



Soft token user guide for
NEW eBanking users



Table of Contents

A. Soft token login and registration guide for new eBanking users	3
A.1. First Login process	3
A.2 Registration process	5
A.3. Login process following the successful registration of the soft token application...	11
B. Submission of authenticated requests using the Entrust IdentityGuard Mobile application	15
Appendix A: How to enable your “Face ID” authentication through the Entrust IdentityGuard Mobile application.....	19

A. Soft token login and registration guide for new eBanking users

In order to login to cdbbank's eBanking system for the first time, you need to follow the steps below:

A.1. First Login process

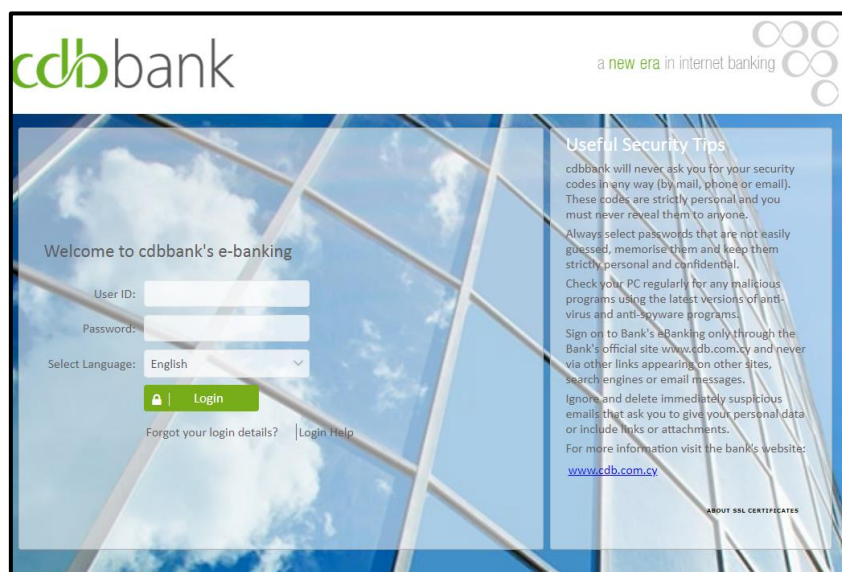
Step 1: Go to the bank's website at www.cdb.com.cy and log-in using the



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

Step 2: Enter the credentials (User ID and Password) you have received and click on the "Login" button. Your User ID has already been sent to you via e-mail and your Password via SMS to the mobile phone number you have provided the Bank.

Kindly note that the Password is case sensitive, therefore enter the digits as they appear.



Step 3: Click on the "Send OTP" button, and enter the OTP (i.e. One-Time-Password) you have received via SMS and click on the "Submit" button.



Step 4: You will be forwarded to the 'Forced Change Password' screen in order to change your password. In the field "Password" enter the password that was sent to



you via SMS. In the field “New Password” enter your new password, and in the field “Confirm New Password”, re-enter your new password.

Kindly note that Your new Password must satisfy the following criteria, which are specified by the bank:

- Must be at least 9 characters long
- At least 1 digit character
- At least 1 symbol
- At least 1 lowercase letter
- At least 1 uppercase letter

Current Password

New Password

Confirm New Password

Step 5: Select and answer three security questions and click on the “Submit” button, which takes you to your eBanking homepage.

Answer security questions

--Please Select--

▼

--Please Select--

▼

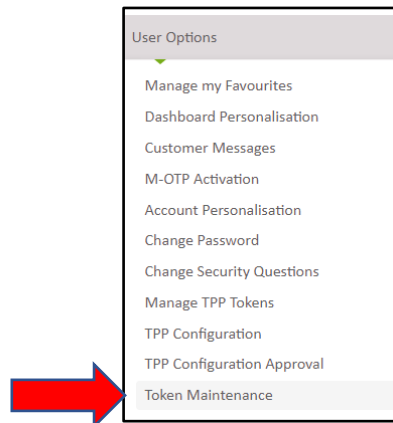
--Please Select--

▼

A.2 Registration process

In order to register your mobile device to cdbbank's eBanking system, you need to follow the steps below:

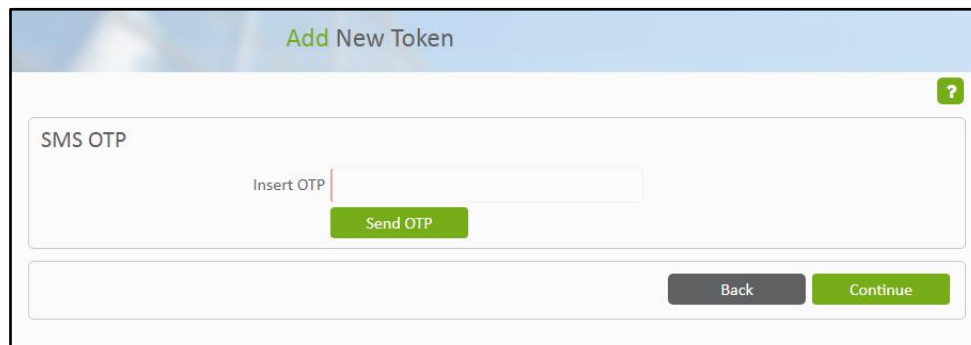
Step 1: Login to eBanking and click on "Token Maintenance" under "User Options".



Step 2: Click on the "Add New Soft Token" button.



Step 3: Click on the "Send OTP" button, enter the OTP (i.e. One-Time-Password) you have received via SMS and click on the "Continue" button.



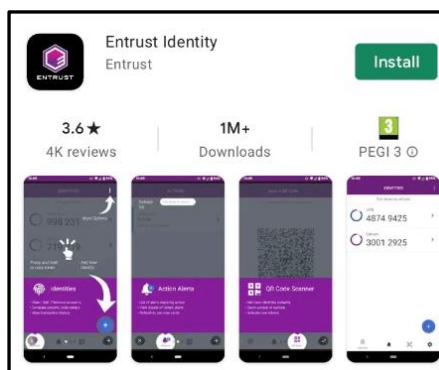
Step 4: Choose the type of device (i.e. iOS or Android) and then click on the “Continue” button.

Step 5: “Add New Mobile Token” by following the two steps below:

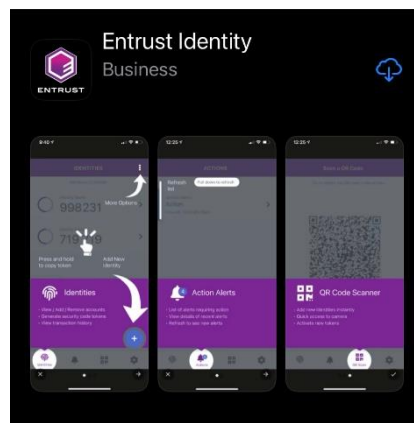
5.1 Download the Entrust IdentityGuard Mobile application to your mobile device, by choosing any of the options of the below list:

- 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:

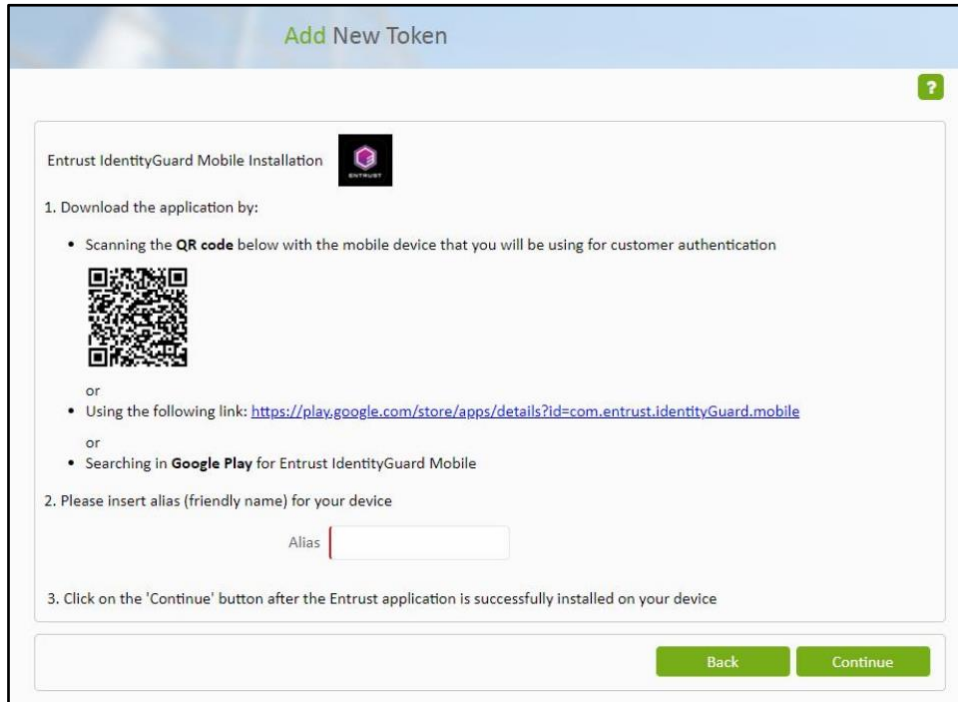


✓ For iOS Users:



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

✓ For Android users:




Add New Token

Entrust IdentityGuard Mobile Installation

1. Download the application by:

- Scanning the **QR code** below with the mobile device that you will be using for customer authentication



or

- Using the following link: <https://play.google.com/store/apps/details?id=com.entrust.identityguard.mobile>

or

- Searching in **Google Play** for Entrust IdentityGuard Mobile

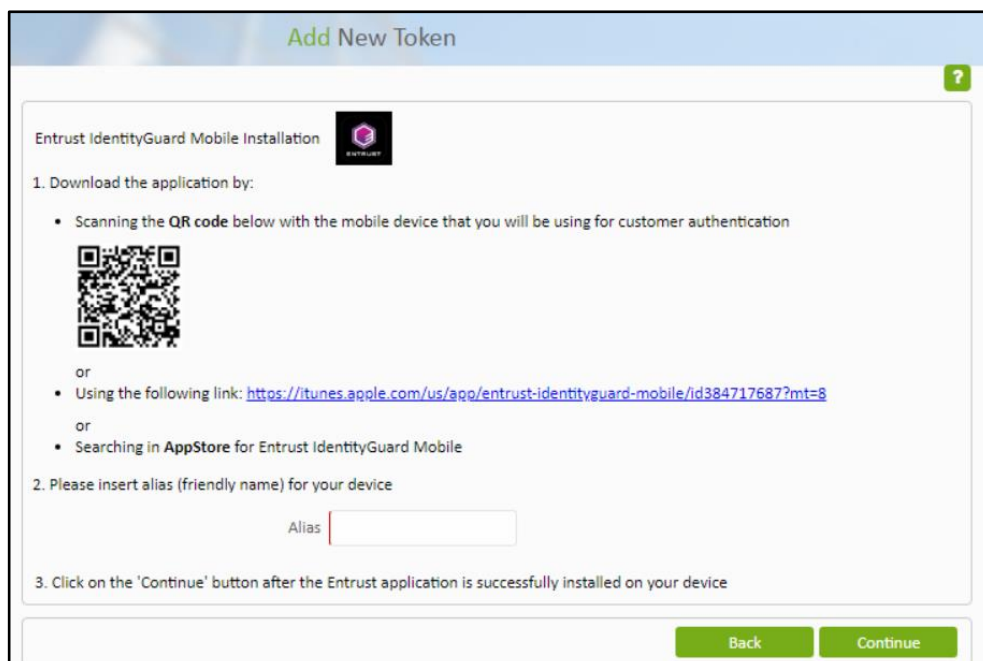
2. Please insert alias (friendly name) for your device

Alias

3. Click on the 'Continue' button after the Entrust application is successfully installed on your device

Back **Continue**

✓ For iOS users:




Add New Token

Entrust IdentityGuard Mobile Installation

1. Download the application by:

- Scanning the **QR code** below with the mobile device that you will be using for customer authentication



or

- Using the following link: <https://itunes.apple.com/us/app/entrust-identityguard-mobile/id384717687?mt=8>

or

- Searching in **AppStore** for Entrust IdentityGuard Mobile

2. Please insert alias (friendly name) for your device

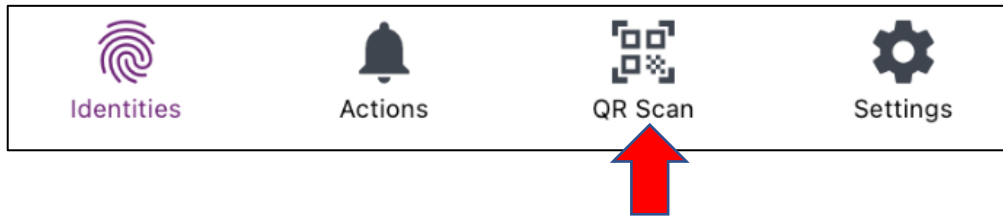
Alias

3. Click on the 'Continue' button after the Entrust application is successfully installed on your device

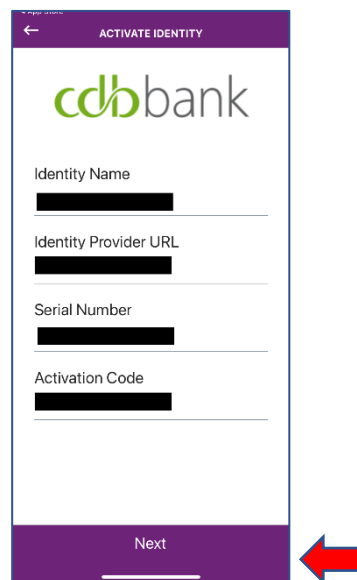
Back **Continue**

Step 6: Enable the use of your new soft token, by following the steps below:

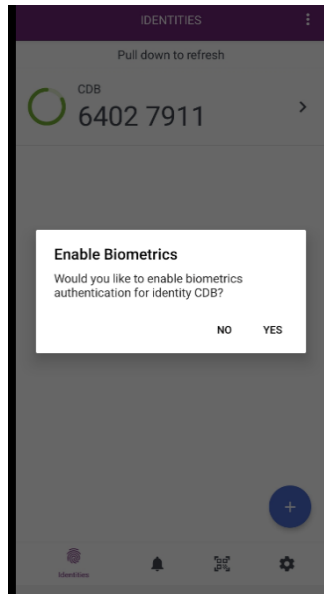
- 6.1. Open the Entrust IdentityGuard Mobile application on your mobile device
- 6.2. Use the QR Code that appears on your eBanking screen, to activate your soft token
 - ✓ Click on the QR code icon in the lower right corner of the Entrust IdentityGuard Mobile application, and then scan the QR code



- 6.3. Enter the password requested from the Entrust IdentityGuard Mobile application, which appears on your eBanking screen
- 6.4. Click on the “Next” button on the Entrust IdentityGuard Mobile application.
 - ✓ The “Next” button is located in the bottom of the screen



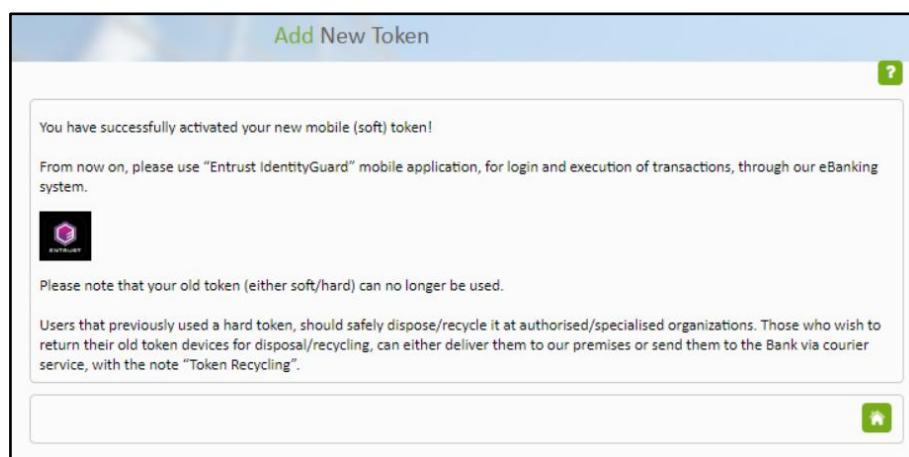
- 6.5. Create a new PIN that you must use onwards to access the Entrust IdentityGuard Mobile application.
- 6.6 Click on the “Yes” button to enable biometrics authentication.



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.

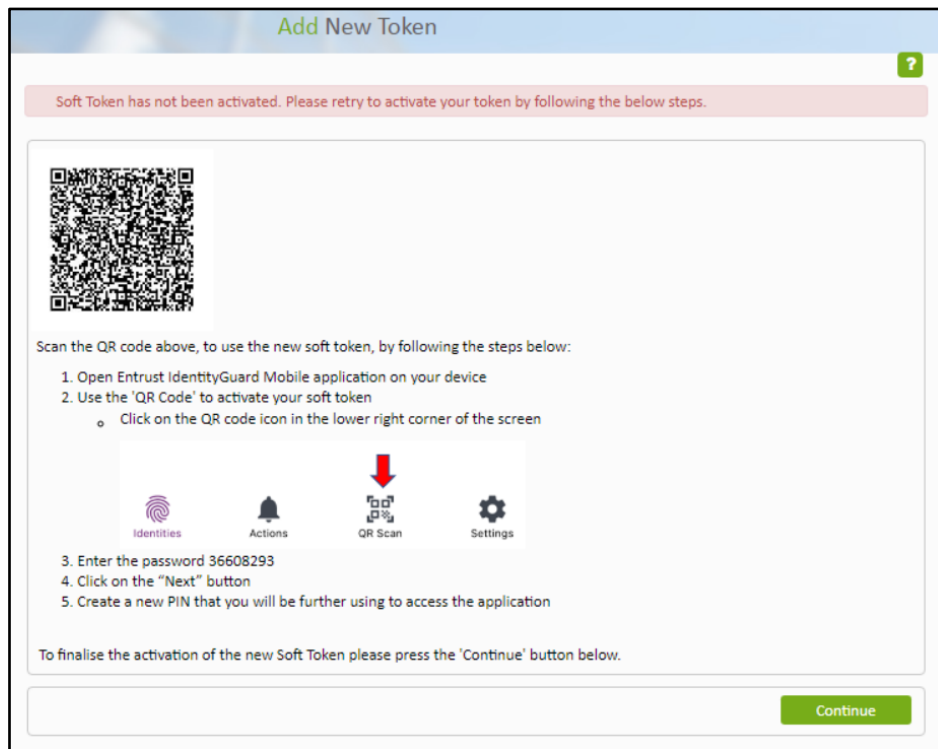
- 6.7 Click on the “Homepage” button on your eBanking screen, to finalise the activation of your new soft token. Then,
 - 6.7.1 If activation is successful, the below messages appear:

✓ **Your eBanking screen:**



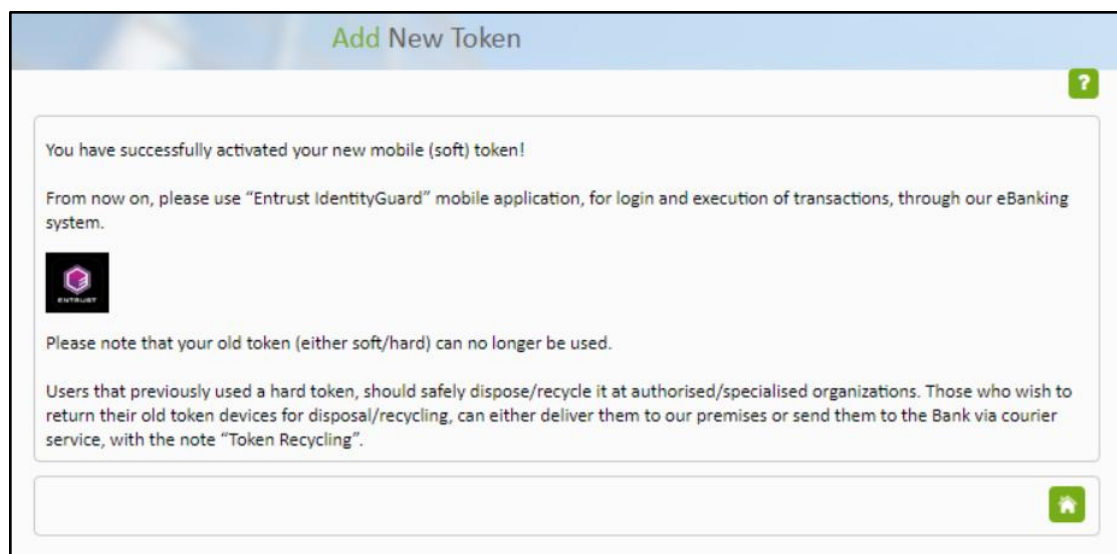
6.7.2 If activation is unsuccessful, the below message appears:

✓ **Your eBanking screen:**




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

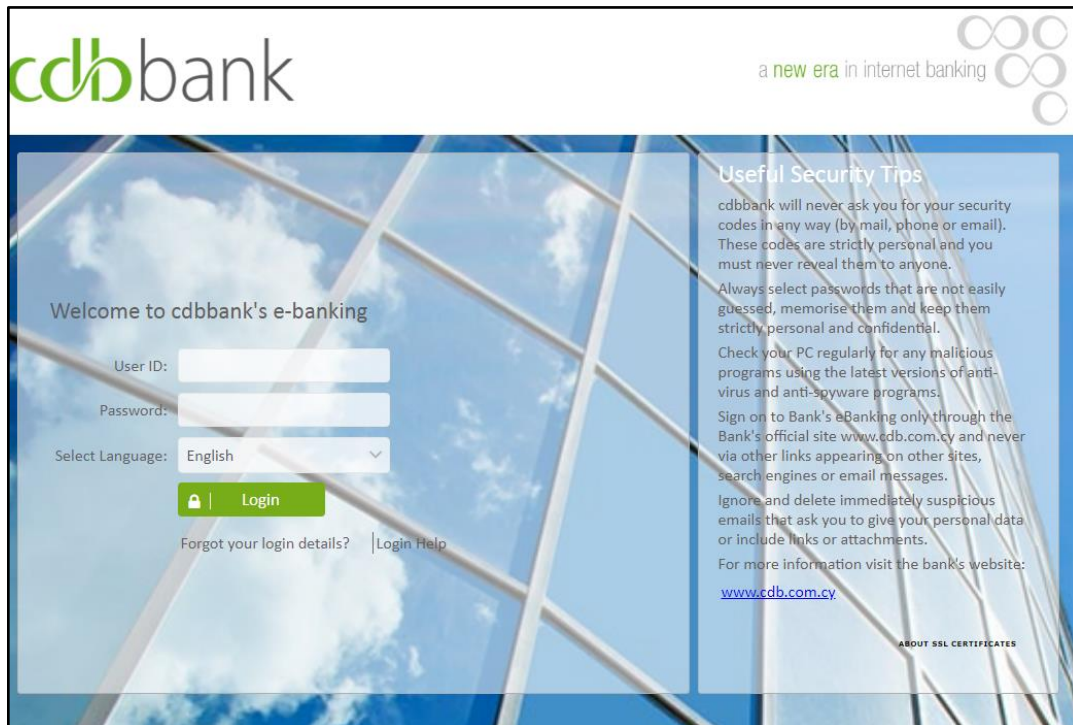
Step 7: If the activation is successful, click on the “Homepage” button, to go to your eBanking homepage.



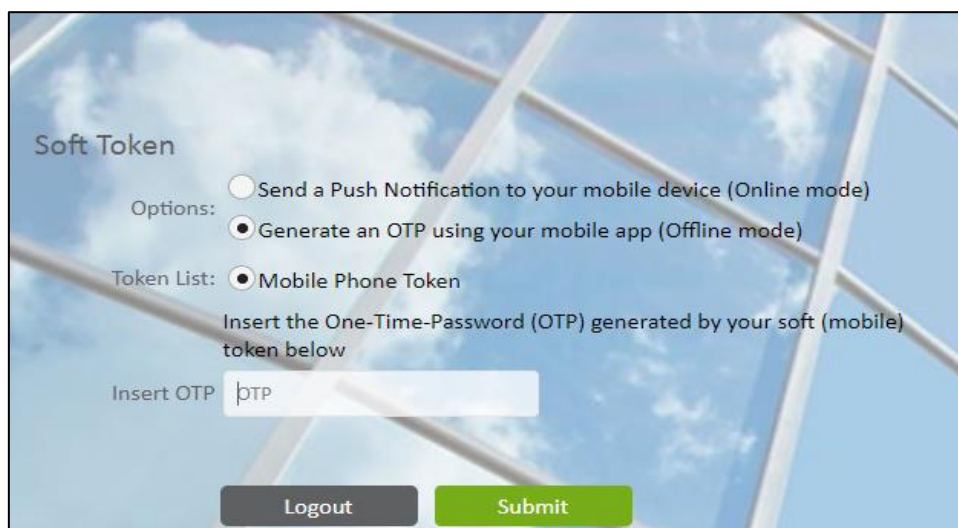
A.3. Login process following the successful registration of the soft token application

Step 1: Go to the bank's website at www.cdb.com.cy and log-in using the **eBanking**  which is located in the upper right-hand corner.

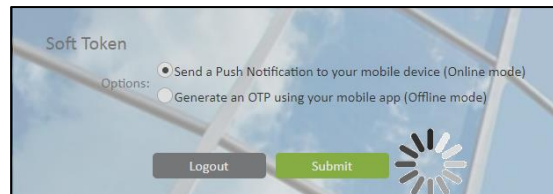
Step 2: Enter your credentials (User ID and Password) and click on the "Login" button.



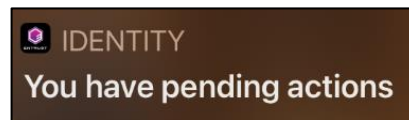
Step 3: You have two options to proceed with login. Select the option that suits you and follow the related steps as these are mentioned below:



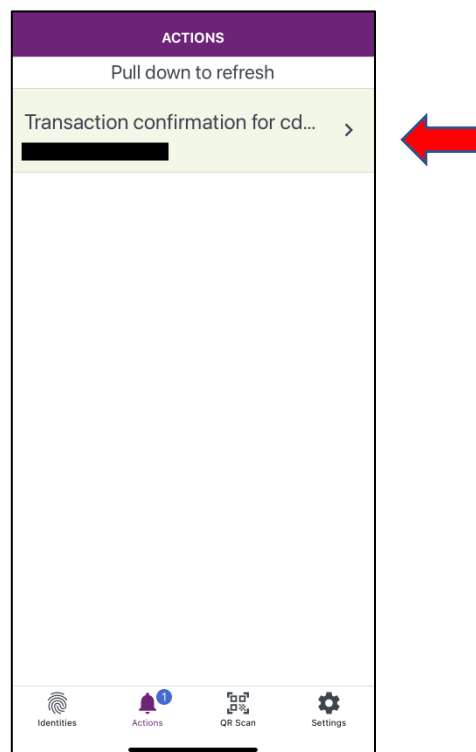
- a) If you have internet access on your mobile device (**i.e. online mode**), then you should follow the below steps:
 - i. Select the option “Send a Push Notification to your mobile device (Online mode)”
 - ii. Click on the “Submit” button
 - ✓ *Your eBanking screen:*



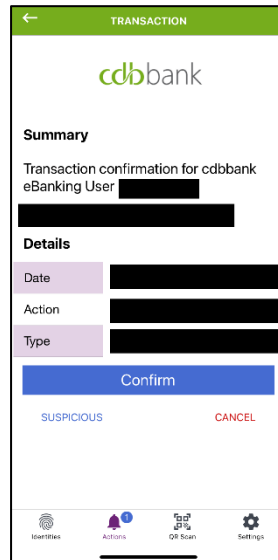
- iii. A pop-up notification is displayed on your mobile device



- iv. Click on the pop-up notification, and when the Entrust IdentityGuard mobile application is opened, all the 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 only be used 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.

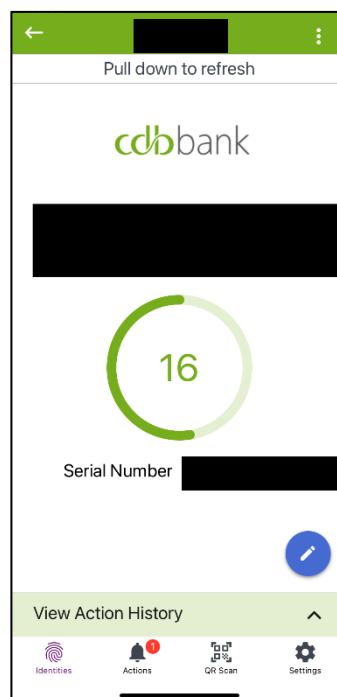
Cancel: The “Cancel” button is used in case of access cancellation. By clicking on the “Cancel” button, you cancel the user access.

Confirm: The “Confirm” button is used in case of access confirmation. By clicking on the “Confirm” button, you give access to the user.

- 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 your Entrust IdentityGuard mobile application either on iOS or Android device and enter to your eBanking screen the 8-digits OTP, which instantly appears on your mobile device.
 - iii. Click on the “Homepage” button on your eBanking screen, which takes you to your eBanking homepage.
 - iv. Click on the “OK” button on your mobile device.

✓ **Your eBanking screen:**

✓ **Your device screen:**



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.**

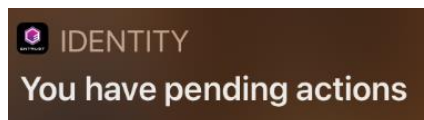
Step 1: You have two options to proceed with the submission of your request. Select the option that suits you and follow the related steps as mentioned below:

a. If you have internet access on your mobile device (i.e. online mode), then you should follow the below steps:

- vii. Select the option “Send a Push Notification to your mobile device (Online mode)”
- viii. Click on the “Confirm” button

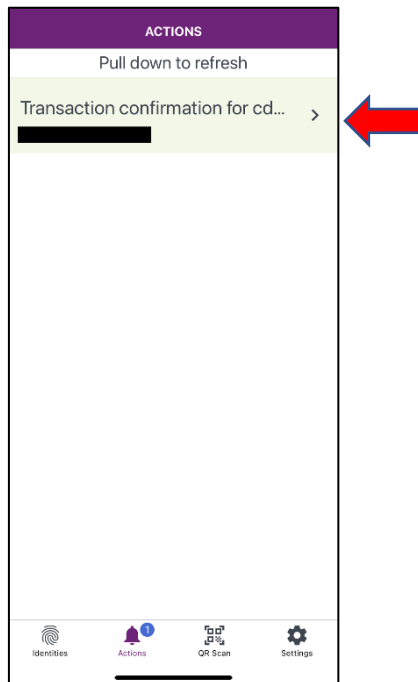
✓ Your eBanking screen:

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

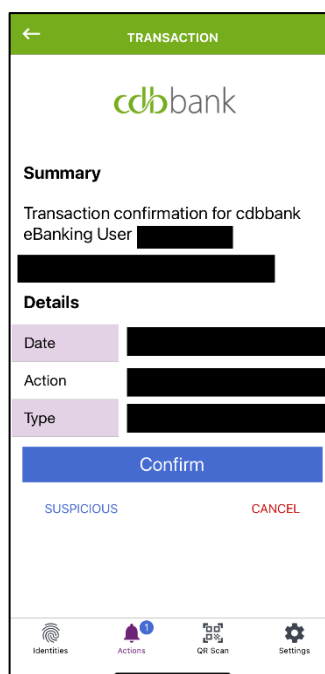


x. Click on the pop-up notification, and when the Entrust IdentityGuard mobile application is opened, all pending transactions appear.

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



- xii. 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:
- Select the option “Generate an OTP using your mobile app (Offline mode)”
 - 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.

Soft Token

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

Token List:
☒ XXXXXXXXXX

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



Insert OTP

Back

Confirm

- Enter the OTP which is generated by the Entrust IdentityGuard mobile application, on your eBanking screen.
- 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:**

← [Redacted] ⋮

Pull down to refresh

Serial Number [Redacted]

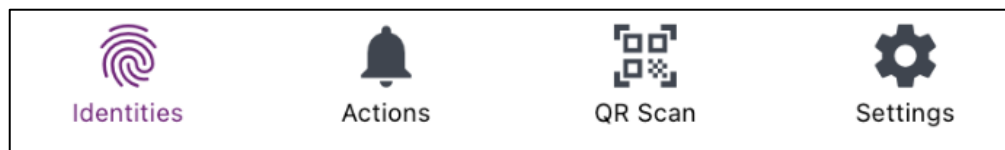
View Action History ^

Identities Actions QR Scan Settings

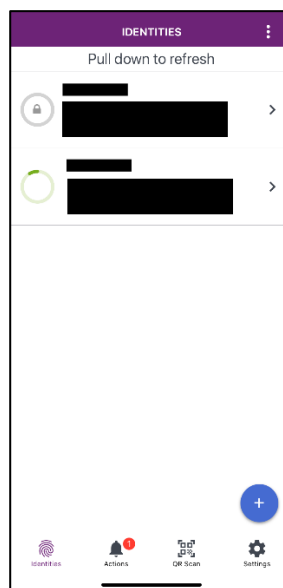
Appendix A: How to enable your “Face ID” authentication through the Entrust IdentityGuard Mobile application


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

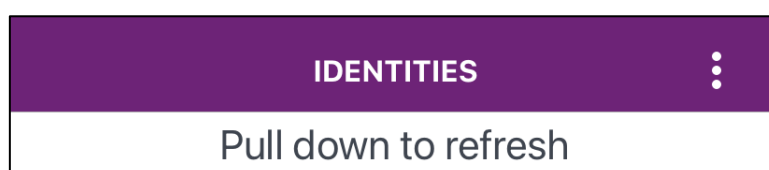
- 1.1. Open the Entrust IdentityGuard Mobile application on your mobile device
- 1.2. Insert your PIN to unlock the Entrust IdentityGuard Mobile application
- 1.3. Click on the Identities button



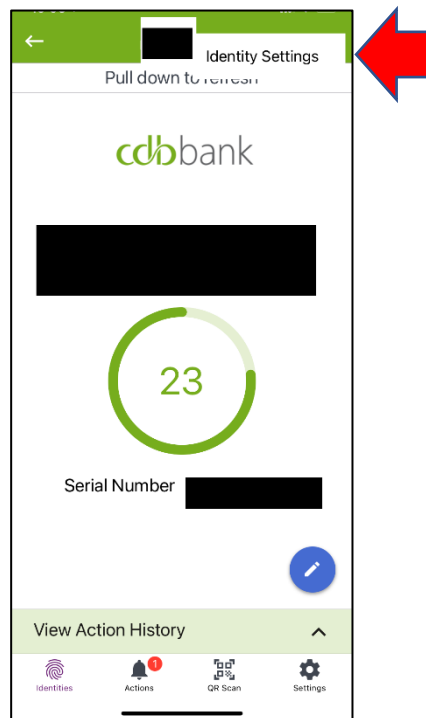
- 1.4. Select your token device



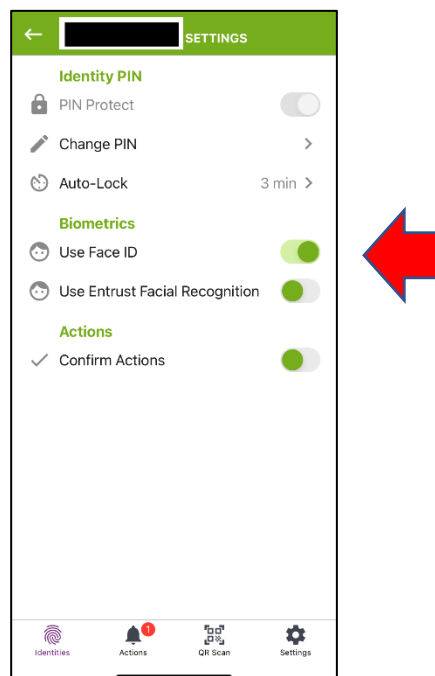
- 1.5. Click on the “Menu” button () of the Entrust IdentityGuard Mobile application



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: Useful Security Tips

- ✓ cdbbank will never ask you for your security codes in any way (by mail, phone or email). These codes are strictly personal, and you must never reveal them to anyone.
- ✓ Always select passwords that are not easily guessed, memorise them and keep them strictly personal and confidential.
- ✓ Check your PC regularly for any malicious programs using the latest versions of anti-virus and anti-spyware programs.
- ✓ Sign on to Bank's eBanking only through the Bank's official site www.cdb.com.cy and never via other links appearing on other sites, search engines or email messages.
- ✓ Ignore and delete immediately suspicious emails that ask you to give your personal data or include links or attachments.
- ✓ For more information visit the bank's website: www.cdb.com.cy