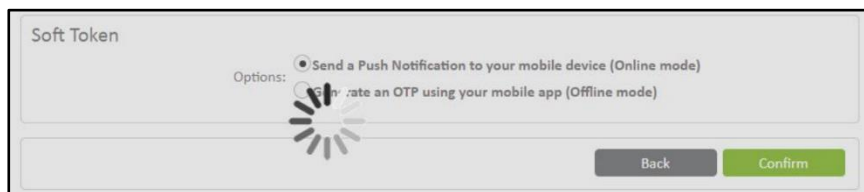
A request is successfully submitted for processing **only if an OTP is entered to verify its authenticity.**

Step 1: You have two options to proceed with the submission of your request. Select the option that suits you and follow the related steps as mentioned below:

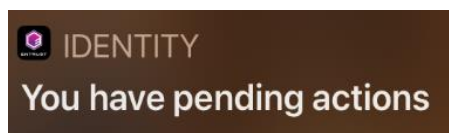


- a. If you have internet access on your mobile device (i.e. online mode), then you should follow the below steps:
 - i. Select the option “Send a Push Notification to your mobile device (Online mode)”
 - ii. Click on the “Confirm” button

✓ **Your eBanking screen:**



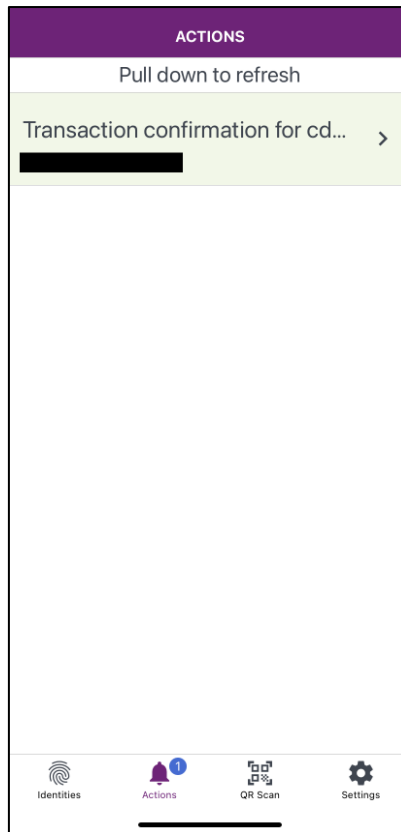
- iii. A pop-up notification will be displayed on your mobile device



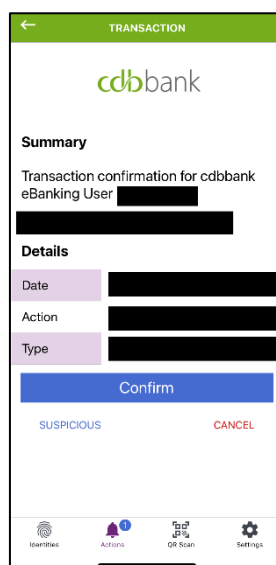
- iv. Click on the pop-up notification, and when the Entrust IdentityGuard mobile application is opened, all pending transactions appear.



- v. Click on the pending transaction(s).



- vi. Select one of the three options which are described below, by clicking on the appropriate button.



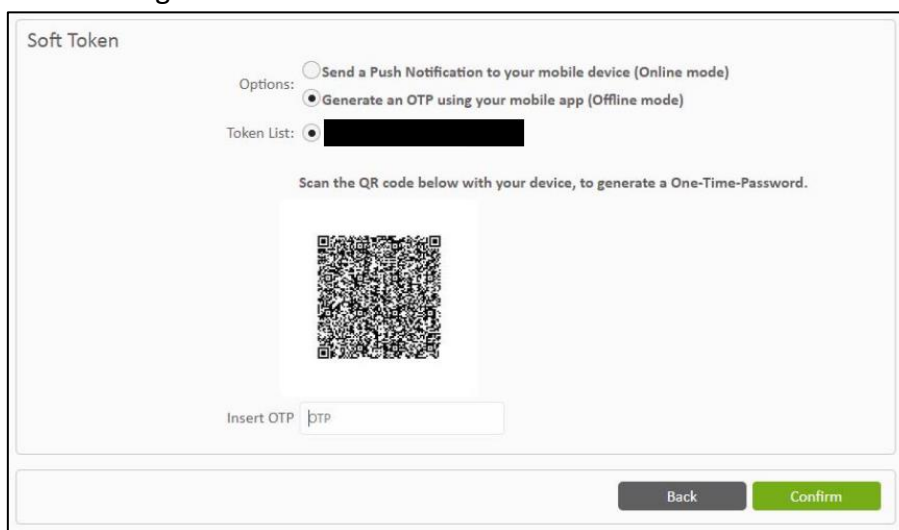


Suspicious: The “Suspicious” button should be used only in the case that the transaction that needs authorisation was not initiated by the user. This will cancel the transaction and the concern will be logged.

Cancel: The “Cancel” button is used in case of transaction cancellation. By clicking on the cancel button, you cancel the transaction.

Confirm: The “Confirm” button is used in case of transaction confirmation. By clicking on the “Confirm” button, you give confirmation for the transaction to be completed.

- b. If you **do not** have internet access on your mobile device (i.e. offline mode), then you should follow the steps below:
 - i. Select the option “Generate an OTP using your mobile app (Offline mode)”
 - ii. Switch on the Entrust IdentityGuard mobile application either on your iOS or Android device, and scan the QR code, which appears on your eBanking screen.



- iii. Enter the OTP which is generated by the Entrust IdentityGuard mobile application, on your eBanking screen.
- iv. Click on the “Confirm” button, which submits your request.



✓ **Your eBanking screen:**

Soft Token

Options: Send a Push Notification to your mobile device (Online mode)
 Generate an OTP using your mobile app (Offline mode)

Token List: [Redacted]

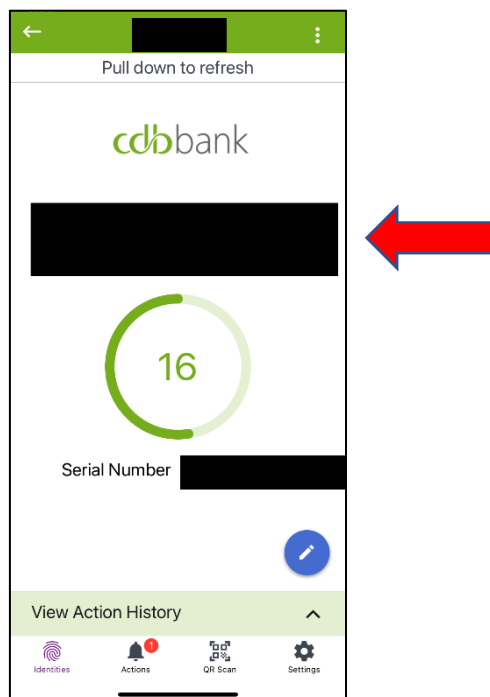
Scan the QR code below with your device, to generate a One-Time-Password.



Insert OTP: ←

Back Confirm

✓ **Your device screen:**

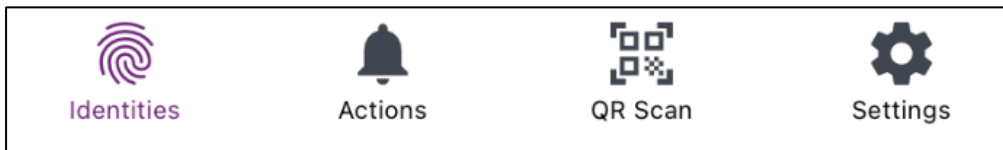




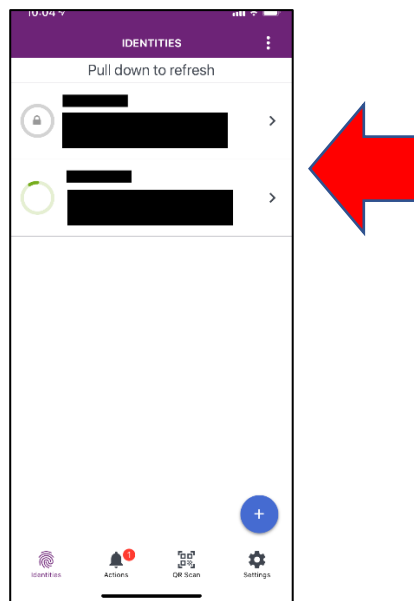
Appendix A: How to enable your “Face ID” authentication through the Entrust IdentityGuard Mobile application


Enable the authentication access with your “Face ID” on the Entrust IdentityGuard Mobile application, by following the steps below:

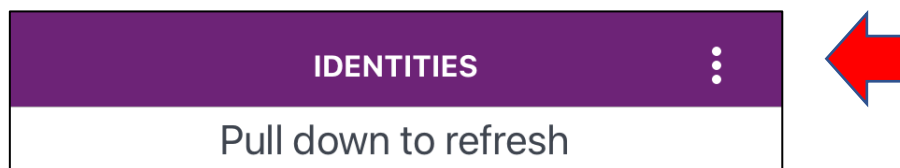
- 1.1. Open the Entrust IdentityGuard Mobile application on your mobile device
- 1.2. Insert your PIN to unlock the Entrust IdentityGuard Mobile application
- 1.3. Click on the Identities button



- 1.4. Select your token device

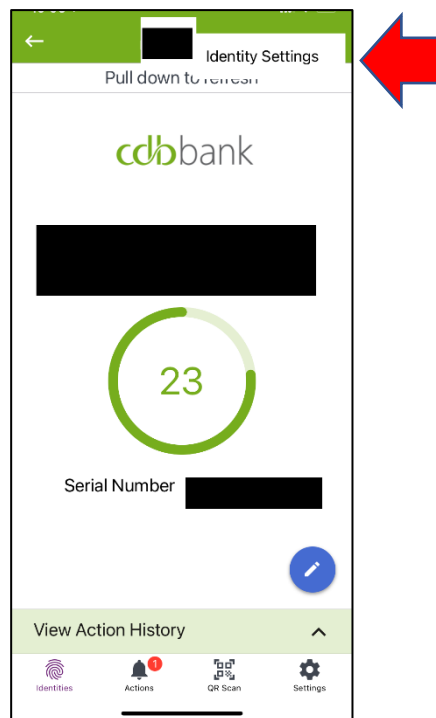


- 1.5. Click on the “Menu” button () of the Entrust IdentityGuard Mobile application

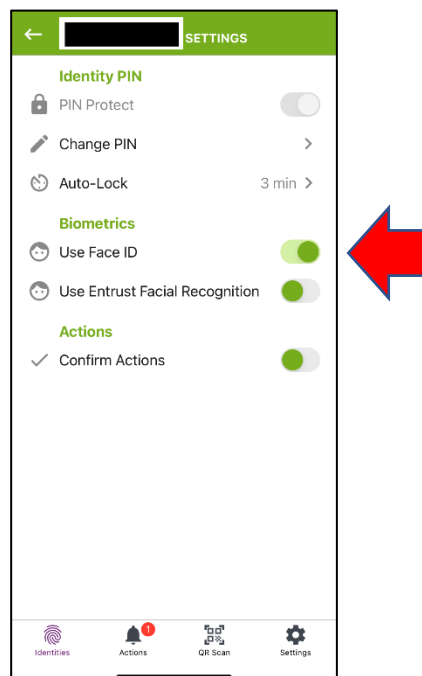




1.6. Click on the “Identity Settings” button



1.7. Enable the use of “Face ID” by clicking on the appropriate button in “Biometrics” section, and insert your PIN.





Appendix B: Important Information

- ✓ “Entrust IdentityGuard” mobile application will always be used to login and execute of transactions, through the eBanking system.
- ✓ Your old token, either soft or hard, can no longer be used.
- ✓ Users that were previously using a hard token, are advised to safely dispose/recycle it at authorised/specialised organizations. Those who wish to return their old token devices for disposal/recycling, can either deliver them to our premises or send them to the Bank via courier service, with the note “Token Recycling”.