OPENOTP TOKEN MOBILE APPLICATION

OpenOTP Token Mobile Application

iOS Android Token

1. Background

OpenOTP Token is a mobile authentication solution available on iPhone and Android systems that provides secure access for websites, VPNs, Citrix, Cloud Apps, Windows, Linux, SAML, OpenID, Wi-Fi and much more. With OpenOTP Authentication Server, it provides the most advanced user authentication system supporting simple registration with QRCode scan, Software Token based on OATH standards and Approve/Deny login with push notifications.
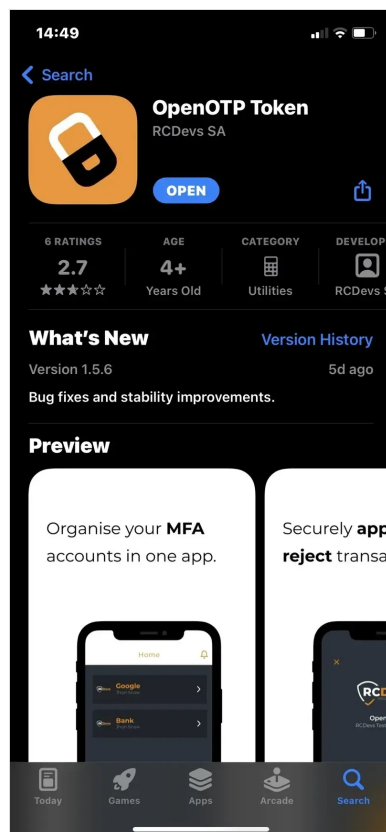
> ⚠ **Minimal OS versions**
>
> › iOS : 10.0 and later
>
> › Android : 6.0 and later

2. How To Install OpenOTP Token

2.1 iPhone / iPad

From your iOS devices, open the App Store application, look for OpenOTP Token and click on the download icon.
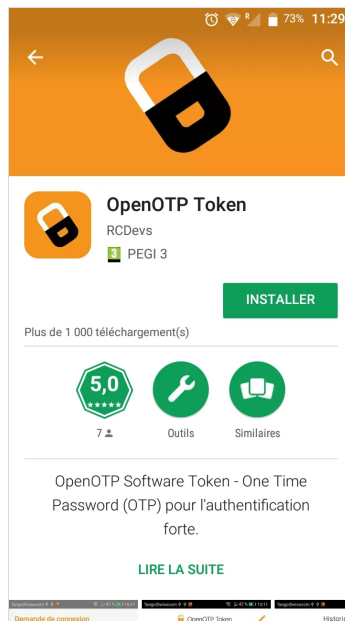
After application installation, click on the application icon on your smartphone to open it.

2.2 Android

From your Android devices, open the Google Store application, look for OpenOTP Token and click on the installation icon.

After application installation, click on the application icon on your desktop to open it.
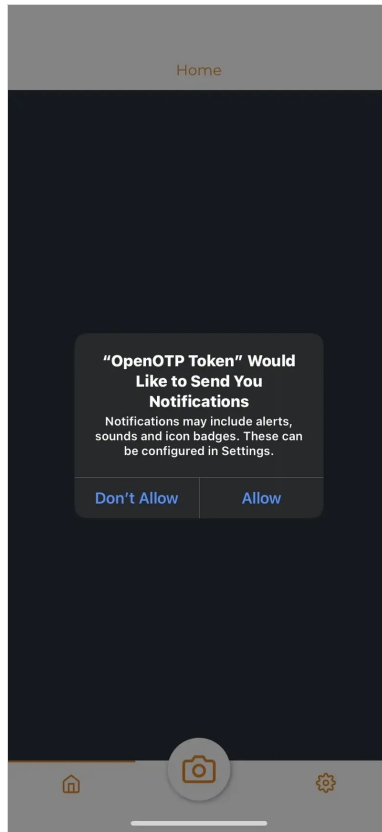

3. First Start of OpenOTP Token Application

When you run the application for the first time, you are prompted for authorizations required by the application.
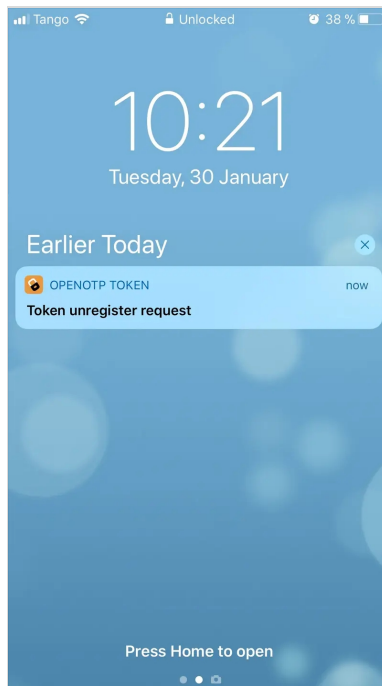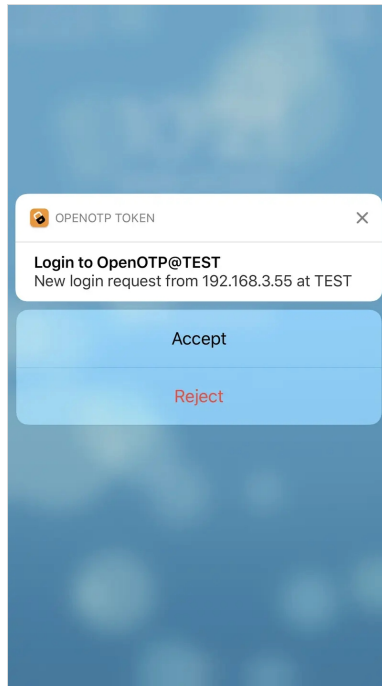
The first authorization is to allow OpenOTP Token to access your location for Anti Phishing protection. Press on Allow button to improve security.
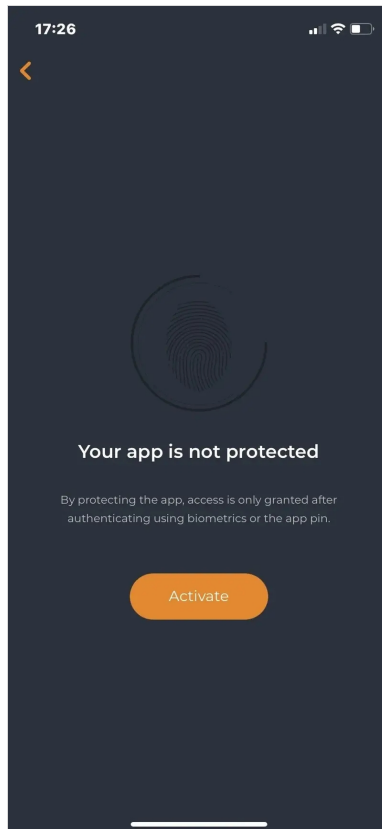
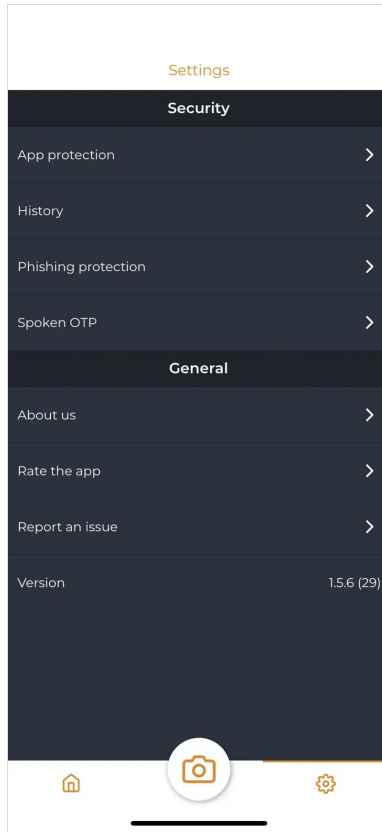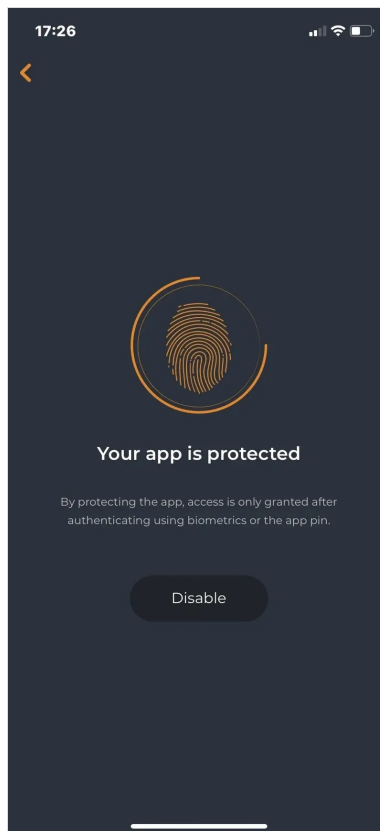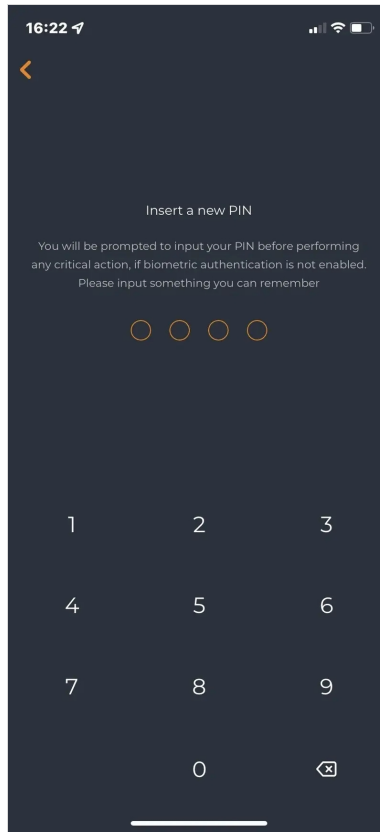The next authorization screen is for Notifications.

Notifications are used for the Push Login requests with the *Approve/Deny* button and push Token removal through the WebADM Admin GUI.
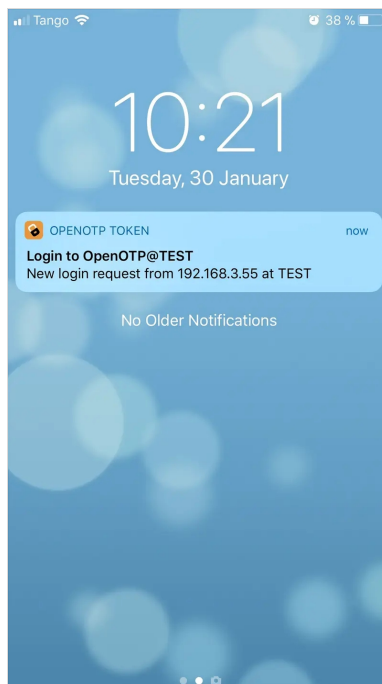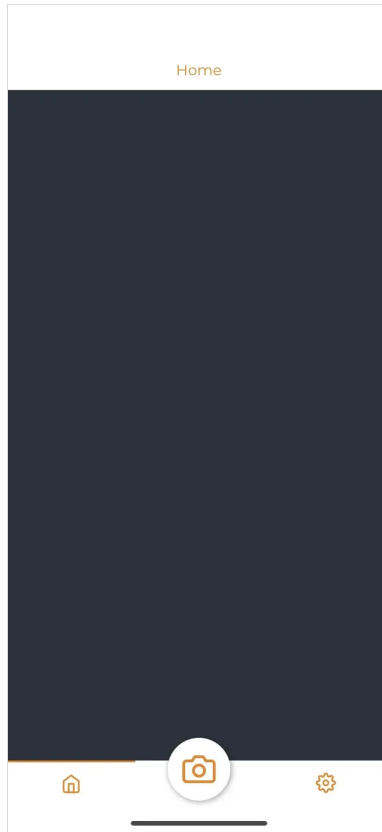
Authorizations are done for now. On the next screen, you will be able to set a password to protect the application. Enter your password twice and next time you will open the Token application, the password will be asked.

Security

App protection ›

History ›

Phishing protection ›

Spoken OTP ›

General

About us ›

Rate the app ›

Report an issue ›

Version 1.5.6 (29)

17:26

‹

Your app is not protected

By protecting the app, access is only granted after
authenticating using biometrics or the app pin.

Activate

16:22

Insert a new PIN

You will be prompted to input your PIN before performing
any critical action, if biometric authentication is not enabled.
Please input something you can remember

○ ○ ○ ○

1	2	3
4	5	6
7	8	9
	0	⌫

17:26

Your app is protected

By protecting the app, access is only granted after
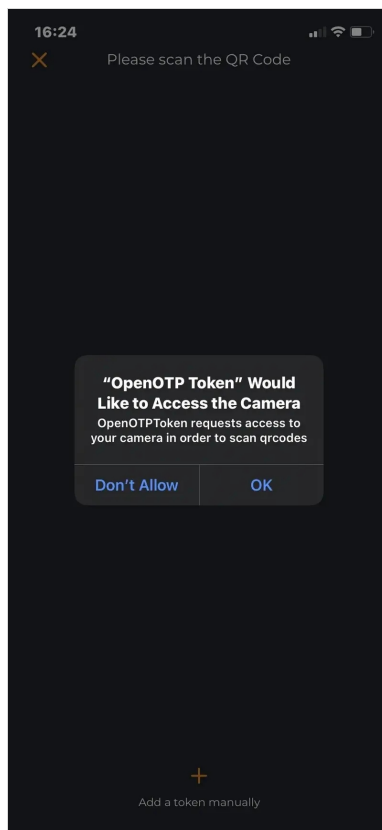authenticating using biometrics or the app pin.

Disable

You are now on the application interface.

When you will click on the camera icon, another authorization will be prompted to authorize the application to access the camera. The camera is used by OpenOTP Token to scan QR Code and enroll a new token. Click on the OK button.
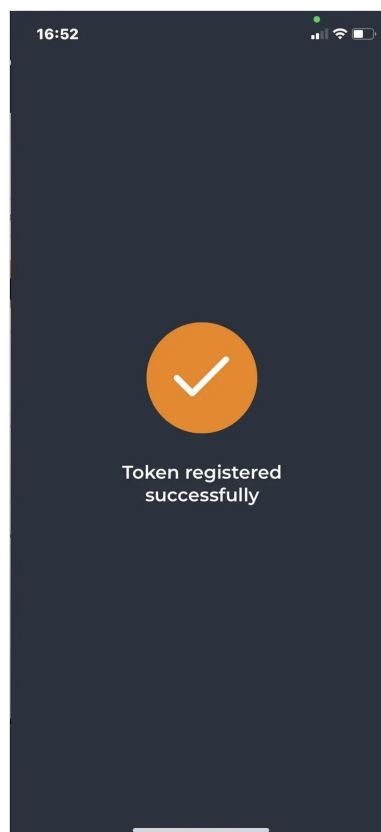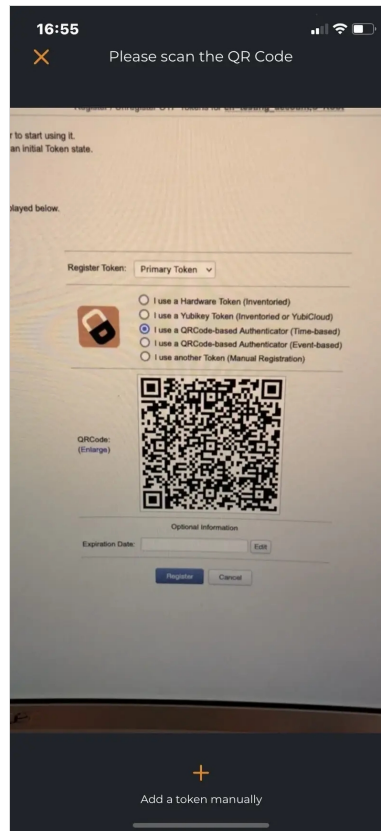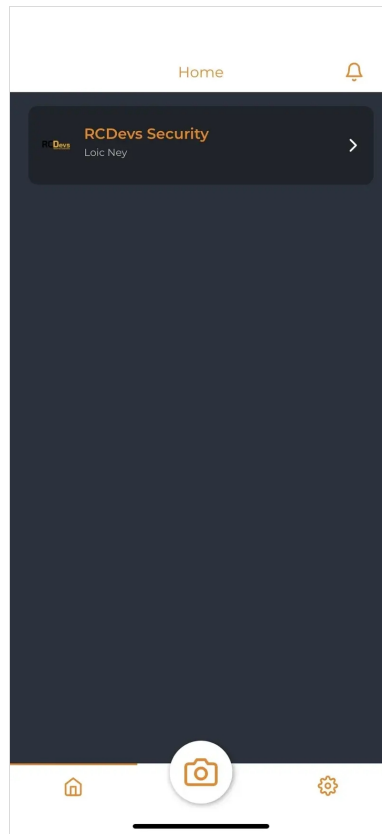
4. Token Enrollment

4.1 With a QRCode

Through the WebADM Admin GUI or Self-Services, you can enroll a Token by scanning a QR Code. When you have the QR Code on your screen, open the OpenOTP Token Application and click on the camera button. You are now able to scan the QR Code with your camera.
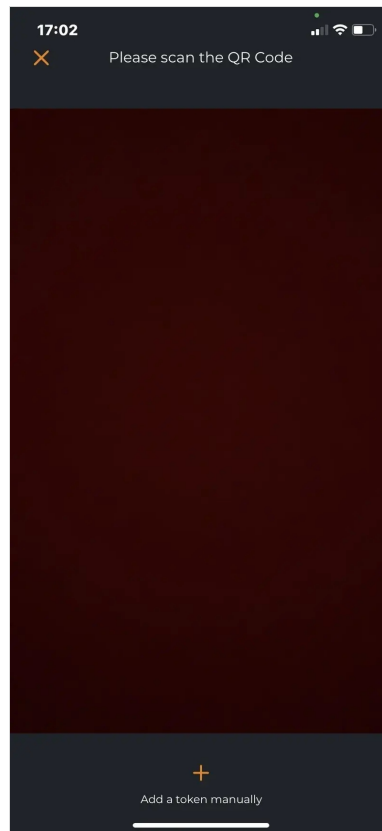
After scanning the QR Code with the application, a Token is now enrolled on your phone :

Your Token is ready to be used.

4.2 Manual Enrollment

OpenOTP Token application offers you the possibility to enroll a Token manually. On the first application screen, click on the camera button. Finally, click on the + button the bottom to enter the manual token registration mode.

Now you have to define the following settings :

› Account: This is your account name (e.g : administrator).

› Issuer: It's generally your company name.

› Algorithm: You can choose the algorithm between `SHA1` , `SHA256` or `SHA512` .

› OTP Length: 6 or 8 are the possibilities.

› Key Format: The key format is also editable between `Hexadecimal` , `Base32` & `Base64` .

› Key: This is the secret key used for codes generation.

› Time-Based: Enable this setting if you want a Token based on the Time, if this setting is not enabled, the token will be event-based.
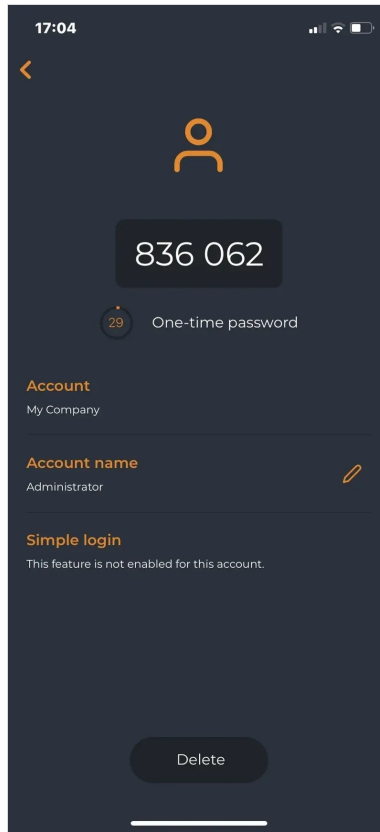
After completing the previous information, you can click on the `Save` button.
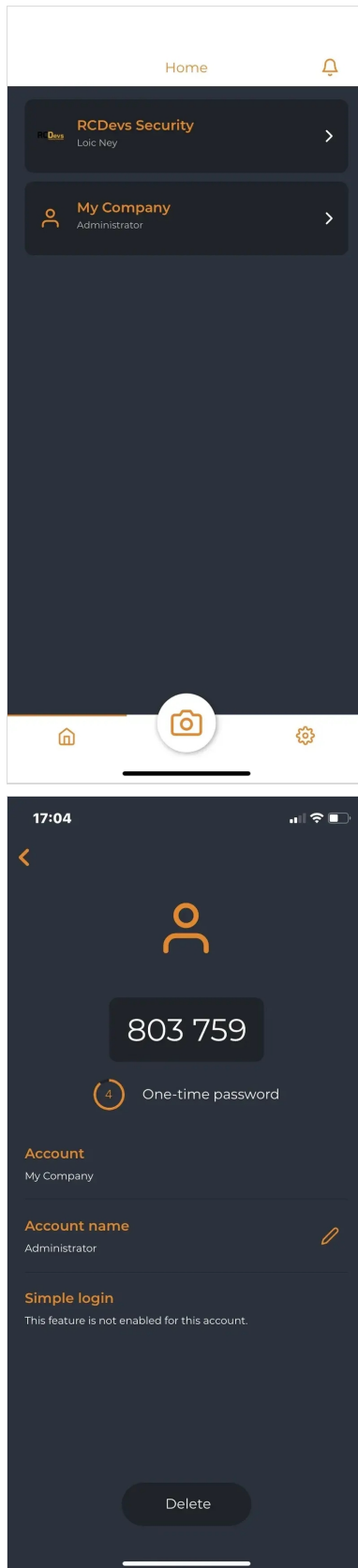
This information should be reported on the server-side to be able to use this new token.
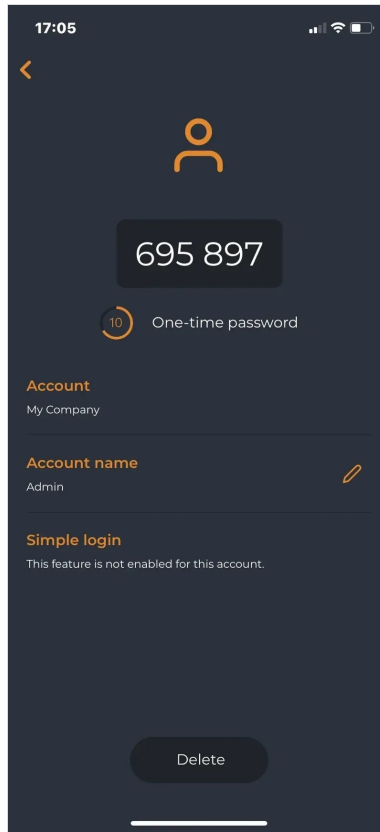
5. Token Management

When you are on the Token list screen, you can click on the pencil icon on the top right. You are now in the `Edit mode`.

Edit mode allows you to rename or remove your Token(s). If I click on the pencil icon next to a Token, I'm able to rename the Token. I will give a short name to this one:
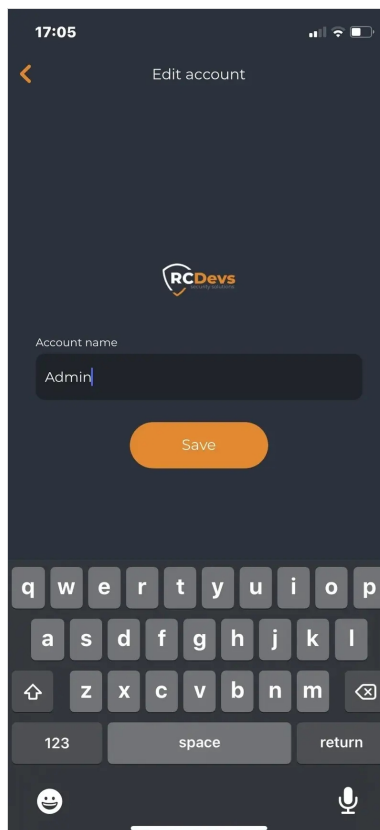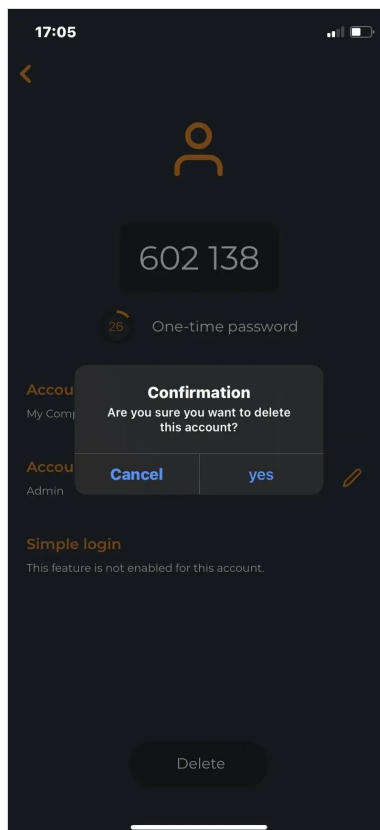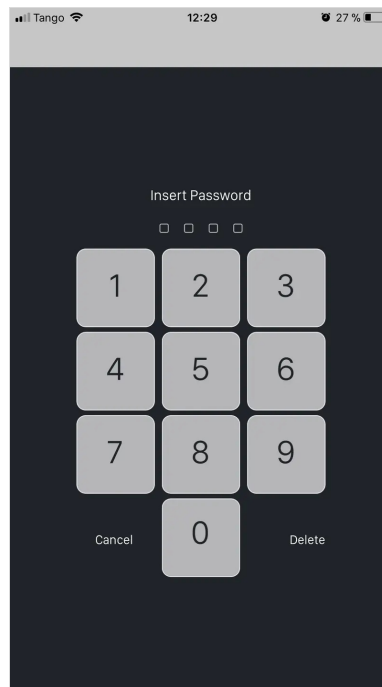

And click on the `Save` button:

Now, I can see in my Tokens list, my Token was previously renamed.

We will now remove a Token through the OpenOTP Token application. Click again on the pencil icon on the top right and enter in `edit mode` again. Select the Token you want to remove:

And click on the `Delete` button. You will be prompted to enter the passcode defined at the first start:

Enter your passcode and the Token will disappear from your Token list:
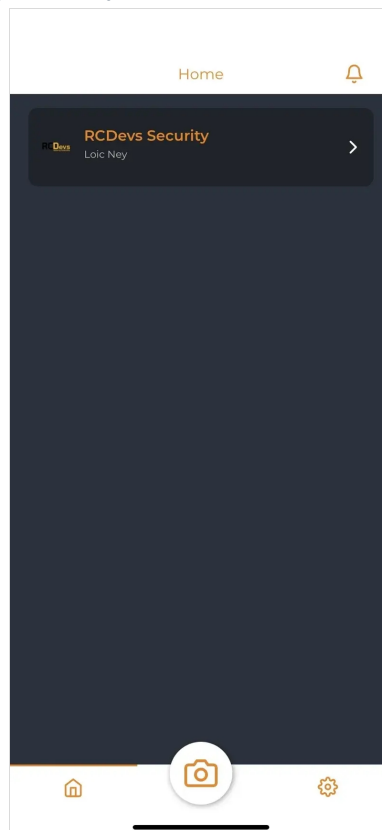
> **⚠ Note**
>
> When you remove a Token from the application, the Token is still present on the server-side of your account.

6. Application Settings

When you are in the OpenOTP Token application, some settings can be defined in the configuration menu:

› Access lock-in: This is the time after which your password will be asked to unlock the application.

› Biometric protection: Instead of using a passcode to unlock the application you can use the biometric functionality available on your phone (Touch ID or Face ID).

› OTP by voice: The OTP code will be spelled.

› Phishing protection: Phishing protection will use your location to prevent phishing attacks. If a phishing attack is suspected, the OpenOTP Token application will prompt you with a screen like below.
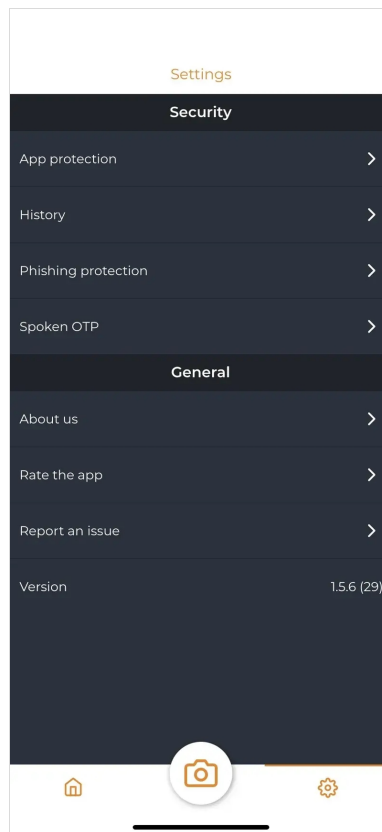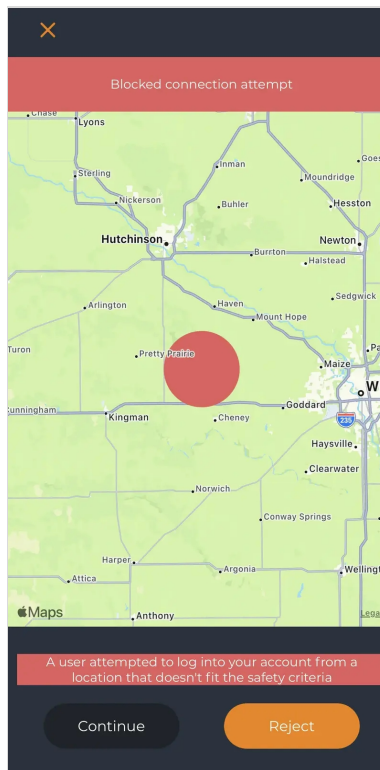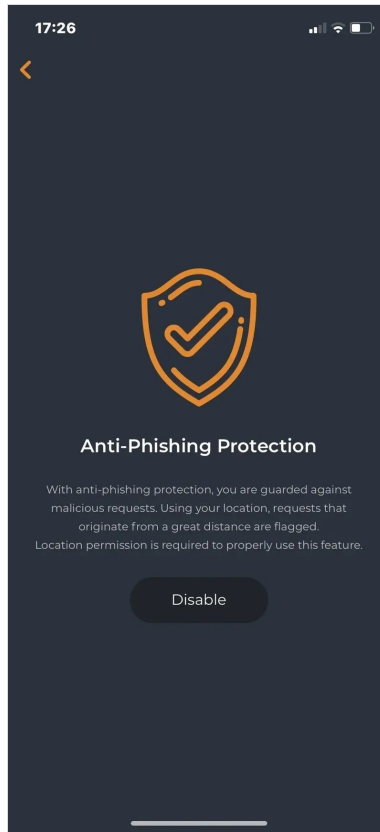
7. Application Logs

OpenOTP Token has a logging functionality to be able to review which authentication was a success or a failure on which client and at which time.
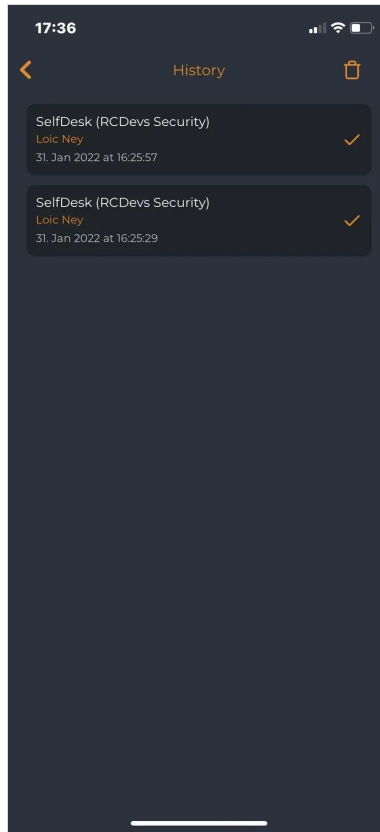
8. Offline Usage

OpenOTP Token application has an offline mode compatible with OpenOTP Credential Provider for Windows. That means, if your Windows station doesn't have any network connection or if your OpenOTP server is not available, the combination of OpenOTP Token and OpenOTP Credential Provider for Windows allows you to log in on the Windows station. You can have a look at the following documentation to have more information and to see how it works with the Credential Provider for Windows.

 Play Video on Youtube

9. Other Video Tutorials where Push Login is used

OpenOTP ADFS Plugin

 Play Video on Youtube

F5 APM BIG-IP

 Play Video on Youtube

Credential Provider for Windows Login
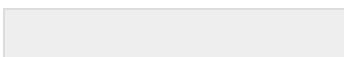
Play Video on Youtube

Custom Website

Play Video on Youtube