



VOICE 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 Security.

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

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**.

The screenshot displays the WebADM Enterprise Edition v2.0.8 admin interface. On the left, an LDAP tree shows a list of users, with 'CN=aduser3' highlighted. The main panel shows the details for 'Object CN=aduser3, CN=Users, DC=adrcdevs, DC=com'. It includes sections for LDAP Actions, Object Details, and Application Actions. The 'Application Actions' section is expanded, showing 'MFA Authentication Server (14 actions)' highlighted. Below this, there are fields for 'Object Name' (aduser3), 'Add Attribute' (WebADM Voice Model), and 'Add Extension' (inetorgperson). A 'User Certificate' section shows details for 'Subject: adrcdevs\aduser3 (User)', 'Signer: WebADM CA #8759 (Serial 94)', and 'Status: Valid (Expires in 339 days)'. At the bottom, there are fields for 'First Name' (aduser3), 'Account Created' (07-07-2020), and 'Account Modified' (24-11-2020).

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



OpenOTP User Actions for `CN=aduser3,CN=Users,DC=adrcdevs,DC=com` (14)

Find below the user actions supported by **MFA Authentication Server** (OpenOTP).



Register / Unregister OTP Tokens

You must register a hardware or software Token before a user can start using it.



Register / Unregister FIDO Devices

You must register a FIDO Device before a user can start using it.



Register / Unregister Voice Biometrics

Enrol your voice fingerprint for voice biometrics authentication.



Resynchronize Tokens

Event-based and time-based tokens can get out of sync. You can use the action to resync the Token counter or clock drift.



Manage OTP PIN Prefix

Set an OTP PIN if you want the OTP passwords to be prepended by a static PIN password. Any OTP password will have to be prefixed by the static PIN code in the form [PIN][OTP].

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.

WebADM Enterprise Edition v2.0.8
Copyright © 2010-2020 RCDevs Security, All Rights Reserved

API     

[Home](#) | [Admin](#) | [Create](#) | [Search](#) | [Import](#) | [Databases](#) | [Statistics](#) | [Applications](#) | [About](#) | [Logout](#)

Register / Unregister Voice Biometrics for CN=aduser3,CN=Users,DC=adrcdevs,DC=com

You must register your voice fingerprint in order to authenticate with voice biometrics.
The registration simply consists in speaking several times the same secret passphrase.
The passphrase must be long enough (minimum 3 seconds).



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.

WebADM Enterprise Edition v2.0.8
Copyright © 2010-2020 RCDevs Security, All Rights Reserved

API     

[Home](#) | [Admin](#) | [Create](#) | [Search](#) | [Import](#) | [Databases](#) | [Statistics](#) | [Applications](#) | [About](#) | [Logout](#)

Register / Unregister Voice Biometrics for CN=aduser3,CN=Users,DC=adrcdevs,DC=com

Voice fingerprint has been registered

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

WebADM Voice Model
[add values] [delete attribute] [BIOMETRIC VOICE MODEL - 196 KBytes]

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 a 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 active user. Then click in the **User-Self-Registration** link on the right to send a **Self-Registration** link to the specific user.

The screenshot displays the WebADM Enterprise Edition v2.0.8 interface. On the left, a LDAP tree shows a list of users from CN=aduser12 to CN=aduser7, with CN=aduser3 selected and highlighted with a blue box. The main content area shows the details for the selected user, CN=aduser3, with the following sections:

- LDAP Actions:** Delete this object, Copy this object, Move this object, Export to LDIF, Change password, Create certificate, Unlock WebApp access, Advanced edit mode.
- Object Details:** Object class(es): webadmAccount, posixAccount, p...; WebADM settings: 4 settings [CONFIGURE]; WebADM data: 13 data [EDIT]; User activated: Yes Deactivate; Logs and inventory: WebApp, WebSrv, Inventory, Record.
- Application Actions:** Secure Password Reset (1 actions), User Self-Registration (1 actions) (highlighted with a blue box), MFA Authentication Server (14 actions), SMS Hub Server (1 actions), SSH Public Key Server (3 actions).

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



Send Registration Email / SMS for CN=aduser3,CN=Users,DC=adrcdevs,DC=com

Self-registration sends a one-time link to the user by email and/or SMS.
The link is usable only once and automatically expires after the expiration time specified below.
The SelfReg WebApp address contained in the link can be specified in the SelfReg configurations.

Username:

Domain:

Message Type:

Use Secure Mail: Yes No

Use SMS Type: Normal Flash

Link Expiration:

Message Comments:

Click in the link for self registration.
It will expire after 1 hour.

Restricted Application:

Focused Item:

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

User Self-Registration

Welcome to the Self-Registration Portal at *rcdevs*.
Your login password is required to continue.



Username:

Domain:

Password:

Login

Cancel



Provided by **RCDevs Security SA**

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

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

User Self-Registration

[Home](#) [OTP](#) [FIDO](#) [Voice](#) [OTP List](#) [App Keys](#) [SSH](#) [PKI](#) [Logout](#)

Hello aduser3.

Welcome to the Self-Registration Portal at *rcdevs*.

Manage your OTP Token or FIDO Device



- Download a Software/Mobile Token.
- Register your Hardware or Software Token.
- Resynchronize your Hardware or Software Token.
- Test login with your Hardware or Software Token.

Manage your SSH Key



- Register or renew your SSH private key.
- Download your SSH public key for external use.



Provided by **RCDevs Security SA**

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:

User Self-Registration

Your voice fingerprint has been registered

Ok



Provided by **RCDevs Security SA**

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

WebADM Voice Model
[add values] [delete attribute]

[BIOMETRIC VOICE MODEL - 196 KBytes]

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.

User Self-Service Desk

Welcome to the Self-Service Portal at *rcdevs*.
Please enter the required information to login.



Username:

Password:

Domain:

Provided by **RCDevs Security SA**

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

User Self-Service Desk

[Home](#) [OTP](#) [FIDO](#) [App Keys](#) [SSH](#) [SSO](#) [PKI](#) [Logout](#)



Register OTP Token(s) to authenticate at *rcdevs*.

Move your cursor on the (i) icons below for more information.

Authentication Settings

Primary OTP Method: **Voice**
Fallback OTP Method: **Not Set**
OTP Challenge Timeout: **90 Seconds**
Enable Push Login: Yes No 

View My Voice Biometrics

Voice Login Status:



[Click to Register](#)

User Statistics

Login Count: **8 success & 4 failure**
Last Login: **2020-11-24 11:56:45**
Blocking Status: **Account active (0 login failed)**



[Download Token](#)



[Register Token](#)



[Resync Token](#)



[Test Login](#)



[Build OTP List](#)



Provided by [RCDevs Security SA](#)

Change [View My](#) to [Voice Biometrics](#). Then click in [Click to Register](#)

User Self-Service Desk

[Home](#) [OTP](#) [FIDO](#) [App Keys](#) [SSH](#) [SSO](#) [PKI](#) [Logout](#)



Register OTP Token(s) to authenticate at *rcdevs*.
Move your cursor on the (i) icons below for more information.

Authentication Settings

Primary OTP Method: **Voice**
Fallback OTP Method: **Not Set**
OTP Challenge Timeout: **90 Seconds**
Enable Push Login: Yes No 

View My **Voice Biometrics**

Voice Login Status:



[Click to Register](#)

User Statistics

Login Count: **8 success & 4 failure**
Last Login: **2020-11-24 11:56:45**
Blocking Status: **Account active (0 login failed)**



[Download Token](#)



[Register Token](#)



[Resync Token](#)



[Test Login](#)



[Build OTP List](#)



Provided by [RCDevs Security SA](#)

User Self-Service Desk

The voice registration consists in speaking several times the same secret passphrase. To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
Or: *My name is aduser3 and my voice is my password.*



 Provided by **RCDevs Security SA**

User Self-Service Desk

Your voice fingerprint has been registered

 Provided by **RCDevs Security SA**

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.

User Self-Service Desk

🏠 Home
OTP
FIDO
App Keys
SSH
SSO
PKI
Logout

Register OTP Token(s) to authenticate at *rcdevs*.
Move your cursor on the (i) icons below for more information.

Authentication Settings

Primary OTP Method: **Voice**

Fallback OTP Method: **Not Set**

OTP Challenge Timeout: **90 Seconds**

Enable Push Login: Yes No (i)

View My Voice Biometrics

Voice Login Status: Ok (Unregister)

User Statistics

Login Count: **8 success & 4 failure**

Last Login: **2020-11-24 11:56:45**

Blocking Status: **Account active (0 login failed)**

[Download Token](#)

[Register Token](#)

[Resync Token](#)

[Test Login](#)

[Build OTP List](#)

Provided by **RCDevs Security SA**

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**

The screenshot shows the WebADM Admin GUI interface. On the left, a tree view lists users from CN=aduser12 to CN=aduser7, with CN=aduser3 selected. The main panel displays details for 'Object CN=aduser3,CN=Users,DC=adrcdevs,DC=com'. The 'WebADM settings' section is highlighted with a blue box and contains the text '4 settings [CONFIGURE]'. Other sections include 'LDAP Actions' and 'Application Actions'.

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

Application Settings for CN=aduser3,CN=Users,DC=adrcdevs,DC=com

Applications

- ✓ **MFA Authentication Server (4)**
- SSH Public Key Server
- OpenID & SAML Provider
- Secure Password Reset
- User Self-Service Desk
- User Self-Registration

Authentication Policy

Login Mode LDAPOTP (Default) ▾

The login mode (required login factors) should be adjusted via Client Policies.

- LDAPOTP: Require both LDAP and OTP passwords.
- LDAPU2F: Require both LDAP and FIDO response.
- LDAPMFA: Require LDAP and either OTP or FIDO.
- LDAP: Require LDAP password only.
- OTP: Require OTP password only.

OTP Type VOICE ▾

- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
- SMS: SMS one-time password (On-demand or Prefetched).
- MAIL: Email one-time password (On-demand or Prefetched).
- LIST: Pre-generated OATH OTP password list (to be printed).
- VOICE: Voice biometrics authenticaton (requires license option).
- PROXY: Forward requests to another RADIUS server (for migrations).

OTP Fallback TOKEN ▾

Fallback OTP Type to be used as secondary authentication method.
SMS/MAIL OTPs are delayed for MobileTimeout seconds before being sent.

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**

WebADM Enterprise Edition v2.0.8
Copyright © 2010-2020 RCDevs Security, All Rights Reserved

Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Object CN=aduser3,CN=Users,DC=adrcdevs,DC=com ⓘ

LDAP Actions	Object Details	Application Actions
<ul style="list-style-type: none"> 🗑 Delete this object 📄 Copy this object 📄 Move this object 📄 Export to LDIF 🔍 Change password ⚙ Create certificate 🔒 Unlock WebApp access 🔧 Advanced edit mode 	<p>Object class(es): webadmAccount, posixAccount, p...</p> <p>WebADM settings: 4 settings [CONFIGURE]</p> <p>WebADM data: 13 data [EDIT]</p> <p>User activated: Yes Deactivate ⓘ</p> <p>Logs and inventory: WebApp, WebSrv, Inventory, Record</p>	<ul style="list-style-type: none"> Secure Password Reset (1 actions) User Self-Registration (1 actions) <li style="border: 2px solid blue;">MFA Authentication Server (14 actions) SMS Hub Server (1 actions) SSH Public Key Server (3 actions)

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



action to set or reset the PIN code on the user account.



Manage Emergency OTP

An emergency OTP is an auto-expirable static OTP which can be used when the user cannot use his usual OTP/FIDO method and requires a temporary access.



Manage Printed OTP List

You can use this action to register, remove, display and download user OTP Lists.



Manage Application Passwords

You can use this action to register, remove and display per-application passwords.



Unblock Account

You can use this action to unblock an account after the max authentication attempts has been reached.



Import OATH-PSKC File

You can use the action to import a PSKC (RFC-6030) OATH Token key file.



Export OATH-PSKC File

You can use the action to export the registered OATH Token to a PSKC (RFC-6030) file.



Test User Authentication

You can use this action to test a user authentication with OpenOTP.



Test User Confirmation

You can use this action to test a transaction confirmation with OpenOTP.

Cancel

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



System: Linux 4.18.0-193.14.2.el8_2.x86_64 x86_64 (64 bit)
Listener: 192.168.3.171:8080 (HTTP/1.1 SSL)
Uptime: 14339s (0 days)
Cluster Node: 1/1 (Session Server)
Local Memory: 1M (33M total)
Shared Memory: 1M (256M total)
Connectors: OK (4 alive & 0 down)

Login Method: Normal Simple

Username:

Domain:

LDAP Password:

OTP Password:

Simulated Client:

Simulated Source:

Simulated Options:

Request Settings:

Virtual Attributes:

Browser Context:

Debug Mode: (enable debug logs for this request)

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!



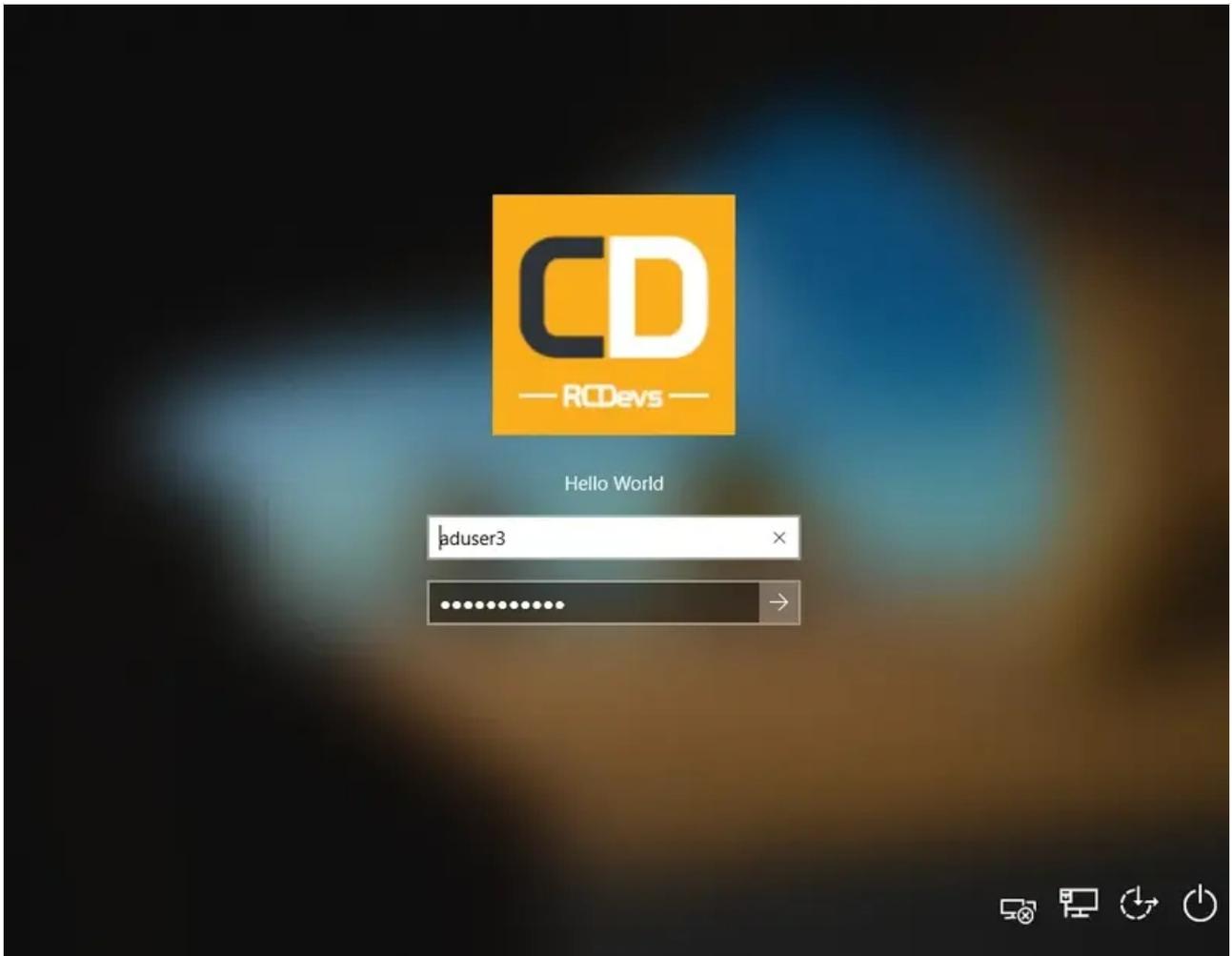
5. Using Voice Biometrics with Credential Provider

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

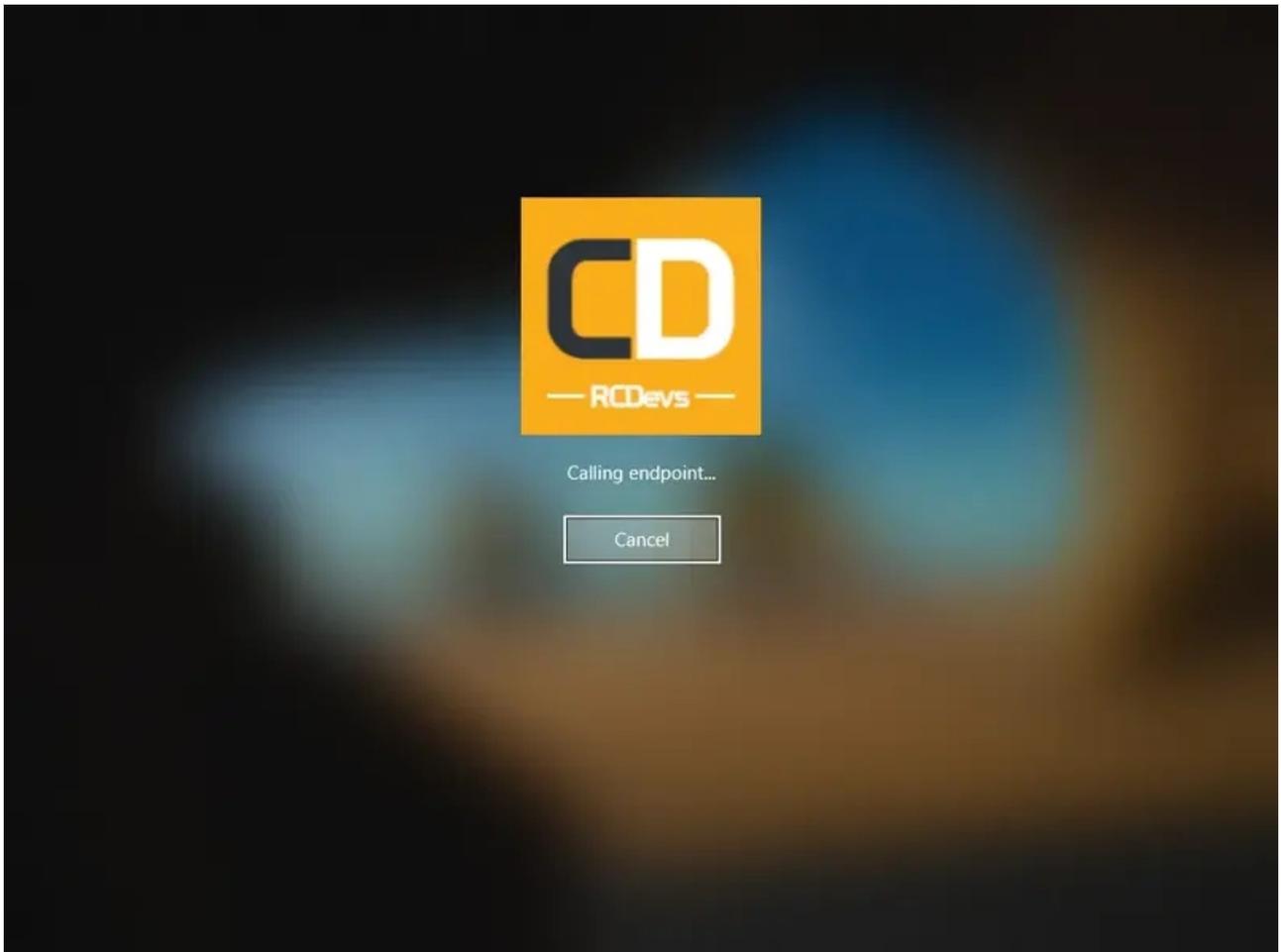
To make it work, we should enable **Push Login** in **MFA (OpenOTP)** application. Also, it is necessary that **OTP Type** is set to **VOICE** and **Mobile Voice Login** is set to **Yes**. Lastly, the user must have a **Software Token** registered via **OpenOTP mobile** application.

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:



192.168.3.218
Primary Token (aduser3)

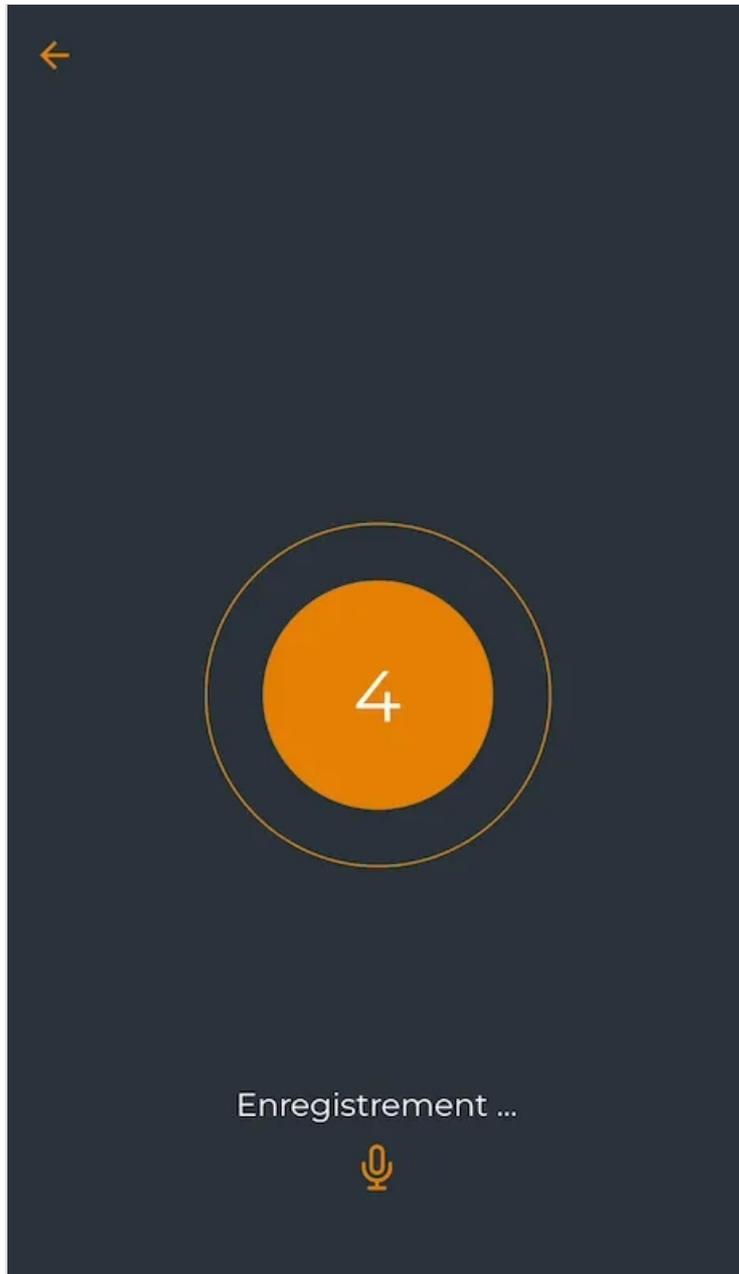


Source inconnue

Record

Rejeter

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 log in.



Connexion réussie !

Vous êtes connecté à 192.168.3.218



Welcome

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:

```
[Tue Nov 24 11:56:31.259121 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] New openotpSimpleLogin SOAP request
[Tue Nov 24 11:56:31.259176 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] > Username: aduser3
[Tue Nov 24 11:56:31.259184 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] > Domain: adrodevs.com
[Tue Nov 24 11:56:31.259219 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] > Password: xxxxxxxxxx
[Tue Nov 24 11:56:31.259232 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] > Options: -LDAP,OFFLINE,NOVOICE
[Tue Nov 24 11:56:31.259254 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Registered openotpSimpleLogin request
[Tue Nov 24 11:56:31.259574 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Resolved LDAP user: CN=aduser3,CN=Users,DC=adrodevs,DC=com (cached)
[Tue Nov 24 11:56:31.259651 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Resolved LDAP groups: group2,remote desktop users
[Tue Nov 24 11:56:31.270757 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Started transaction lock for user
[Tue Nov 24 11:56:31.283882 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Found user fullname: aduser3
[Tue Nov 24 11:56:31.283912 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Found 1 user mobiles: +352 691
[Tue Nov 24 11:56:31.283921 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Found 1 user emails: aduser3@adrodevs.com
[Tue Nov 24 11:56:31.284501 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Found 49 user settings: LoginMode=LDAPOTP,OTPType=VOICE,PushLogin=Yes,PushVoice=Yes,BlockNotify=MAIL,ExpireNotify=MAIL,ChallengeMode=Yes
[Tue Nov 24 11:56:31.285679 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Found 6 user data: VoiceState,TokenType,TokenKey,TokenState,TokenID,TokenSerial
[Tue Nov 24 11:56:31.285783 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Found 1 registered OTP token (TOTP)
[Tue Nov 24 11:56:31.287052 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Requested login factors: OTP
[Tue Nov 24 11:56:31.287274 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Authentication challenge required
[Tue Nov 24 11:56:31.409081 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Sent push notification for token #1
[Tue Nov 24 11:56:31.409111 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Waiting 28 seconds for mobile response
[Tue Nov 24 11:56:44.612725 2020] [192.168.3.172] [OpenOTP:ESJ7U1XC] Received mobile voice response from 192.170.3.17
[Tue Nov 24 11:56:44.612756 2020] [192.168.3.172] [OpenOTP:ESJ7U1XC] > Session: 77E8xx0zDK02LEIK
[Tue Nov 24 11:56:44.612764 2020] [192.168.3.172] [OpenOTP:ESJ7U1XC] > Sample: 152368 Bytes
[Tue Nov 24 11:56:44.612770 2020] [192.168.3.172] [OpenOTP:ESJ7U1XC] Found authentication session started 2020-11-24 11:56:31
[Tue Nov 24 11:56:45.318400 2020] [192.168.3.172] [OpenOTP:ESJ7U1XC] 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:ESJ7U1XC] Updated user data
[Tue Nov 24 11:56:45.334469 2020] [192.168.3.218] [OpenOTP:ESJ7U1XC] Sent login success response
```

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: xxxxxxxxxxxx

[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,ExpireNotify=MAIL 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.

This manual was prepared with great care. However, RCDevs Security 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 Security 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 Security 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 Security S.A. The latter especially applies for data processing systems. RCDevs Security 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 Security. © 2024 RCDevs Security S.A., All Rights Reserved