



# TOKEN REGISTRATION

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](mailto:info@rcdevs.com).

# Token Registration

[iOS](#) [Android](#) [Token](#)

## 1. Overview

In this how-to, we will demonstrate the possible ways to enroll a hardware token or a software token on your mobile. For software token registration, you must have a token application installed on your phone like [OpenOTP Token](#) or Google Authenticator. [OpenOTP Token](#) is the recommended one to enjoy all features offered by OpenOTP server (like push login, phishing protection...).

## 2. Admin Enrollment through the WebADM Admin GUI

A token enrollment can be done by a `super_admin` or `other_admin` user through the WebADM admin GUI. To be able to register a token on a user account, the user account must be activated. Have a look at the following [documentation](#) if you don't know how to activate a user.

### 2.1 Hardware Tokens

#### 2.1.1 Import the Hardware Token Inventory

The hardware tokens can be registered with the Token serial number wrote in the back of the hardware Token. But to be able to assign a hardware token, the token should be available in the WebADM inventory database. RCDevs provides an inventory file for every Tokens sold. This inventory contains the token seeds. So first, you have to import the inventory file. To do that, log in on the WebADM Admin GUI, click on `Import` tab and click on `Import Inventory File`.

»

Next page allows you to choose your inventory file on your computer. Select the file and click on the `Import` button.

»

Your hardware tokens are imported and can be assigned to users.

#### 2.1.2 Hardware Token Registration

In order to perform the **hardware token** enrollment, log in on the WebADM admin GUI, in the left LDAP tree, click on the user account for the one you want to register a token. Once you are on the activated user account, in the `Application Actions` box, click on `MFA Authentication Server`.

»

Under the next menu, click on `Register/Unregister OTP Tokens` item and you will be in the registration page:

»

Select the token slot (here is primary Token) and choose the option `Use Hardware Token (Inventoried)`.

Enter the serial number of the token and click **Register** button.

The token is now registered on the user account.

## 2.2 Software Token Registration

In order to perform the **software token** enrollment, log in on the WebADM admin GUI, in the left LDAP tree, click on the user account for the one you want to register a token. Once you are on the activated user account, in the **Application Actions** box, click on **MFA Authentication Server**.

Under the next menu, click on **Register/Unregister OTP Tokens** item and you will be in the registration page:

3 options are now available for software token registration:

- > I use a QRCode-based Authenticator (Time-based)
- > I use a QRCode-based Authenticator (Event-based)
- > I use another Token (Manual Registration)

The manual registration is not explained in this documentation. Select the time-based Token registration (preferred one) or event-based Token registration and a QRCode will be prompted. Open your Token application installed on your phone and scan the QRCode.

### Note

The message 'Mobile Push Data: [Waiting for Mobile Response]' is only available when you have configured the Push login infrastructure.

Once the QRCode is scanned, the Token will appear in your software token application. Click on the **Register** button once the Token is enrolled on your phone.

## ⚠ Push Token enrollment

When you have configured a Push login infrastructure with OpenOTP, you don't need to click on the Register button. The registration at the WebADM level is automatically done by the mobile response.

The enrollment through the WebADM Admin GUI is now done and you should be able to login with an OTP.

### 2.3 Voice Registration

In order to record a **voice biometric** to a user, log in on the **WebADM admin GUI**, in the left LDAP tree, click on the user account that you want to register a voice. Once you are on the activated user account, in the **Application Actions** box, click on **MFA Authentication Server**.

Under the next menu, click on **Register / Unregister Voice Biometrics** item and you will be in the registration page:

In that page, click in **Click to Start**, then record your **voice biometric**. It is recommended you use an earphone with microphone or other kind of dedicated audio input device.

To make sure it will not be misunderstood by **OpenOTP**, you have to repeat your voice biometric 4 times and not use too short messages.

Once the Voice registration is finished, you should see the attribute **WebADM Voice Model** (webadmVoice).

If you can see the **WebADM Voice attribute**, that means the voice registration was done successfully.

## 3. End-User enrollment through RCDevs Web Applications

RCDevs provides 3 web applications ([selfdesk](#), [selfreg](#) and [helpdesk](#)) for the user self-enrollment. These applications are free and must be installed on your WebADM server. To limit the end-user access to the WebADM/OpenOTP servers, you can allow access to these web applications through a [WebADM Publishing Proxy](#). By this way, your end-users will access to the webapps through the WAProxy server and not from the WebADM server.

The **User Self-Registration** application is similar to the **User Self-Service Desk**, the only difference between both applications is that the **Self-Registration** can be accessed only with a **WebADM Administrator** request. To allow the user to access this

application, the Administrator has to send a **Self-Registration** request to the user. The user will receive a one time link by mail or SMS to access the application. Once logged on the application through the one time link, the access link is revoked and the user cannot access the application anymore. The **Selfdesk** and **HelpDesk** application are accessible at any time by the end-user (if the application is not locked by default in its configuration).

### 3.1 User Self-Registration

Have a look here for the [soft token enrollment through the selfreg](#) application. This documentation will show you how to send a self-registration request to a user. Once you are logged on the selfreg application, then you can follow the 3.2 part to enroll a Token (selfdesk and selfreg are similar for the token registration part)

### 3.2 User Self-Service Desk

The user self-service desk is accessible to the following address:

```
https://YOUR_WEBADM/webapps/selfdesk/login_uid.php
```

through the WAPRoxy the address is:

```
https://YOUR_WAPROXY/selfdesk/login_uid.php
```

#### 3.2.1 SelfDesk Token Registration

##### 3.2.1.1 Hardware Token Registration

To allow the user to enroll a Token, you have to allow the OTP management under the [Selfdesk configuration](#).

When that setting is checked, you can log in to the Selfdesk application.

»

»

Once logged on the Selfdesk application, go on the **OTP** tab.

»

Click now on **Register Token** button.

You are now on the menu to register a Token. As you can see, it looks like the admin enrollment page. Select the Hardware Token method. Then enter the token serial and the OTP displayed in the HW Token screen.

»

Enter the OTP code provided by your token application under the QRCode.

»

And click on **Register** button.

»

Your hardware token is now registered.

### 3.2.1.2 Software Token Registration

To allow the user to enroll a Software Token, you have to allow the OTP management under the [Selfdesk configuration](#).

When that setting is checked, you can log in to the Selfdesk application.

»

»

Once logged on the Selfdesk application, go on the **OTP** tab.

»

Click now on **Register Token** button.

You are now on the menu to register a Token. As you can see, it looks like the admin enrollment page. Select one of both QRCode method. The QRCode will appear on your screen. Scan it with your preferred Token application and you should see the token registered in the application.

»

Enter the OTP code provided by your token application under the QRCode.

»

And click on **Register** button.

»

Your software token is now registered.

### 3.2.3 SelfDesk Voice Registration

First, log in to the **SelfDesk** application.

»

Once logged on the **SelfDesk** application, go on the **OTP** tab.

»

Change **View My** to **Voice Biometrics**. Then click in **Click to Register**

»

»

»

It is recommended you use an earphone with microphone or other kind of dedicated audio input device. To make sure it will not be misunderstood by **OpenOTP**, you have to repeat your voice biometric 4 times and not use a too short message.

After the **Voice registration** is done. You will see, under **OTP tab**, that the **Voice Login Status** is Ok.

»

## 3.3 HelpDesk Enrollment

It is also possible to enroll a Token in the [HelpDesk](#) application.

The **HelpDesk** application is accessible to the following address:

```
https://YOUR_WEBADM/webapps/helpdesk/login_uid.php
```

through the WAPRoxy the address is:

```
https://YOUR_WAPROXY/helpdesk/login_uid.php
```

### 3.3.1 HelpDesk Hardware Token Registration

To allow the user to enroll a Hardware Token, you have to allow the OTP management under the [HelpDesk configuration](#).

When that setting is checked, you can log in to the **HelpDesk** application.

»

After login in the application, select the user you want to register a **Hardware Token**

Once the user is select, go to **OTP** tab and, at the bottom of the page, click in **Add a Token**.

In the next page, please, click in **Hardware Token**.

Then enter the serial of your inventoried **Token** and click in **Register**

If everything goes right, you should see the Token you have just registered in the user's **OTP** tab.

So, you have your **Hardware Token** registered.

### 3.3.2 HelpDesk Software Token Registration

To allow the user to enroll a **Software Token**, you have to allow the OTP management under the [HelpDesk configuration](#).

When that setting is checked, you can log in to the HelpDesk application.

After login in the application, select the user you want to register a **Software Token**.

Once the user is select, go to **OTP** tab and, at the bottom of the page, click in **Add a Token**.

In the next page, please, click in **Software Token**.

Then scan the QRCODE to register your **Software Token**.

If everything goes right, you should see the **Software Token** you just registered in the user's **OTP** tab.



So, you have your **Software Token** registered.

## 4. Authentication Test through the WebADM Admin GUI

### 4.1 Hardware Token Login

Login on the WebADM admin GUI and click on your user in the left tree. In **Applications Actions** box, click on **MFA Authentication Server**

We scroll down and click on **Test User Login** :

We insert the **LDAP password** and the **OTP password**, then we click in **OK** :

We are authenticated!

### 4.2 Software Token Login

Login on the WebADM admin GUI and click on your user in the left tree. In **Applications Actions** box, click on **MFA Authentication Server**

We scroll down and click on **Test User Login** :

If you are using **PUSH login**, you can insert the **LDAP password** and wait the **PUSH notification** in your cellphone. If you are not using PUSH, insert the **OTP password** now, and click in **OK** :

We are authenticated!

## 4.2 Voice Login

Log in the **WebADM** admin GUI and click in your user in the left tree. In **WebADM settings**, click on **Configure**

Make sure the **OTP Type** type is set to **VOICE**.

### Note

Voice Biometrics feature requires that PUSH is configured and enabled in MFA/OpenOTP application settings. Also, in a real scenario, the user should have an OpenOTP software token registered.

Then, in **Applications Actions** box, click on **MFA Authentication Server**

We scroll down and click on **Test User Authentication**:

We insert the LDAP password and click on **Start**:

Then, if you have **Soft Token with Push** registered, you will get a notification in your mobile. Perform the authentication with **Voice** in your mobile. Otherwise, you will be asked to enter your **Voice biometrics** in the test page.

We are authenticated!

## 5. Logs

### 5.1 Hardware Token Logs

Now we can check the logs, we click on **Databases** tab:

Click on **WebADM Server log Files**. It corresponds to the **/opt/webadm/log/webadm.log** file:

Each authentication is identified by an ID. Here, it is **FIR6BF3T**.

```
[Fri Dec 04 17:41:39.533892 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] New
openotpNormalLogin SOAP request
[Fri Dec 04 17:41:39.533951 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] > Username:
aduser2
[Fri Dec 04 17:41:39.533959 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] > Domain: adrcdevs
[Fri Dec 04 17:41:39.533967 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] > LDAP Password:
xxxxxxxxxxx
[Fri Dec 04 17:41:39.533974 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] > OTP Password:
xxxxxx
[Fri Dec 04 17:41:39.533981 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] > Client ID:
OpenOTP
[Fri Dec 04 17:41:39.533988 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] > Source IP:
192.168.3.146
[Fri Dec 04 17:41:39.533994 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] > Context ID:
ceda89db9677cf789dcbb1b652566970
[Fri Dec 04 17:41:39.534044 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Registered
openotpNormalLogin request
[Fri Dec 04 17:41:39.534267 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Resolved LDAP
user: CN=aduser2,CN=Users,DC=adrcdevs,DC=com (cached)
[Fri Dec 04 17:41:39.534429 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Resolved LDAP
groups: group1
[Fri Dec 04 17:41:39.549342 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Started
transaction lock for user
[Fri Dec 04 17:41:39.566228 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Found user
fullname: aduser2
[Fri Dec 04 17:41:39.566317 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Found 1 user
mobiles: 123456789
[Fri Dec 04 17:41:39.566327 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Found 1 user
emails: aduser2@adrcdevs.com
[Fri Dec 04 17:41:39.567017 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Found 49 user
settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,PushLogin=Yes,BlockNotify=MAIL,ExpireNotify=MAIL,Challeng
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,PrefetchExpire=10,

[Fri Dec 04 17:41:39.568098 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Found 11 user
data:
VoiceState,LastOTP,TokenType,TokenKey,TokenState,TokenSerial,Token2Type,Token2Key,Token2S

[Fri Dec 04 17:41:39.568168 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Last OTP present
(valid until 2020-12-04 17:45:30)
[Fri Dec 04 17:41:39.568211 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Token #2 (TOTP) is
disabled
[Fri Dec 04 17:41:39.568224 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Found 1 registered
OTP token (TOTP)
[Fri Dec 04 17:41:39.568252 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Requested login
factors: LDAP & OTP
[Fri Dec 04 17:41:39.580701 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] LDAP password Ok
[Fri Dec 04 17:41:39.581193 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] TOTP password Ok
```

(token #1)

```
[Fri Dec 04 17:41:39.585778 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Updated user data  
[Fri Dec 04 17:41:39.586939 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Sent login success  
response
```

## 5.2 Software Token Logs

Now we can check the logs, we click on **Databases** tab:

Click on **WebADM Server log Files**. It corresponds to the `/opt/webadm/log/webadm.log` file:

Each authentication is identified by an ID. Here, it is **JTLYVX00**.

```
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] New openotpNormalLogin SOAP  
request  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] > Username: testing_account  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] > Domain: yorcdevs  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] > LDAP Password: xxxxxxxx  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] > OTP Password: xxxxxxx  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] > Client ID: OpenOTP  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] > Source IP: 192.168.3.54  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] > Context ID:  
669a5a28e23dad1d3a50cc5d8a24ac30  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Registered openotpNormalLogin  
request  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Resolved LDAP user:  
CN=testing_account,CN=Users,DC=yorcdevs,DC=com  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Started transaction lock for  
user  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Found user fullname:  
testing_account  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Found 43 user settings:  
LoginMode=LDAPOTP,OTPTType=TOKEN,OTPLength=6,ChallengeMode=Yes,ChallengeTimeout=90,Mobile1  
1:HOTP-SHA1-6:QN06-  
TIM,DeviceType=FID02,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,PrefetchExpire=10,  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Found 5 user data:  
TokenType,TokenKey,TokenState,TokenID,TokenSerial  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Found 1 registered OTP token  
(TOTP)  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Requested login factors: LDAP &  
OTP  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] LDAP password Ok  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] TOTP password Ok (token #1)  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Updated user data  
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX00] Sent success response
```

## 5.3 Voice Biometrics Logs

Now, we can check the logs using Voice Biometrics. We click on **Databases** tab:

Click on **WebADM Server log Files**. It corresponds to the `/opt/webadm/log/webadm.log` file:

Each authentication is identified by an ID. Here, it is **Z5J7U1XC**.

```
[Tue Nov 24 11:56:31.259122 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] New
openotpSimpleLogin SOAP request
[Tue Nov 24 11:56:31.259176 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] > Username:
aduser3
[Tue Nov 24 11:56:31.259184 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] > Domain:
adrcdevs.com
[Tue Nov 24 11:56:31.259219 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] > Password:
xxxxxxxxxxx
[Tue Nov 24 11:56:31.259232 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] > Options: -
LDAP,OFFLINE,NOVOICE
[Tue Nov 24 11:56:31.259254 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Registered
openotpSimpleLogin request
[Tue Nov 24 11:56:31.259574 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Resolved LDAP
user: CN=aduser3,CN=Users,DC=adrcdevs,DC=com (cached)
[Tue Nov 24 11:56:31.259651 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Resolved LDAP
groups: group2,remote desktop users
[Tue Nov 24 11:56:31.270757 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Started
transaction lock for user
[Tue Nov 24 11:56:31.283882 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Found user
fullname: aduser3
[Tue Nov 24 11:56:31.283912 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Found 1 user
mobiles: +123 456789012
[Tue Nov 24 11:56:31.283921 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Found 1 user
emails: aduser3@adrcdevs.com
[Tue Nov 24 11:56:31.284501 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Found 49 user
settings:
LoginMode=LDAPOTP,OTPTType=VOICE,PushLogin=Yes,PushVoice=Yes,BlockNotify=MAIL,ExpireNotif
y:1:HOTP-SHA1-6:QN06-
TIM,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,PrefetchExpire=10,

[Tue Nov 24 11:56:31.285679 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Found 6 user data:
VoiceState,TokenType,TokenKey,TokenState,TokenID,TokenSerial
[Tue Nov 24 11:56:31.285783 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Found 1 registered
OTP token (TOTP)
[Tue Nov 24 11:56:31.287052 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Requested login
factors: OTP
[Tue Nov 24 11:56:31.287276 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Authentication
challenge required
```

```
[Tue Nov 24 11:56:31.409081 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Sent push notification for token #1
[Tue Nov 24 11:56:31.409111 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Waiting 28 seconds for mobile response
[Tue Nov 24 11:56:44.612725 2020] [192.168.3.172] [OpenOTP:Z5J7U1XC] Received mobile voice response from 192.170.3.17
[Tue Nov 24 11:56:44.612756 2020] [192.168.3.172] [OpenOTP:Z5J7U1XC] > Session: 77Hxxx0zDK02tE1K
[Tue Nov 24 11:56:44.612764 2020] [192.168.3.172] [OpenOTP:Z5J7U1XC] > Sample: 152368 Bytes
[Tue Nov 24 11:56:44.612770 2020] [192.168.3.172] [OpenOTP:Z5J7U1XC] Found authentication session started 2020-11-24 11:56:31
[Tue Nov 24 11:56:45.318400 2020] [192.168.3.172] [OpenOTP:Z5J7U1XC] Voice sample Ok (score: 2.066 / 1.936[2.626] with token #1)
[Tue Nov 24 11:56:45.328857 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Updated user data
[Tue Nov 24 11:56:45.334469 2020] [192.168.3.218] [OpenOTP:Z5J7U1XC] Sent login success response
```

The last line, **Sent login success response** indicates the authentication worked.

*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*