



OPENOTP TOKEN MOBILE APPLICATION

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs.

Copyright (c) 2010-2017 RCDevs SA. All rights reserved.

<http://www.rcdevs.com>

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

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.

Minimal OS versions

> iOS : 8.0 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, looking for OpenOTP Token and click on the download icon.

»

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.

»

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.

Next authorization screen is for Notifications.

Notifications are used for the Push Login requests with the Approve/Deny button and for 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.

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.

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.

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

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.

After completing the previous informations, you can click on **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 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:

I will give a short name to this one:

And click on **Save** button:

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:

»

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.

»

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 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](#).



9. Other Video Tutorials where Push Login is used

OpenOTP ADFS Plugin



F5 APM BIG-IP



Credential Provider for Windows Login



Custom Website



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. © 2021 RCDevs SA, All Rights Reserved