OPENOTP TOKEN MOBILE APPLICATION

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

OpenOTP Token Mobile Application

iOS Android Token

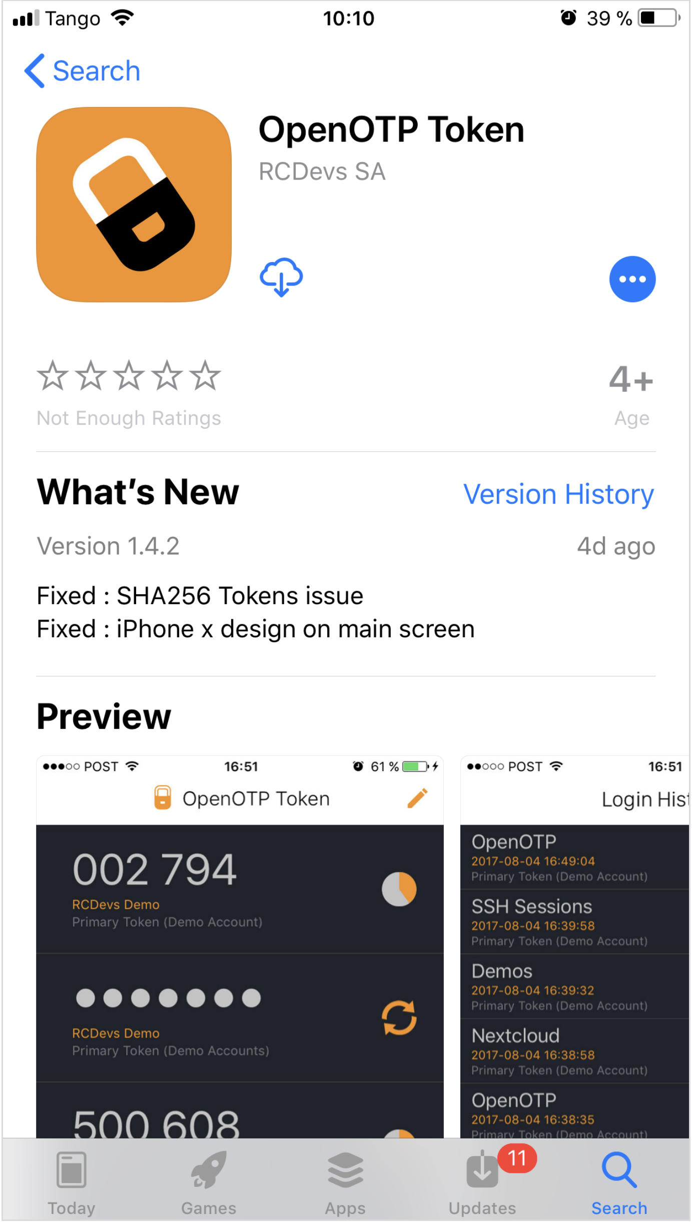
1. Background

OpenOTP Token is a mobile authentication solution available on iPhone and Android systems which provides secure access for websites, VPNs, Citrix, Cloud Apps, Windows, Linux, SAML, OpenID, Wifi 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.

2. How To Install OpenOTP Token

2.1 iPhone / iPad

From your iOS devices, open the App Store application, looking for OpenOTP Token and click on the download icon.



Tango 10:10 39 %

Search

OpenOTP Token

RCDevs SA

Not Enough Ratings

4+

Age

What's New

Version History

Version 1.4.2

4d ago

Fixed : SHA256 Tokens issue

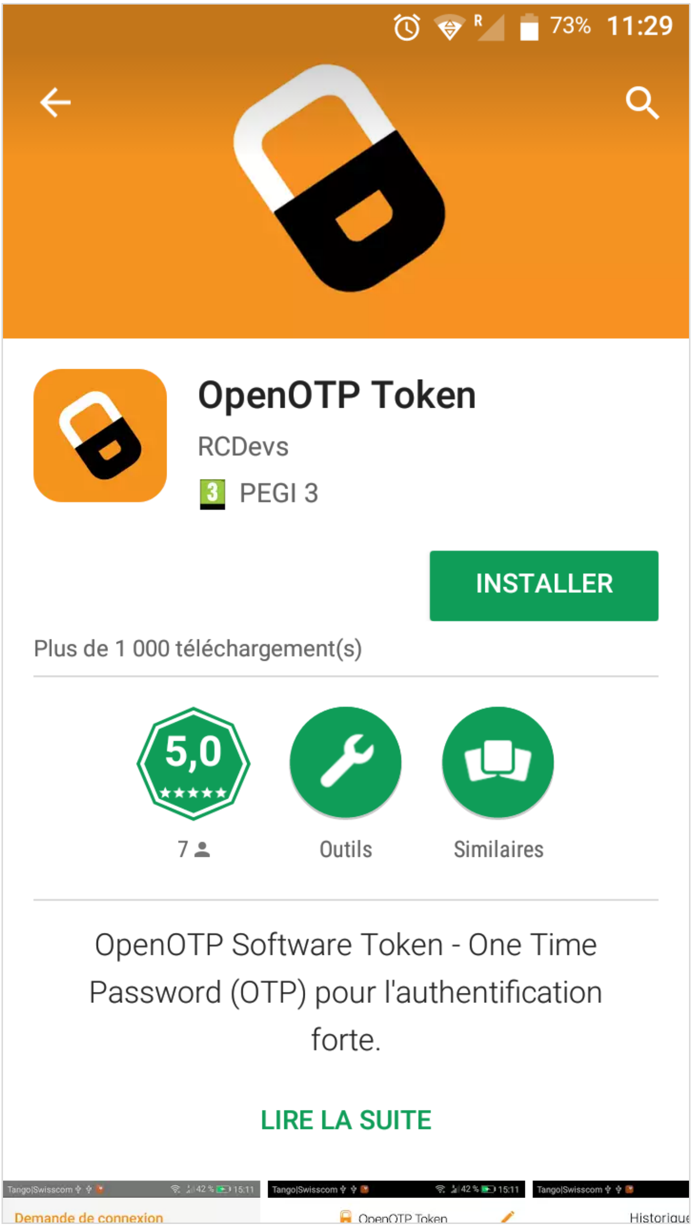
Fixed : iPhone x design on main screen

Preview

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

2.2 Android

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



73% 11:29

OpenOTP Token

RCDevs

PEGI 3

INSTALLER

Plus de 1 000 téléchargement(s)

5,0

7

Outils

Similaires

OpenOTP Software Token - One Time Password (OTP) pour l'authentification forte.

LIRE LA SUITE

Demande de connexion

OpenOTP Token

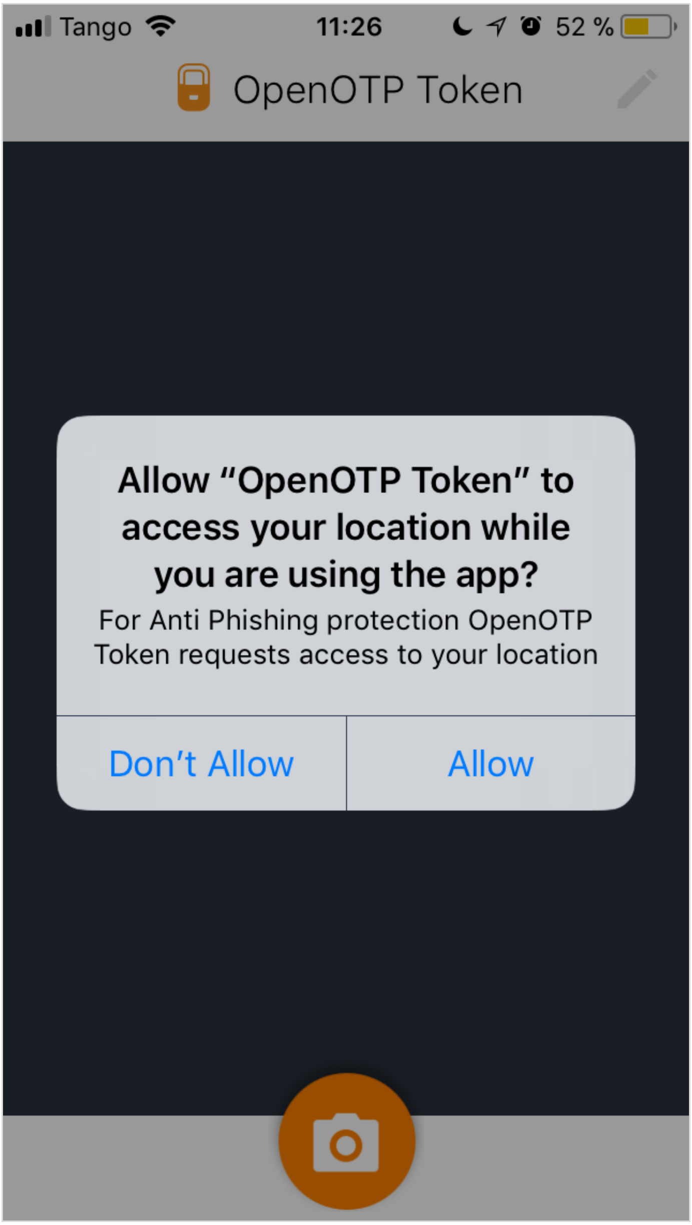
Historique

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.

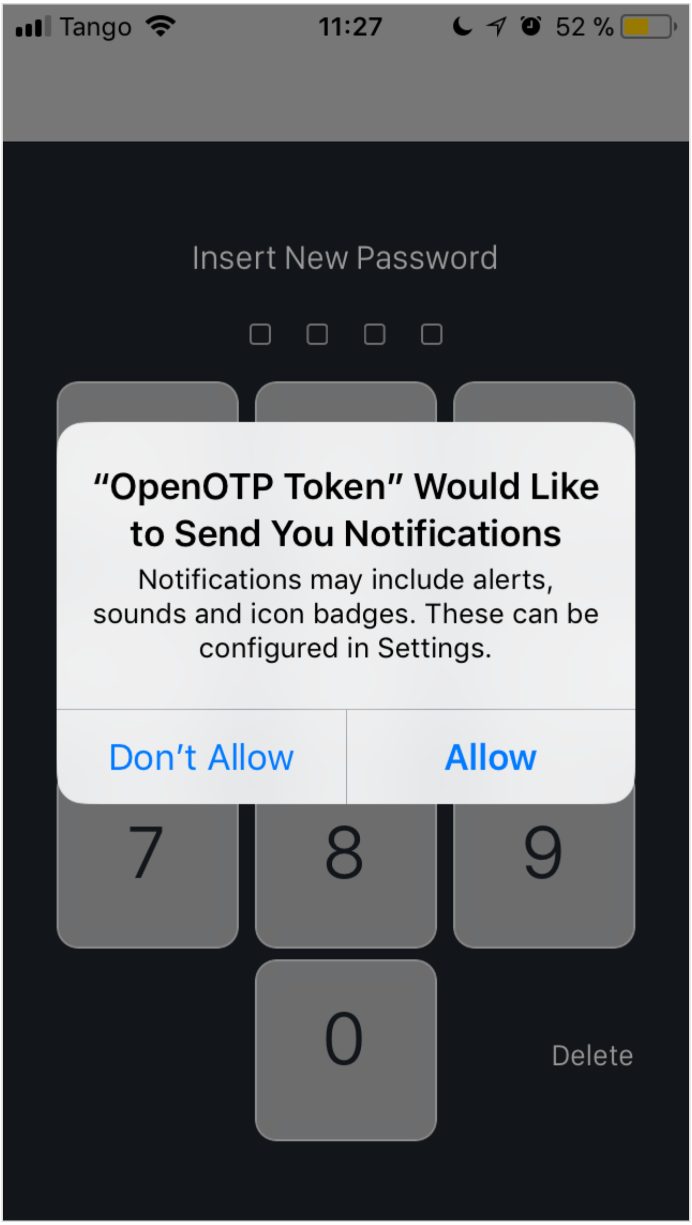
First authorization is to allow OpenOTP Token to access to your location for the Anti Phishing protection. Press on Allow button to improve security.



Allow “OpenOTP Token” to access your location while you are using the app?

For Anti Phishing protection OpenOTP Token requests access to your location

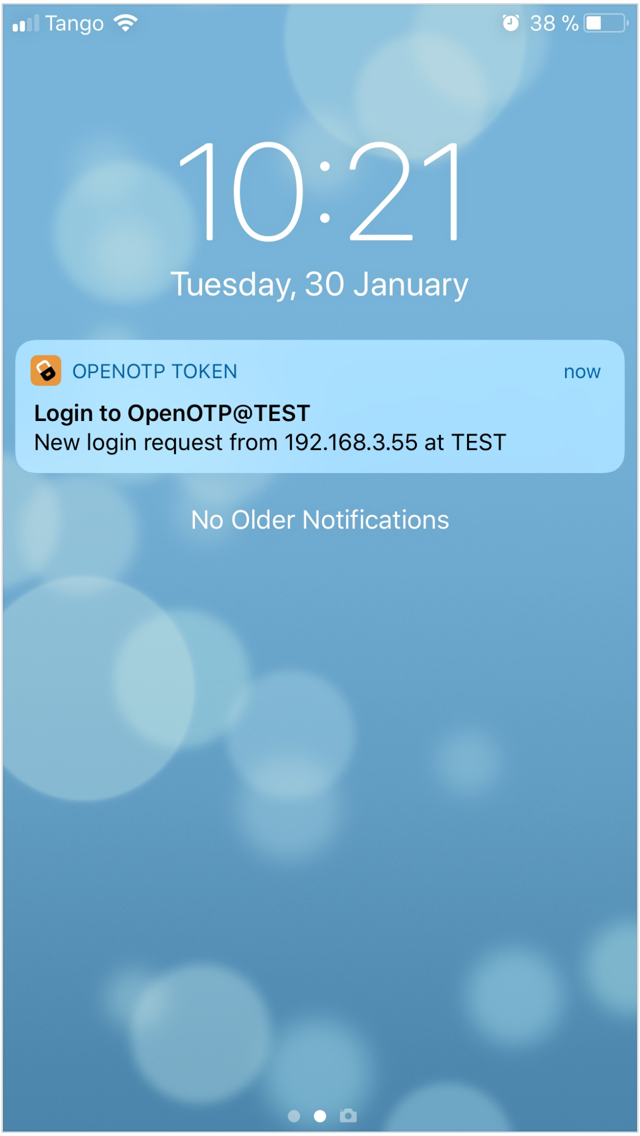
Next authorization screen is for Notifications.



“OpenOTP Token” Would Like to Send You Notifications

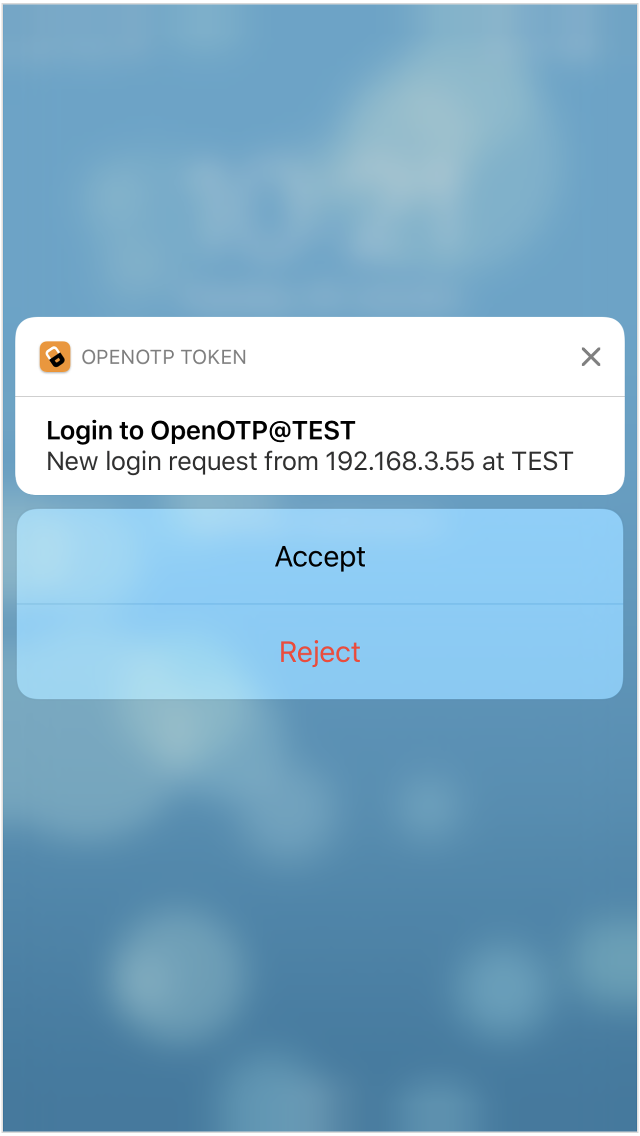
Notifications may include alerts, sounds and icon badges. These can be configured in Settings.

Notifications are used for the Push Login requests with the Approve/Deny button and for push Token removal through the WebADM Admin GUI.



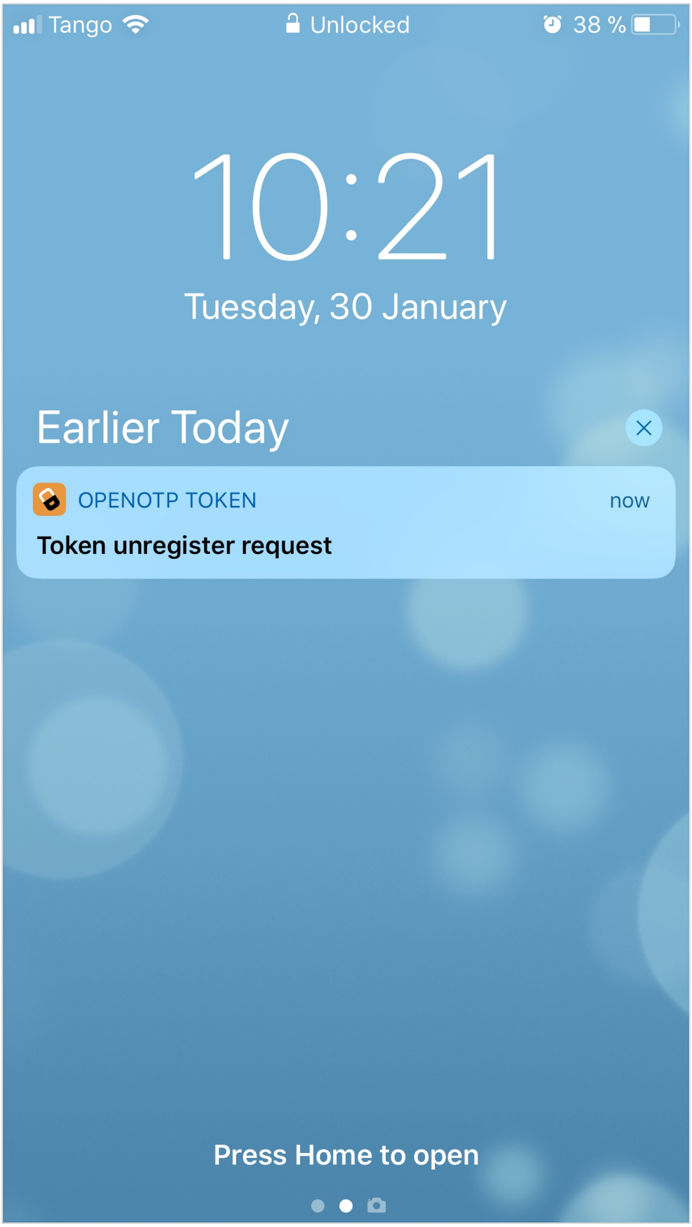
OPENOTP TOKEN now

Login to OpenOTP@TEST
New login request from 192.168.3.55 at TEST



OPENOTP TOKEN

Login to OpenOTP@TEST
New login request from 192.168.3.55 at TEST



Tango Unlocked 38 %

10:21

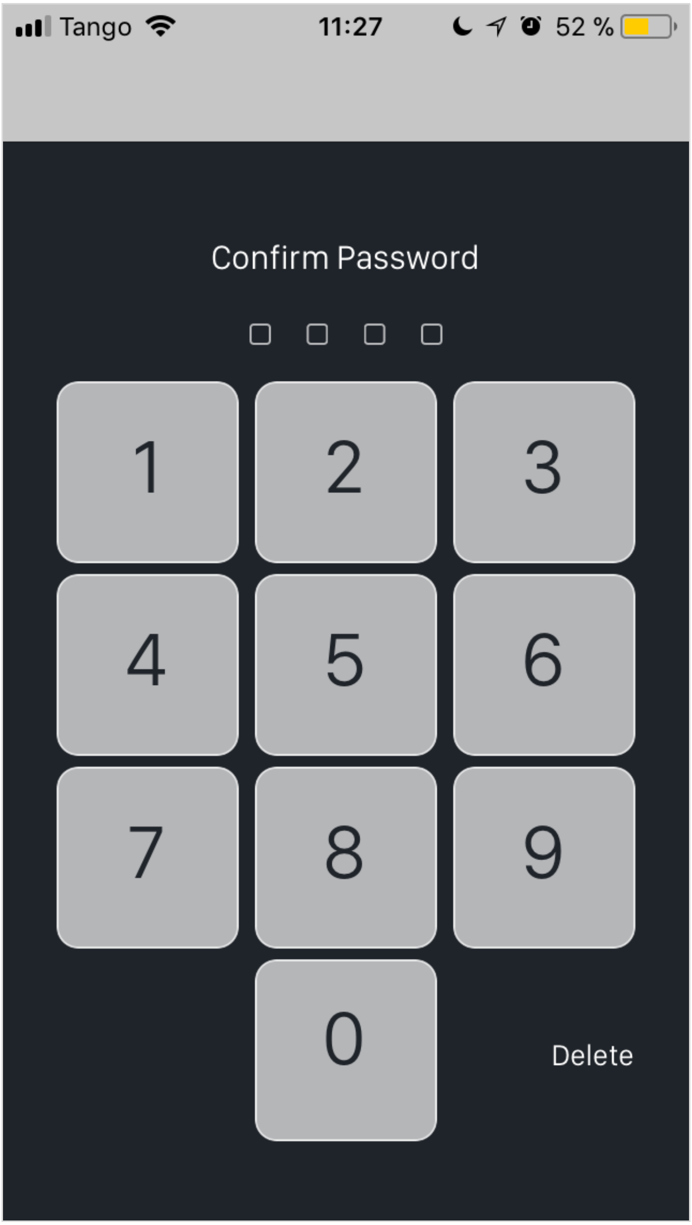
Tuesday, 30 January

Earlier Today

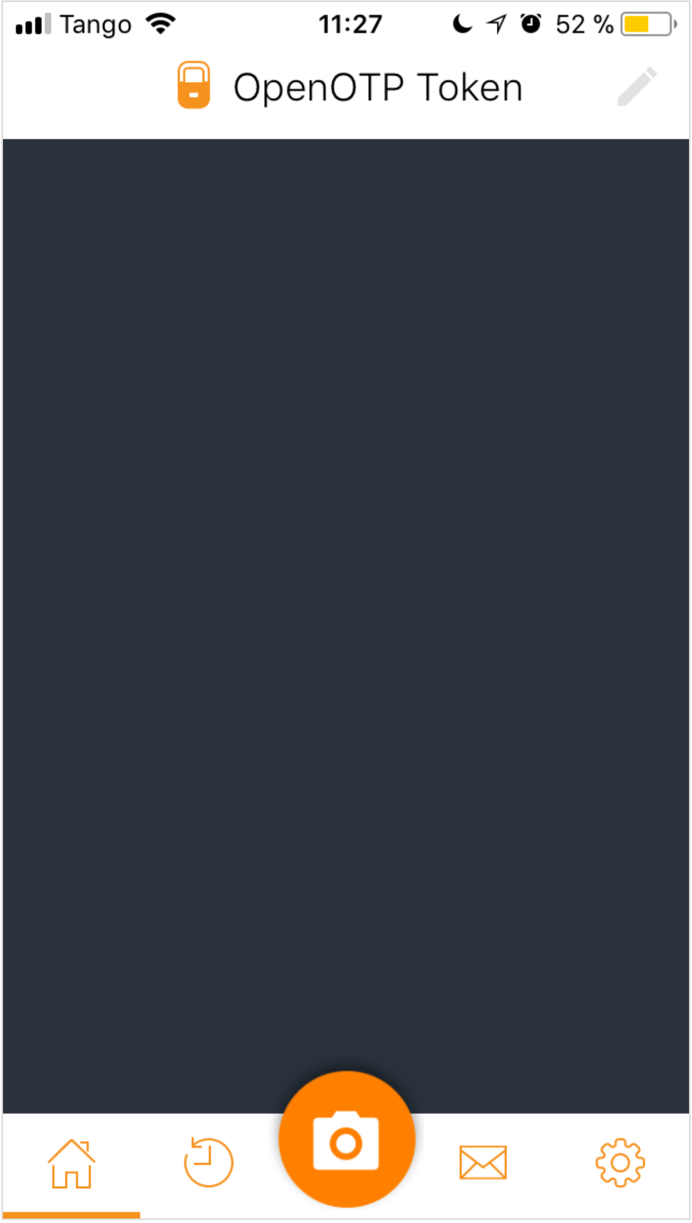
OPENOTP TOKEN now

Token unregister request

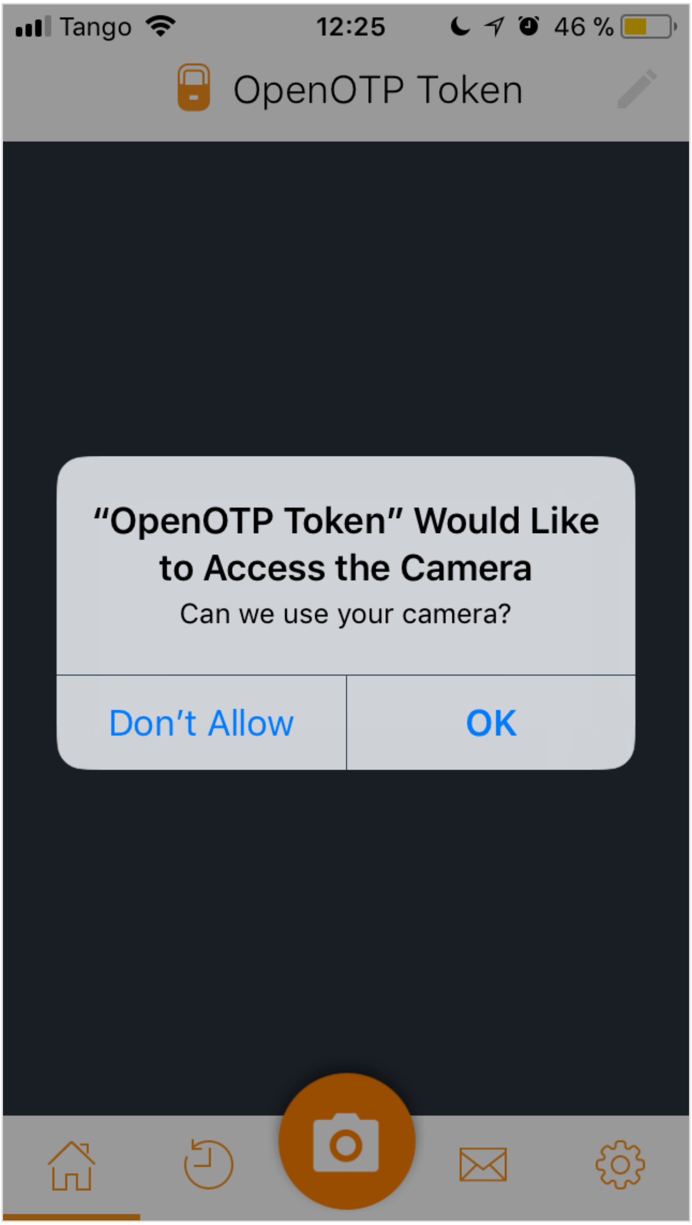
Authorizations are done for now. On the next screen, you will be able to set a password to protect the application. Enter your password twice and next time you will open the Token application, the password will be asked.



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 QRCode and enroll a new token. Click on `Ok` button.



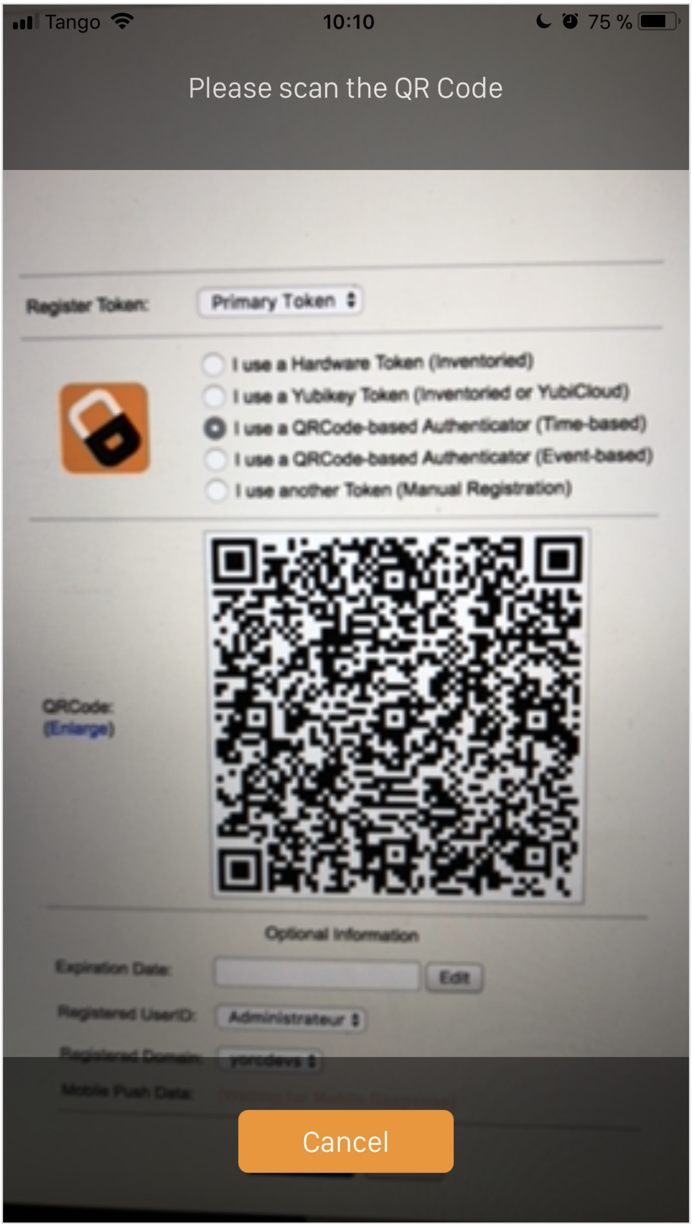
"OpenOTP Token" Would Like to Access the Camera

Can we use your camera?

4. Token Enrolment

4.1 With a QRCode

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



Please scan the QR Code

Register Token: Primary Token

○ I use a Hardware Token (Inventoried)

○ I use a Yubikey Token (Inventoried or YubiCloud)

● I use a QRCode-based Authenticator (Time-based)

○ I use a QRCode-based Authenticator (Event-based)

○ I use another Token (Manual Registration)

QRCode:
(Enlarge)

Optional Information

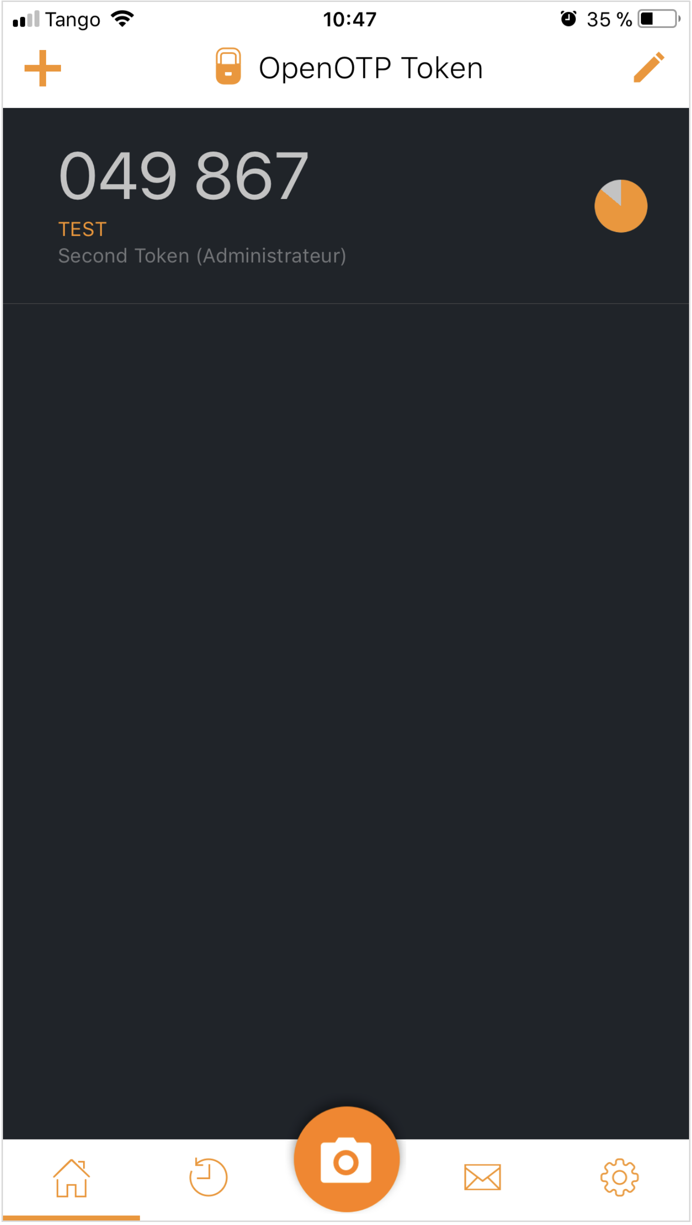
Expiration Date:

Registered UserID: Administrateur

Registered Domain: yorcdevs

Mobile Push Data:

After scanning the QRCode with the application, a Token is now enrolled on your phone :



Tango 10:47 35 %

OpenOTP Token

049 867

TEST

Second Token (Administrateur)

Your Token is ready to be used.

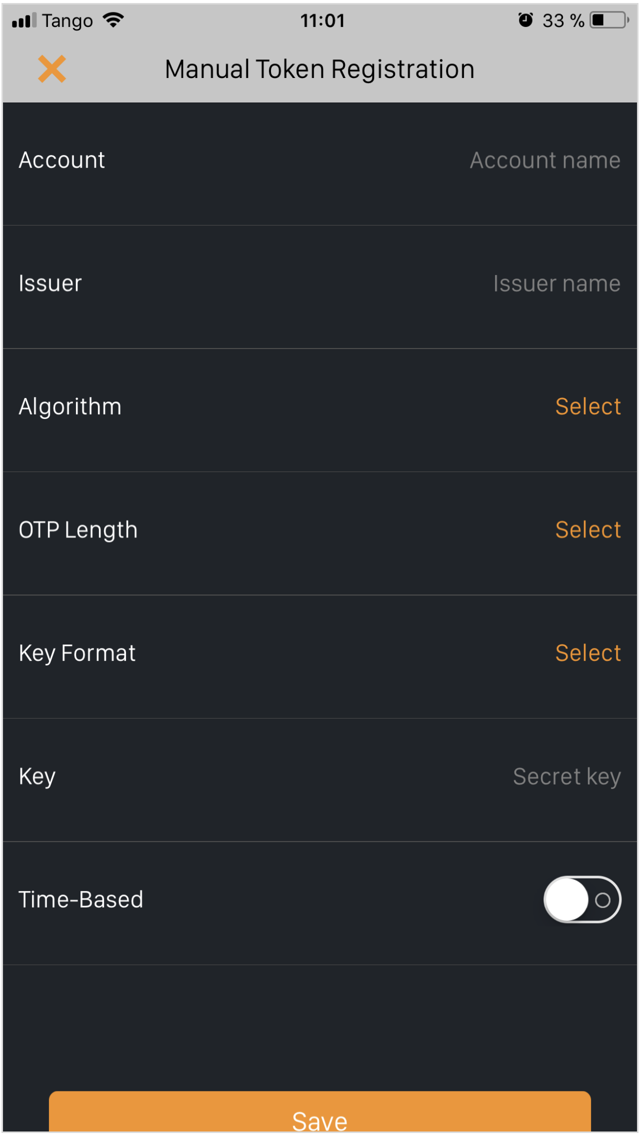
4.2 Manual Enrolment

OpenOTP Token application offers you the possibility to enroll a Token manually. On the first application screen, click on the `+` button on the top left to enter in the manual token registration mode.

By this way, 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 an event-based.



Tango 11:01 33 %

Manual Token Registration

Account: Account name

Issuer: Issuer name

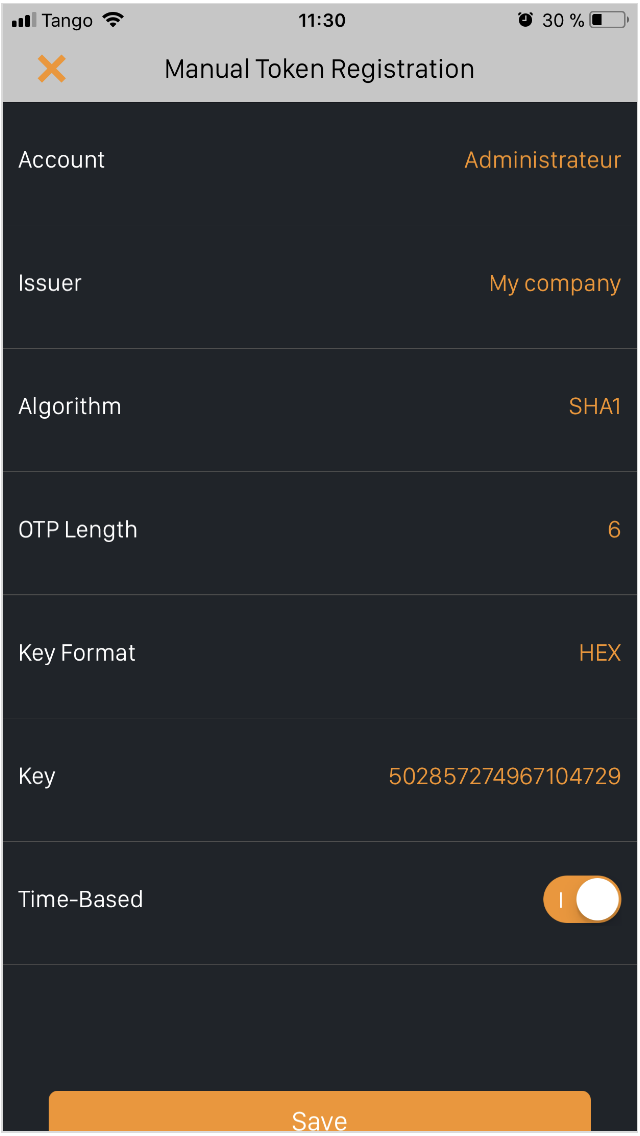
Algorithm: Select

OTP Length: Select

Key Format: Select

Key: Secret key

Time-Based: ○



Tango 11:30 30 %

Manual Token Registration

Account: Administrateur

Issuer: My company

Algorithm: SHA1

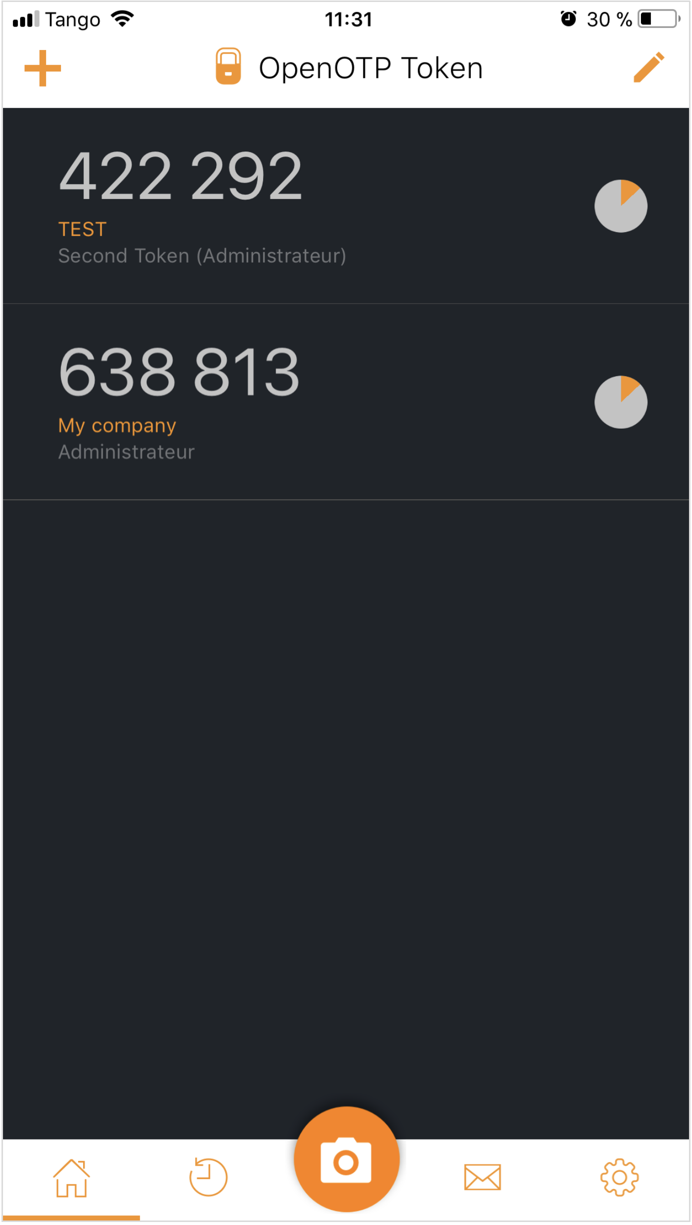
OTP Length: 6

Key Format: HEX

Key: 502857274967104729

Time-Based: I

After completing the previous informations, you can click on `Save` button.



Tango 11:31 30 %

OpenOTP Token

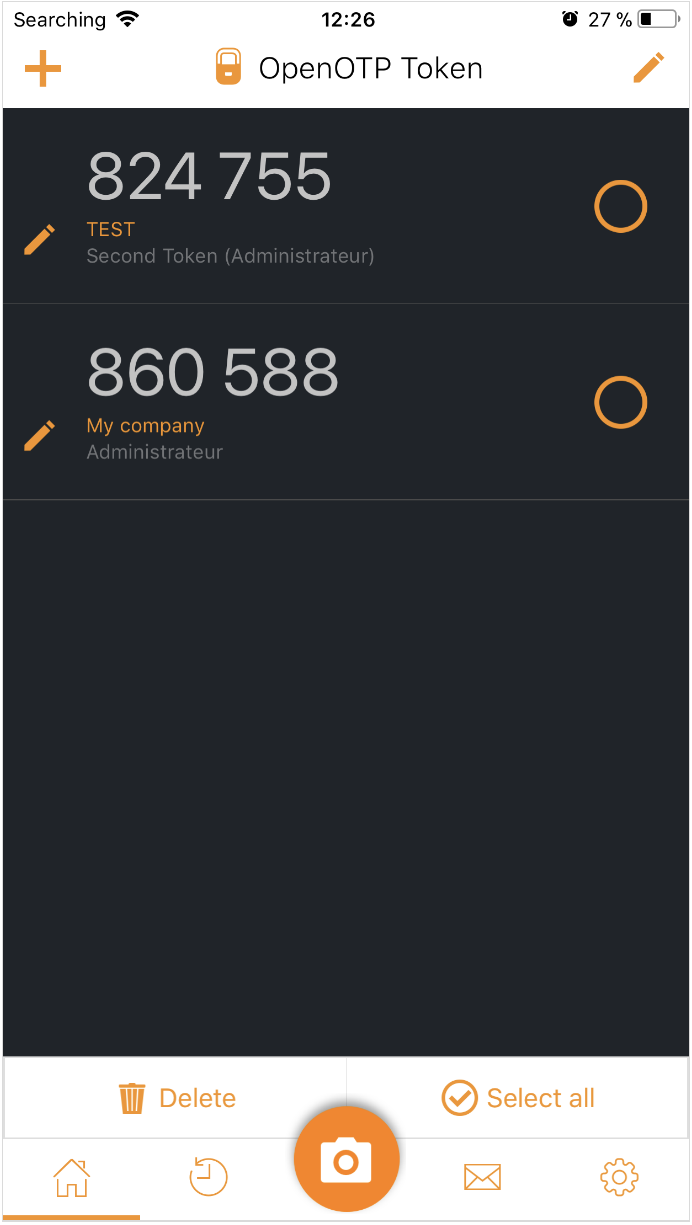
422 292
TEST
Second Token (Administrateur)

638 813
My company
Administrateur

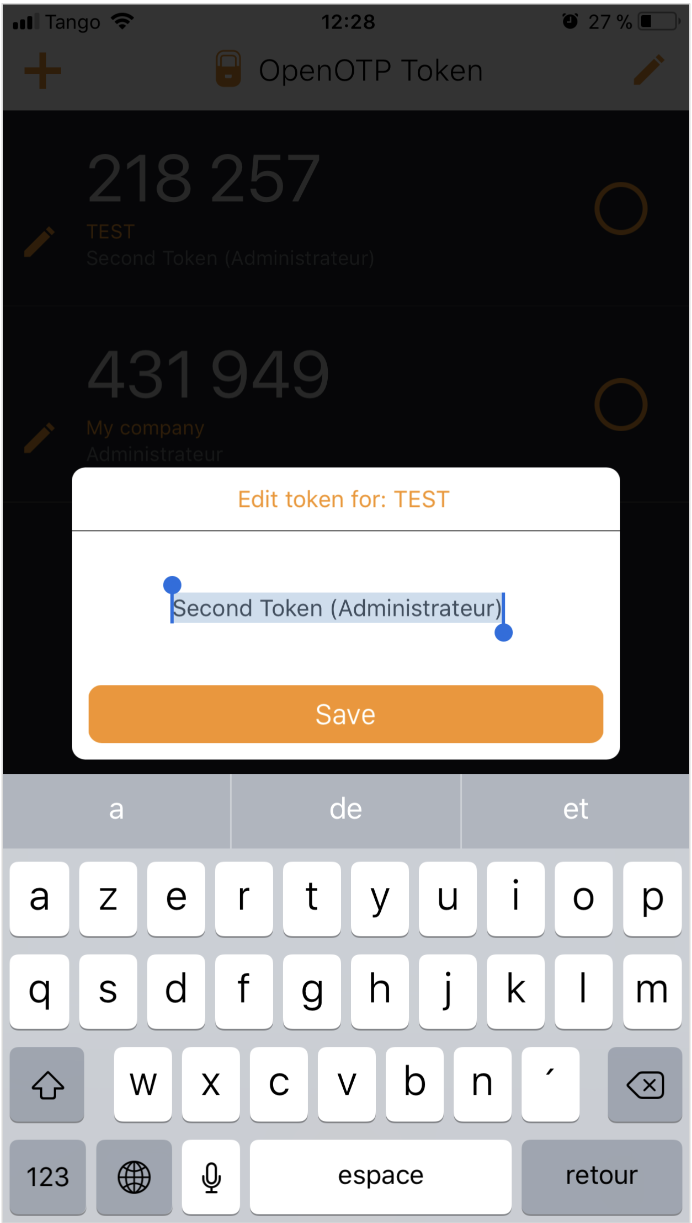
This information should be reported on the server side to be able to use this new token.

5. Token Management

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



Edit mode allow 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:



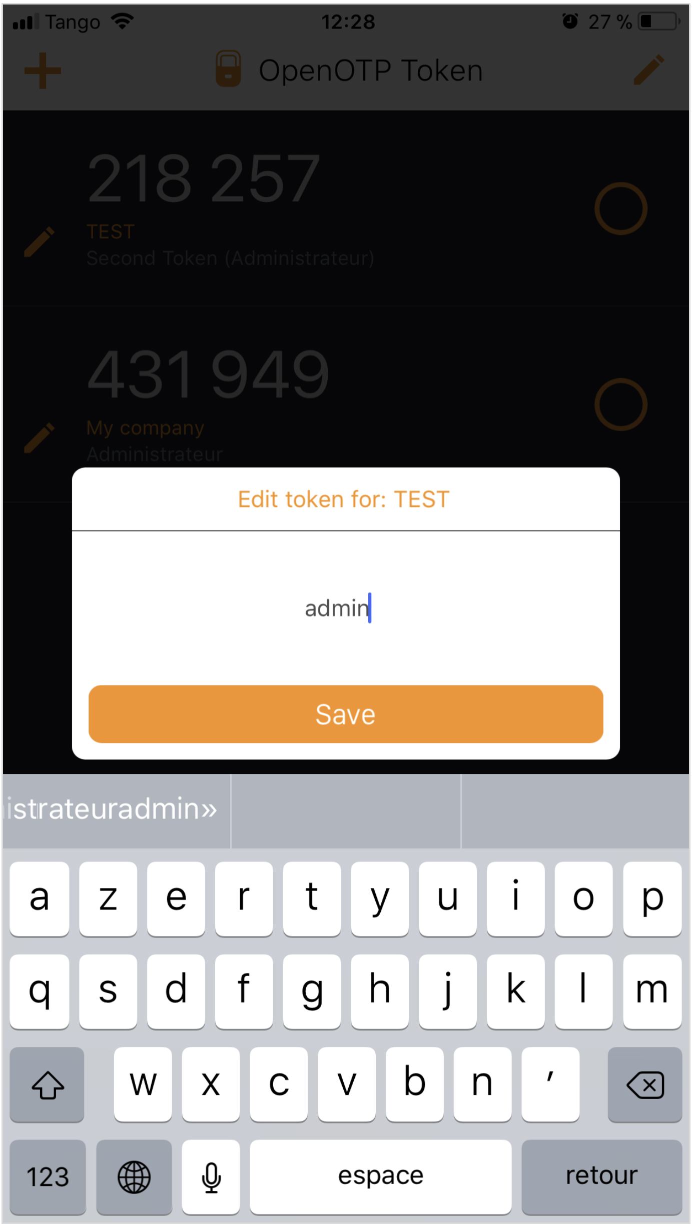
218 257
TEST
Second Token (Administrateur)

431 949
My company
Administrateur

Edit token for: TEST

Second Token (Administrateur)

I will give a short name to this one:



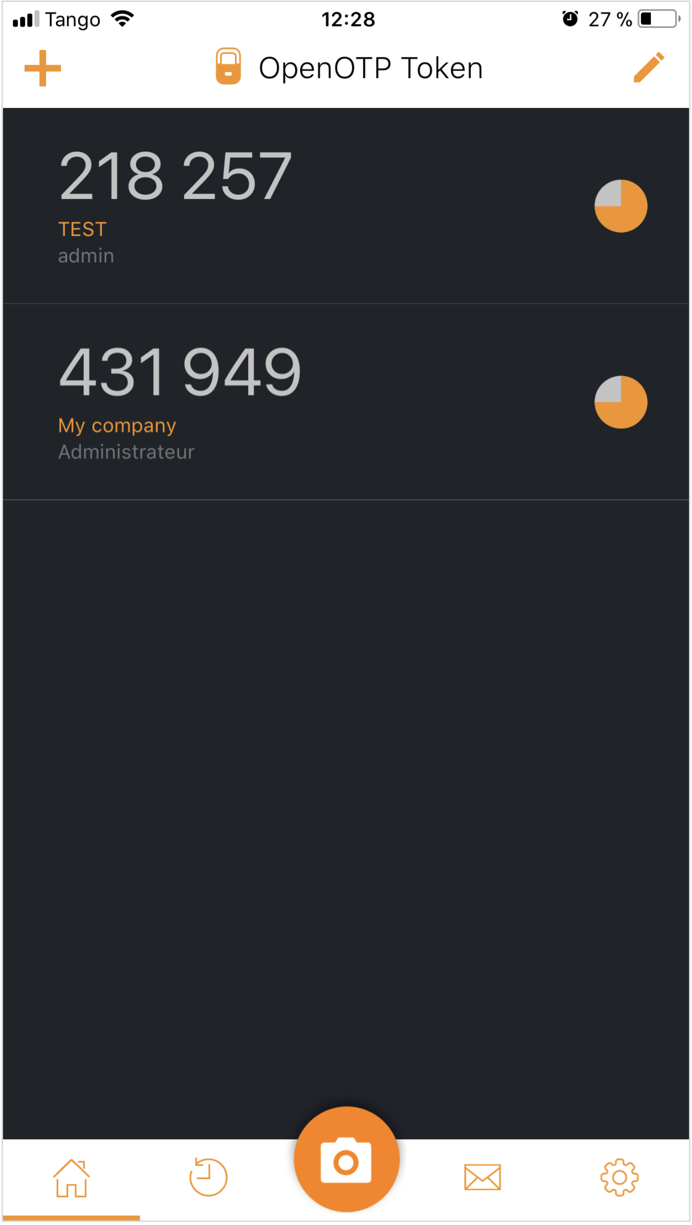
218 257
TEST
Second Token (Administrateur)

431 949
My company
Administrateur

Edit token for: TEST

admin

And click on `Save` button:

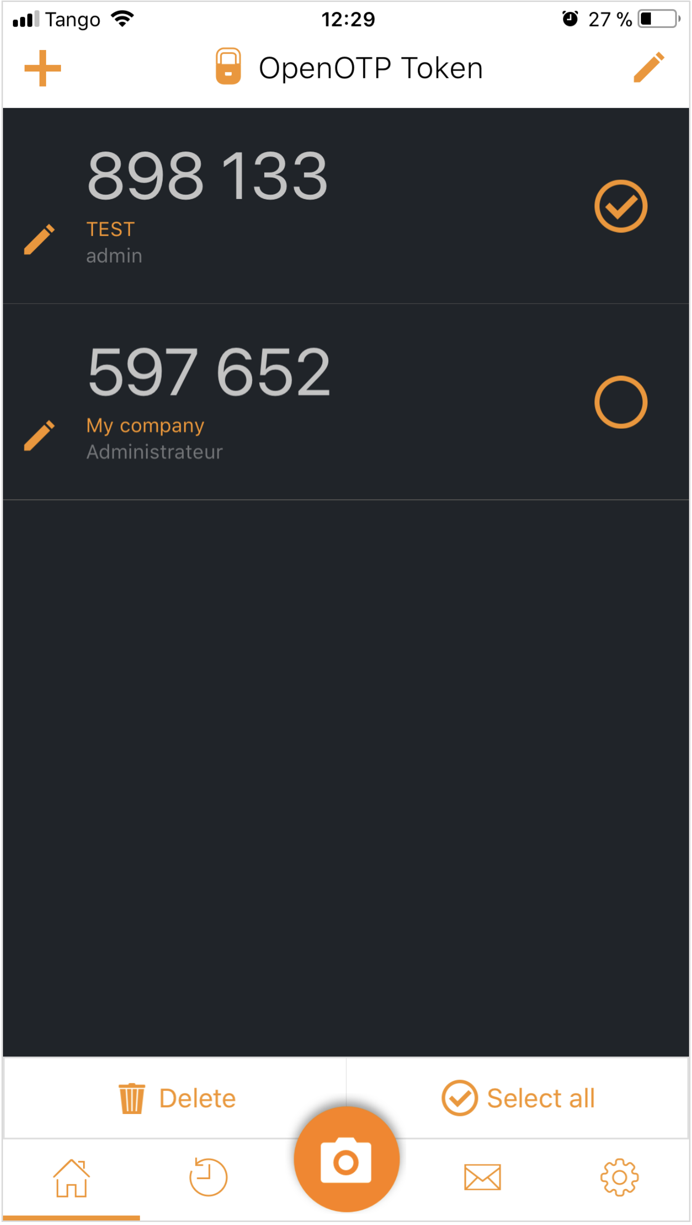


218 257
TEST
admin

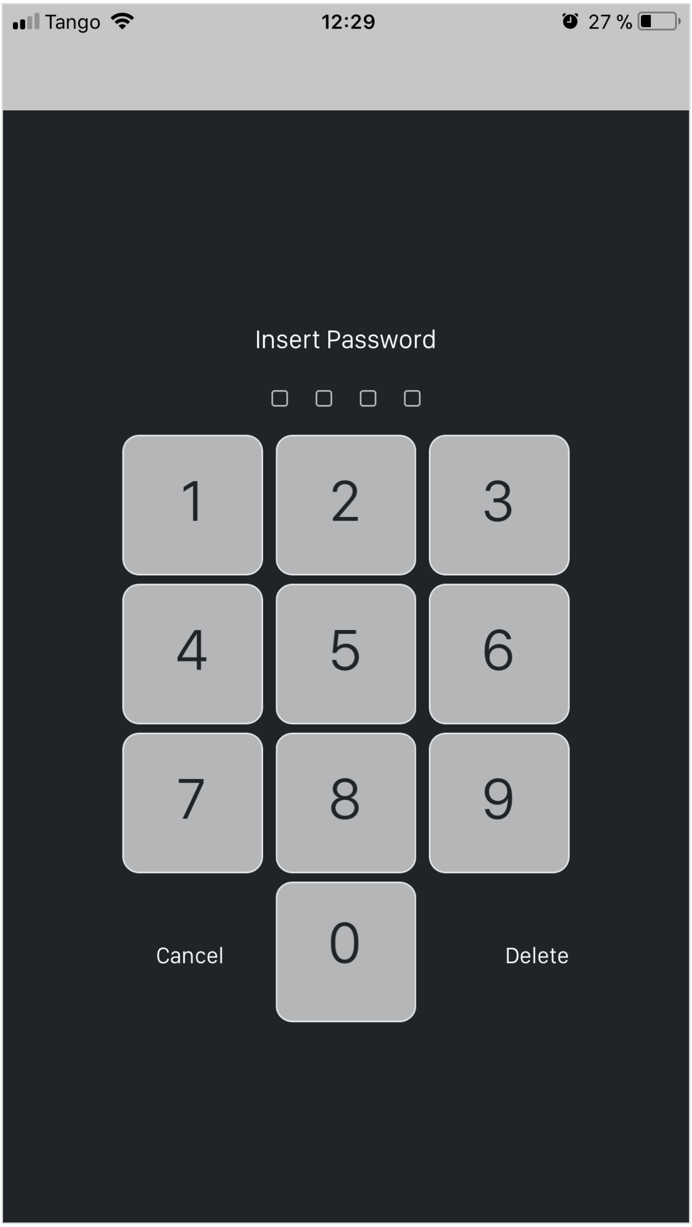
431 949
My company
Administrateur

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

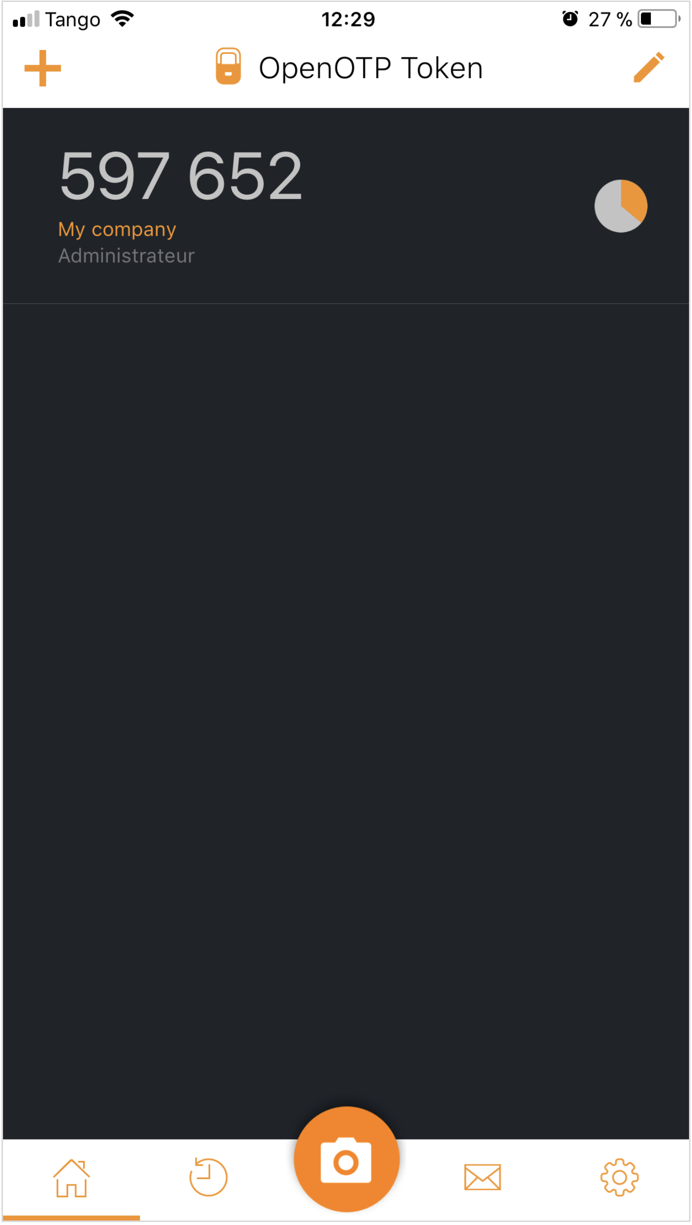
We will now remove a Token through the OpenOTP Token application. Click again on the spencil icon on the top right, you enter in `edit mode` again. Select the Token you want to remove:



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:



597 652
My company
Administrateur

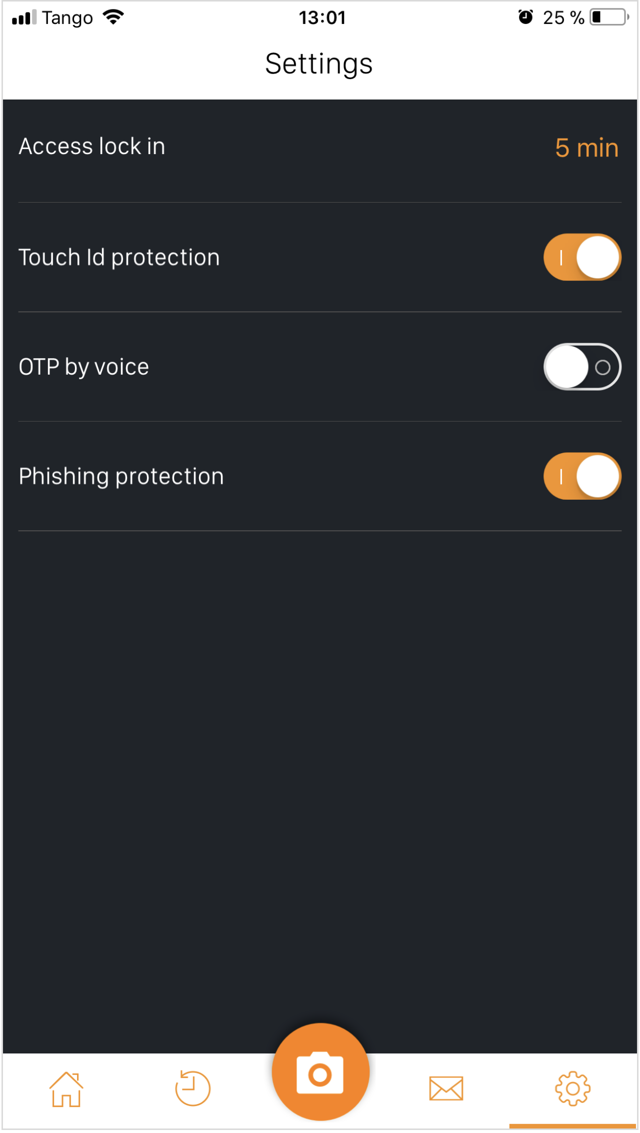
> **Note**
>
> When you remove a Token from the application, the Token is still present on the server side on your account.

6. Application Settings

When you are in 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 attack. If a phishing attack is suspected, OpenOTP Token application will prompt you a screen like below.



Tango 13:01 25 %

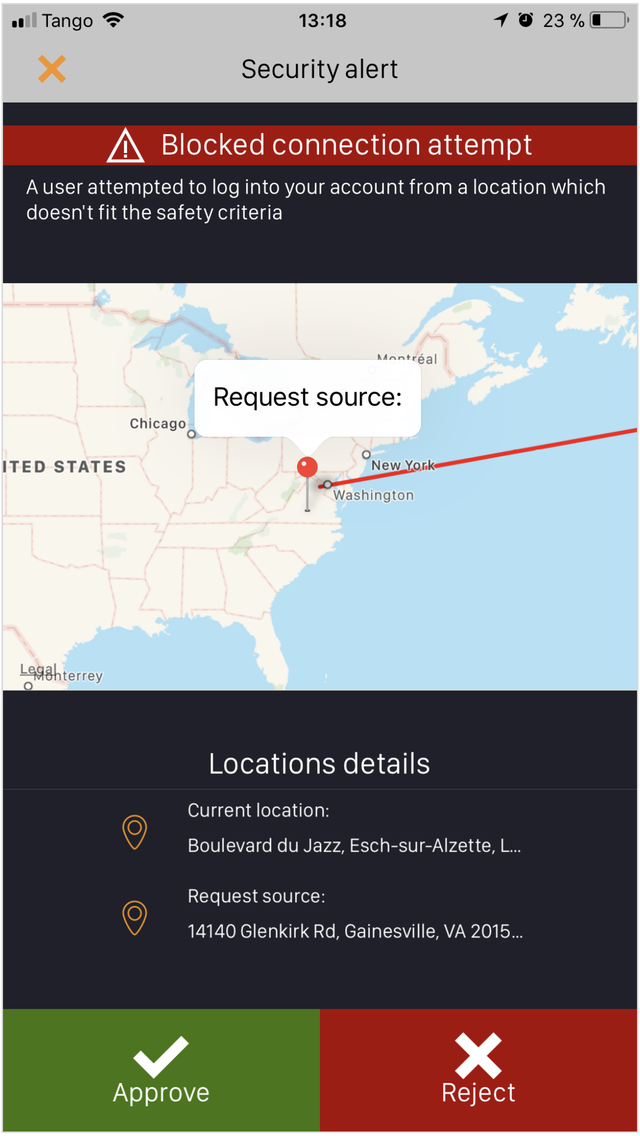
Settings

Access lock in 5 min

Touch Id protection ☑

OTP by voice ☐

Phishing protection ☑



Tango 13:18 23 %

Security alert

Blocked connection attempt

A user attempted to log into your account from a location which doesn't fit the safety criteria

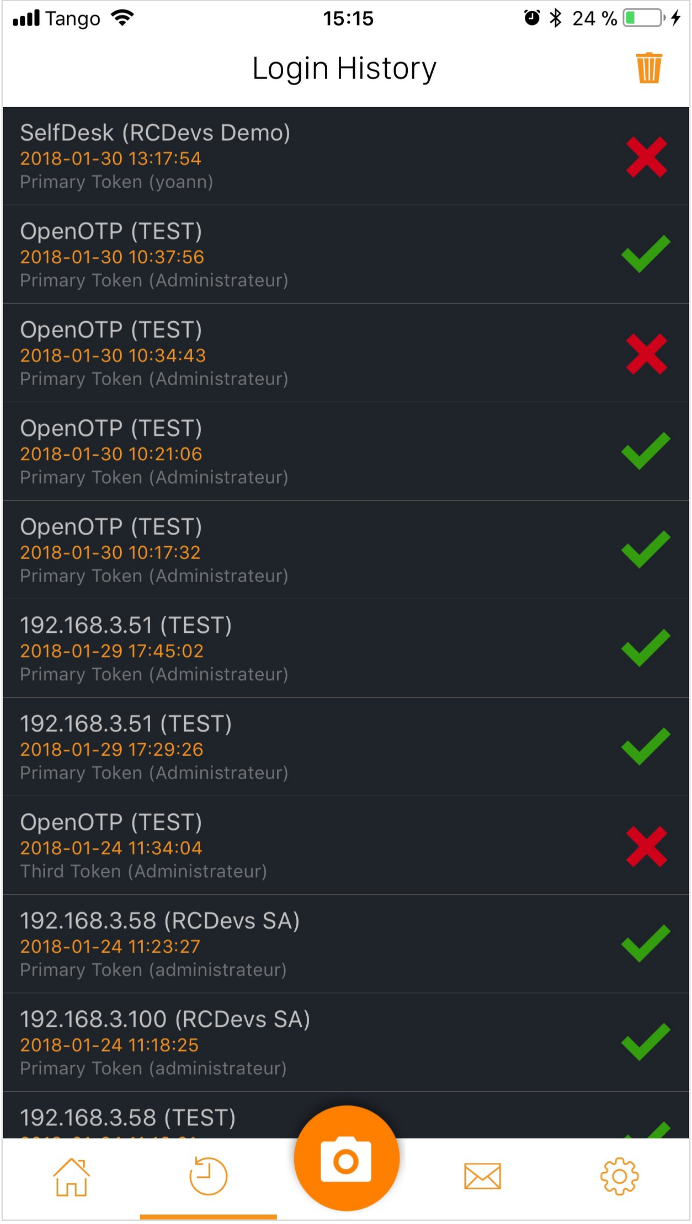
Locations details

Current location:
Boulevard du Jazz, Esch-sur-Alzette, L...

Request source:
14140 Glenkirk Rd, Gainesville, VA 2015...

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.



Tango 15:15 24 %

Login History

SelfDesk (RCDevs Demo)
2018-01-30 13:17:54
Primary Token (yoann) ✗

OpenOTP (TEST)
2018-01-30 10:37:56
Primary Token (Administrateur) ✓

OpenOTP (TEST)
2018-01-30 10:34:43
Primary Token (Administrateur) ✗

OpenOTP (TEST)
2018-01-30 10:21:06
Primary Token (Administrateur) ✓

OpenOTP (TEST)
2018-01-30 10:17:32
Primary Token (Administrateur) ✓

192.168.3.51 (TEST)
2018-01-29 17:45:02
Primary Token (Administrateur) ✓

192.168.3.51 (TEST)
2018-01-29 17:29:26
Primary Token (Administrateur) ✓

OpenOTP (TEST)
2018-01-24 11:34:04
Third Token (Administrateur) ✗

192.168.3.58 (RCDevs SA)
2018-01-24 11:23:27
Primary Token (administrateur) ✓

192.168.3.100 (RCDevs SA)
2018-01-24 11:18:25
Primary Token (administrateur) ✓

192.168.3.58 (TEST)

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 allow 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.

You Tube Play Video on Youtube

9. Other Video Tutorials where Push Login is used

OpenOTP ADFS Plugin

You Tube 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

This manual was prepared with great care. However, RCDevs S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs S.A. The latter especially applies for data processing systems. RCDevs S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs S.A. © 2019 RCDevs SA, All Rights Reserved