VOICE REGISTRATION

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.

Voice Registration

iOS Android Voice Biometric Token

1. Overview

In this article, we will demonstrate how to record a **voice** to enable 2FA using **voice biometrics**.

To use **Voice Biometrics**, it is necessary **WebADM 2.0.*** and **OpenOTP** mobile application version **1.4.11** or higher for Android and version **1.4.13** or higher for **iOS**.

2. Voice Biometric 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 2 Web Applications: SelfDesk and SelfReg 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 have 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 under a **WebADM Administrator** request. To allow the user to access this application, the **Administrator** has to send a **Self-Registration** request to the user. Then, the user will receive an one-time link by mail or SMS to access the application.

Selfdesk application is accessible at any time by the end-user (if it is not locked in its configuration).

3.1 User Self-Registration

In this section, we will focus how to use **Self-Registration** for **Voice** registration. If you want a more complete understanding of how **Self Registration** works, you can check Self Registration documentation.

In **WebADM portal**, select the user you want under the LDAP tree, the user must be an actived user. Then click in the **User-Self-Registration** link on the right to send an **Self-Registration** link to the specific user.

In the next page, write a personalized message and set the parameters accordingly.

The user should receive an email with the registration link. After the user click in the link sent, he should enter his crendentials to login in the **Self-Registration portal**.

Once it is done, the user can start the **Voice Model** registration.

CLick in **Voice** tab, then **CLick to Start**

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 procedure is done, you should see the below message:

Then you can go to **Voice** tab again and check if there is a **voice biometrics** already registered.

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`

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.

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.

4. Authentication Test through the WebADM Admin GUI

Login on the WebADM admin GUI and click on 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 shoud 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.

We are authenticated!

5. Using Voice Biometrics with Credential Provider

In order to see **Voice Biometrics** working in a real scenario, we will test it with **Windows Credential Provider** plugin.

To make it works, we should enable **Push Login** in **MFA (OpenOTP)** application. Also, it is necessary that **OTP Type** is set to **VOICE** and **Mobile Voice Login** is set yo **Yes**. Lastly, the user must have a **Software Token** registered via **OpenOTP mobile** application.

Since we are testing using **Windows Credential Provider**, having Windows CP working is also a requirement here.

In Windows **OpenOTP** page, enter the LDAP credentials as usual:

After doing that, **WebADM** endpoint will be called:

Then the following notification should appear in your mobile phone:

After you click in the **Record** button, you have 5 seconds to enter your **Voice** authentication.

If everything works correctly, you should be able to login.

6. Logs

Now, we can check the logs using Voice Biometrics in a real scenario., 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 11:56:31.259121 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,OTPType=VOICE,PushLogin=Yes,PushVoice=Yes,BlockNotify=MAIL,ExpireNotif
```

```
1:HOTP-SHA1-6:QN06-
T1M,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:
77HxxxOzDKO2tE1K
[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.