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 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.

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…).

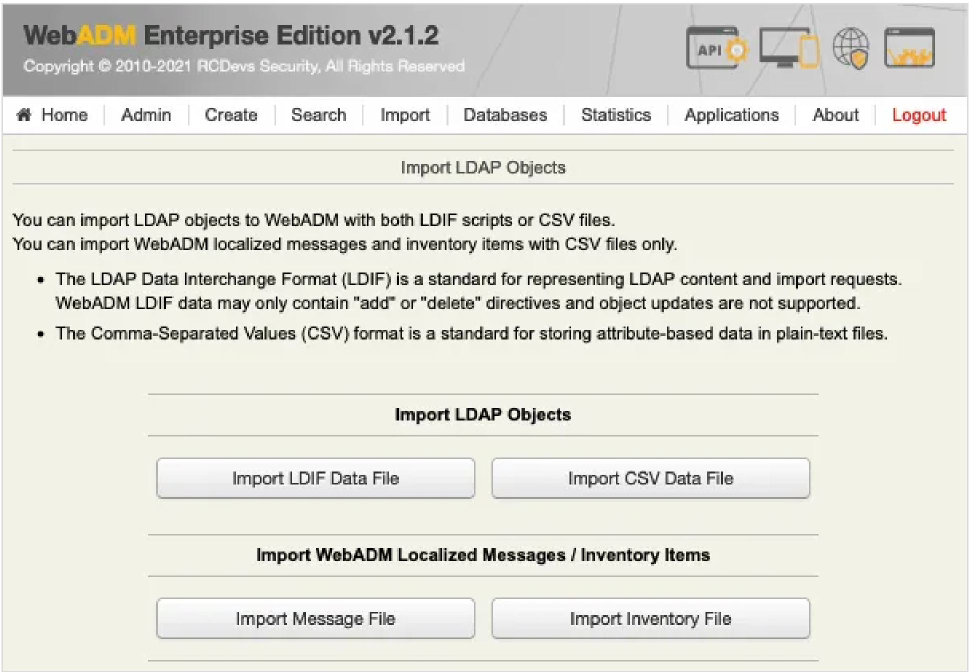
2. Admin Enrollment through the WebADM Admin GUI

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`.


WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
API
Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

Import LDAP Objects

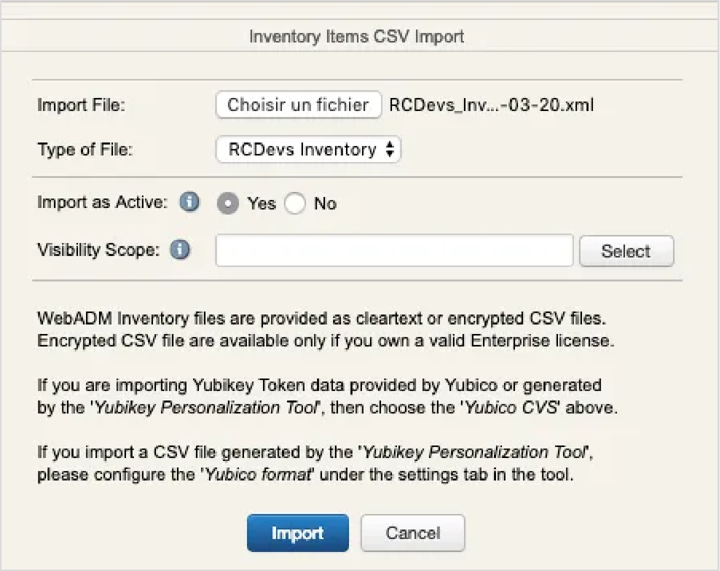
You can import LDAP objects to WebADM with both LDIF scripts or CSV files.
You can import WebADM localized messages and inventory items with CSV files only.

- The LDAP Data Interchange Format (LDIF) is a standard for representing LDAP content and import requests. WebADM LDIF data may only contain "add" or "delete" directives and object updates are not supported.
- The Comma-Separated Values (CSV) format is a standard for storing attribute-based data in plain-text files.

Import LDAP Objects

Import WebADM Localized Messages / Inventory Items

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



Inventory Items CSV Import

Import File: Choisir un fichier RCDevs_Inv...-03-20.xml

Type of File: RCDevs Inventory

Import as Active: ● Yes ○ No

Visibility Scope: Select

WebADM Inventory files are provided as cleartext or encrypted CSV files.
Encrypted CSV file are available only if you own a valid Enterprise license.

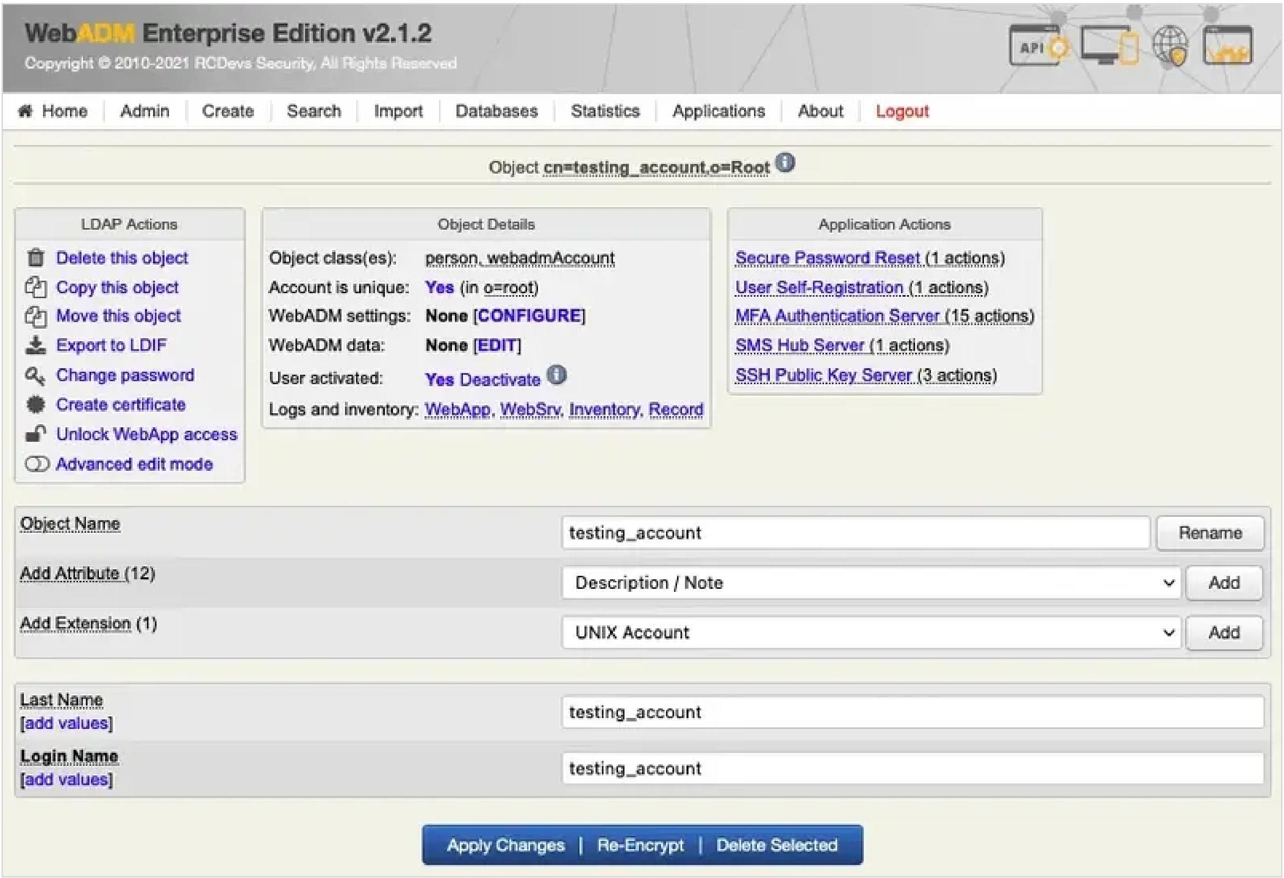
If you are importing Yubikey Token data provided by Yubico or generated by the '*Yubikey Personalization Tool*', then choose the '*Yubico CVS*' above.

If you import a CSV file generated by the '*Yubikey Personalization Tool*', please configure the '*Yubico format*' under the settings tab in the tool.

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`.



WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

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

Object cn=testing_account,o=Root

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

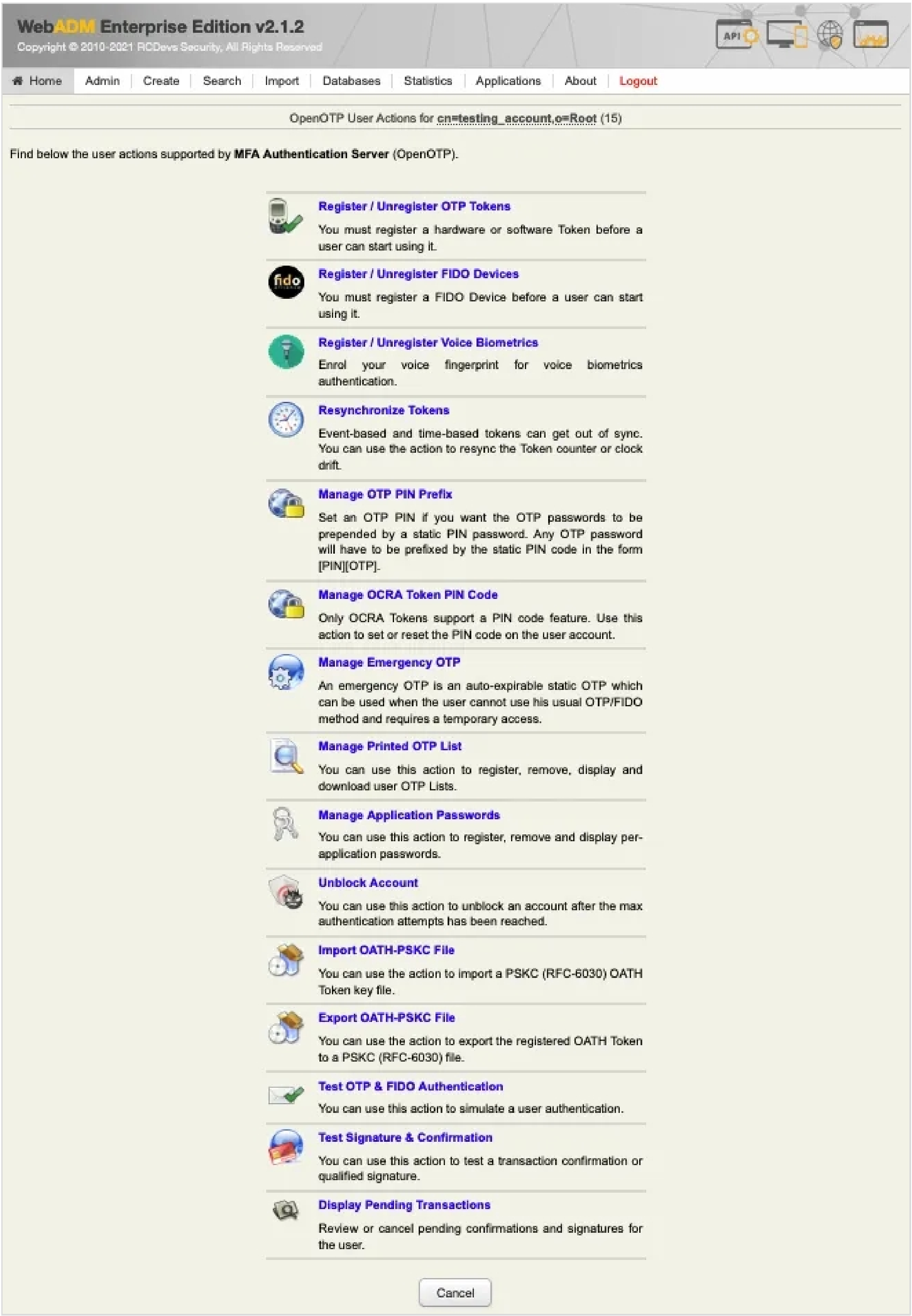
Object class(es): person, webadmAccount
Account is unique: Yes (in o=root)
WebADM settings: None [CONFIGURE]
WebADM data: None [EDIT]
User activated: Yes Deactivate
Logs and inventory: WebApp, WebSrv, Inventory, Record

Application Actions
- Secure Password Reset (1 actions)
- User Self-Registration (1 actions)
- MFA Authentication Server (15 actions)
- SMS Hub Server (1 actions)
- SSH Public Key Server (3 actions)

Object Name: testing_account (Rename)
Add Attribute (12): Description / Note (Add)
Add Extension (1): UNIX Account (Add)

Last Name [add values]: testing_account
Login Name [add values]: testing_account

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



WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

OpenOTP User Actions for cn=testing_account,o=Root (15)

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].

Manage OCRA Token PIN Code
Only OCRA Tokens support a PIN code feature. Use this 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.

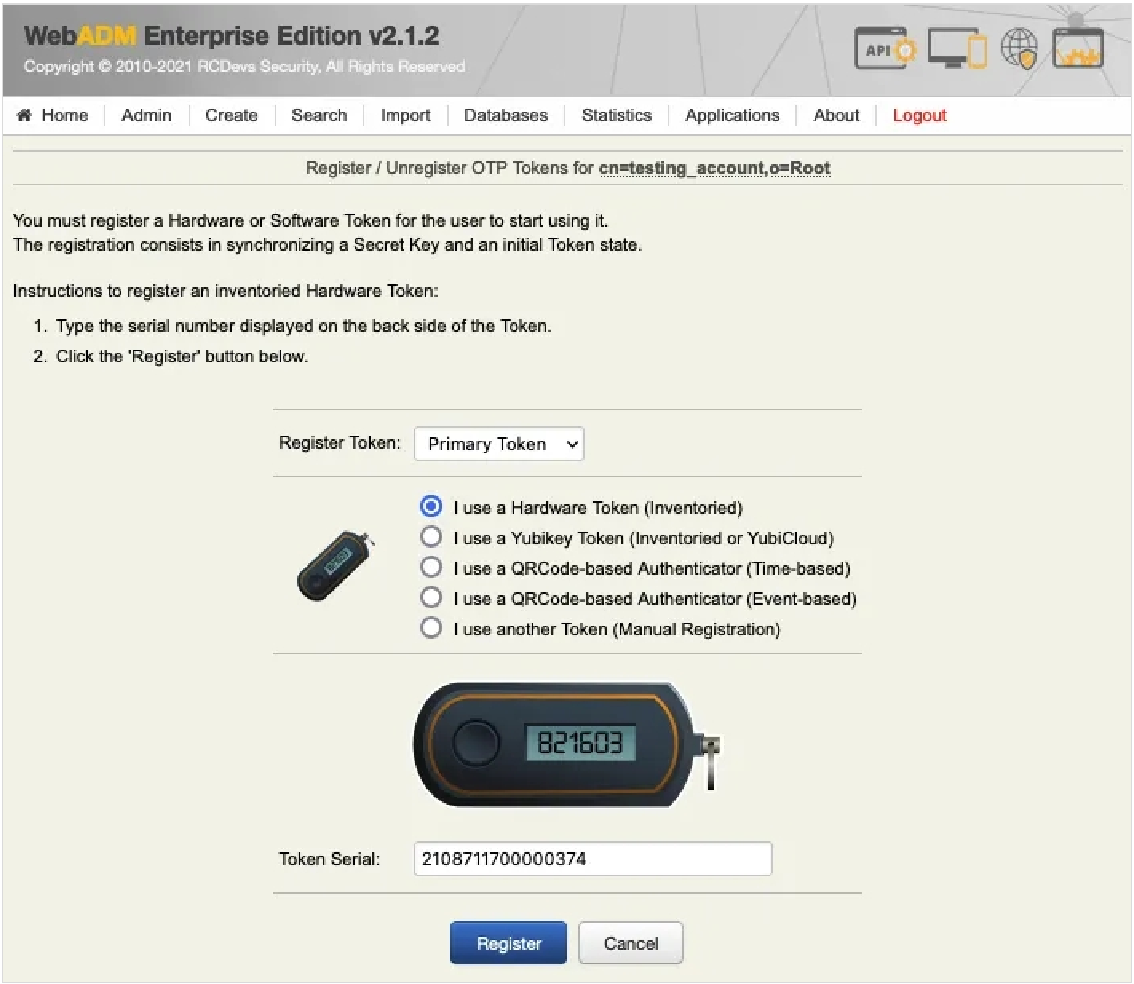
Export OATH-PSKC File
You can use the action to export the registered OATH Token to a PSKC (RFC-6030) file.

Test OTP & FIDO Authentication
You can use this action to simulate a user authentication.

Test Signature & Confirmation
You can use this action to test a transaction confirmation or qualified signature.

Display Pending Transactions
Review or cancel pending confirmations and signatures for the user.

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


WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

Register / Unregister OTP Tokens for cn=testing_account,o=Root

You must register a Hardware or Software Token for the user to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register an inventoried Hardware Token:

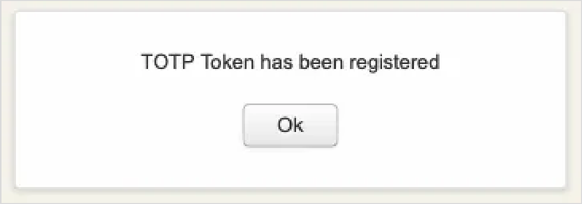
1. Type the serial number displayed on the back side of the Token.
2. Click the 'Register' button below.

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)

Token Serial: 2108711700000374

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

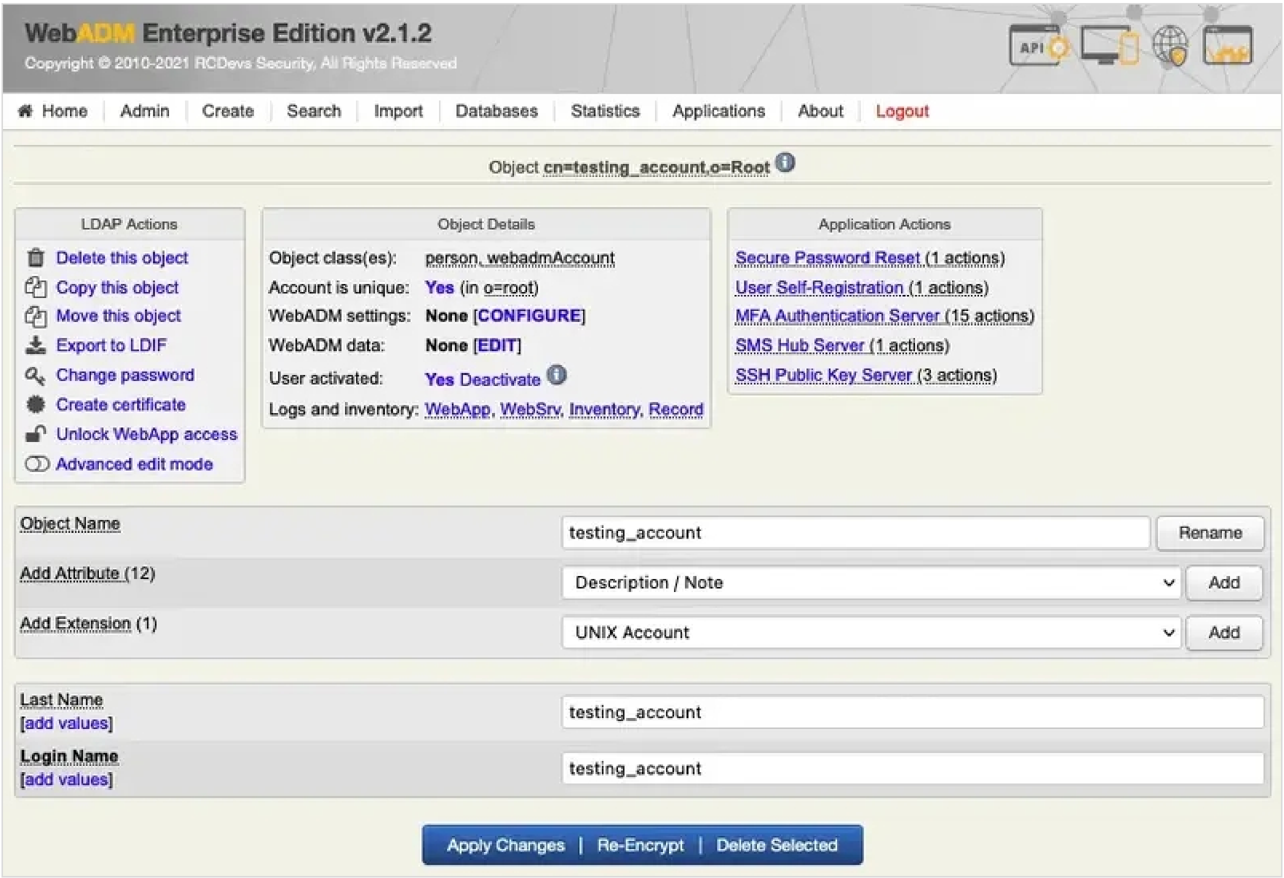


TOTP Token has been registered

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`.


WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
API
Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout
LDAP Actions
Delete this object
Copy this object
Move this object
Export to LDIF
Change password
Create certificate
Unlock WebApp access
Advanced edit mode
Rename
Add
Add
Apply Changes | Re-Encrypt | Delete Selected

Object cn=testing_account,o=Root

Object Details

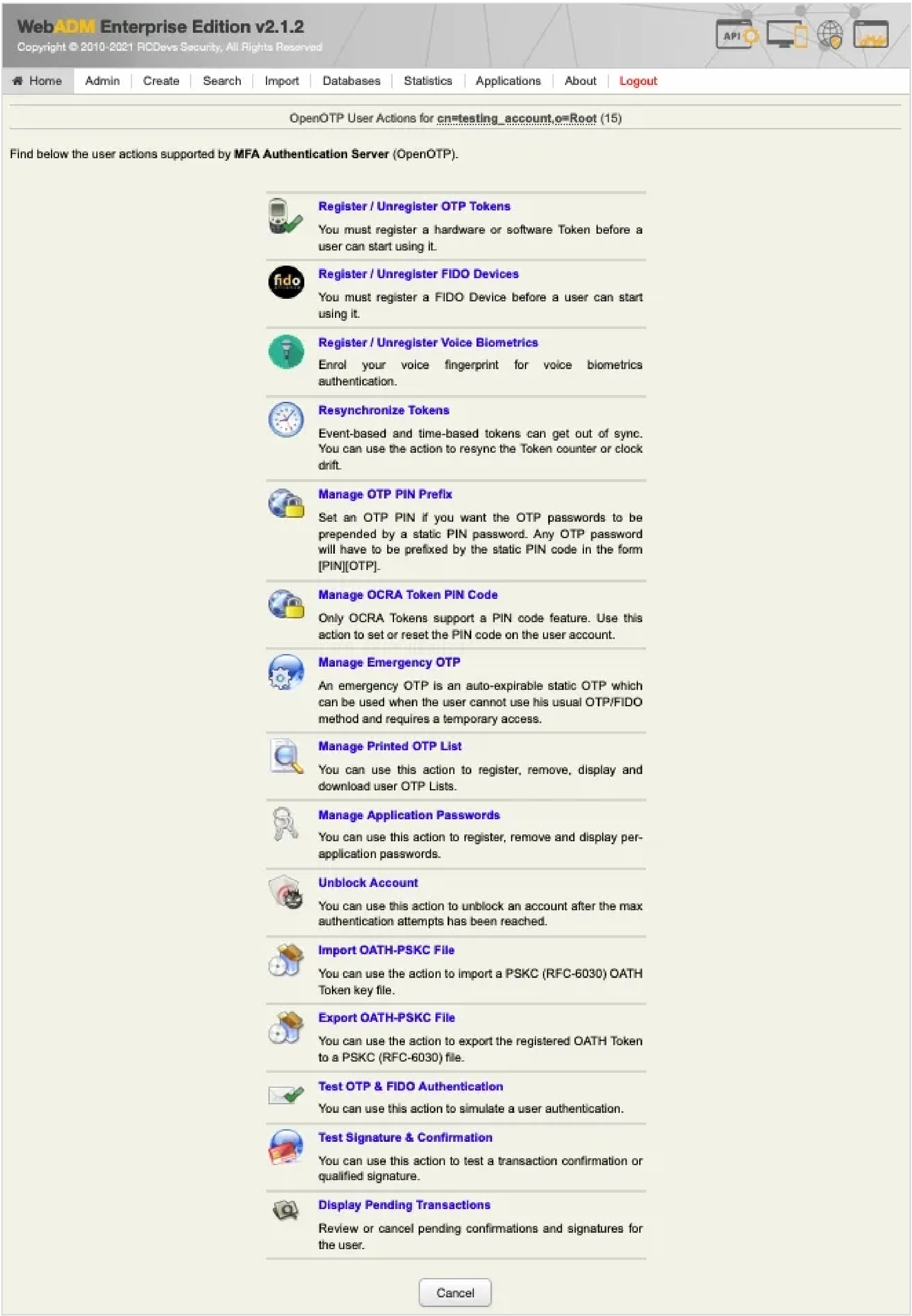
Object class(es):	person, webadmAccount
Account is unique:	Yes (in o=root)
WebADM settings:	None [CONFIGURE]
WebADM data:	None [EDIT]
User activated:	Yes Deactivate
Logs and inventory:	WebApp, WebSrv, Inventory, Record

Application Actions

- Secure Password Reset (1 actions)
- User Self-Registration (1 actions)
- MFA Authentication Server (15 actions)
- SMS Hub Server (1 actions)
- SSH Public Key Server (3 actions)

Object Name	testing_account
Add Attribute (12)	Description / Note
Add Extension (1)	UNIX Account
Last Name [add values]	testing_account
Login Name [add values]	testing_account

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


WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
API
Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout
Cancel

OpenOTP User Actions for cn=testing_account,o=Root (15)

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].

Manage OCRA Token PIN Code
Only OCRA Tokens support a PIN code feature. Use this 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.

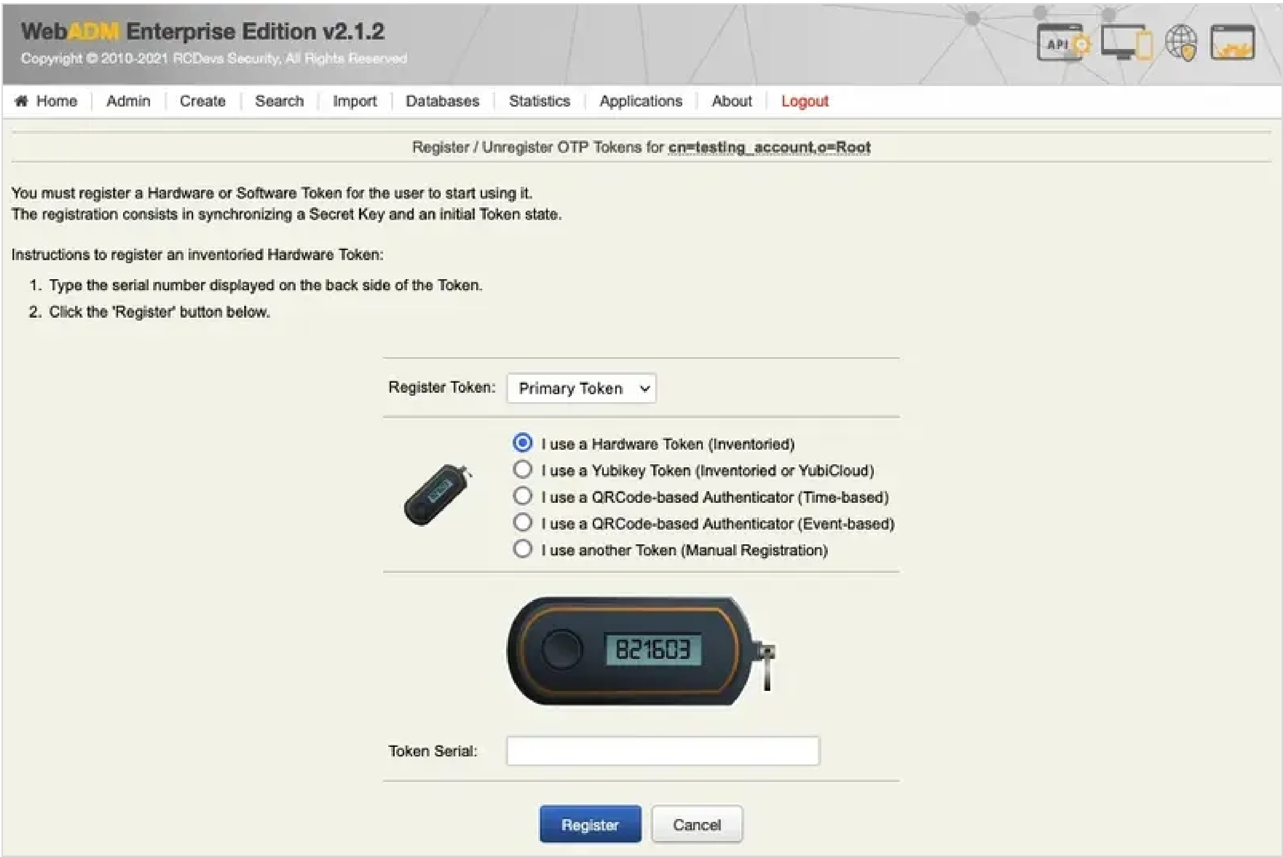
Import OATH-PSKC File
You can use the action to import a PSKC (RFC-6030) OATH Token key file.

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

Test OTP & FIDO Authentication
You can use this action to simulate a user authentication.

Test Signature & Confirmation
You can use this action to test a transaction confirmation or qualified signature.

Display Pending Transactions
Review or cancel pending confirmations and signatures for the user.


WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout
821603
Register
Cancel

Register / Unregister OTP Tokens for cn=testing_account,o=Root

You must register a Hardware or Software Token for the user to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register an inventoried Hardware Token:

1. Type the serial number displayed on the back side of the Token.
2. Click the 'Register' button below.

Register Token: Primary Token

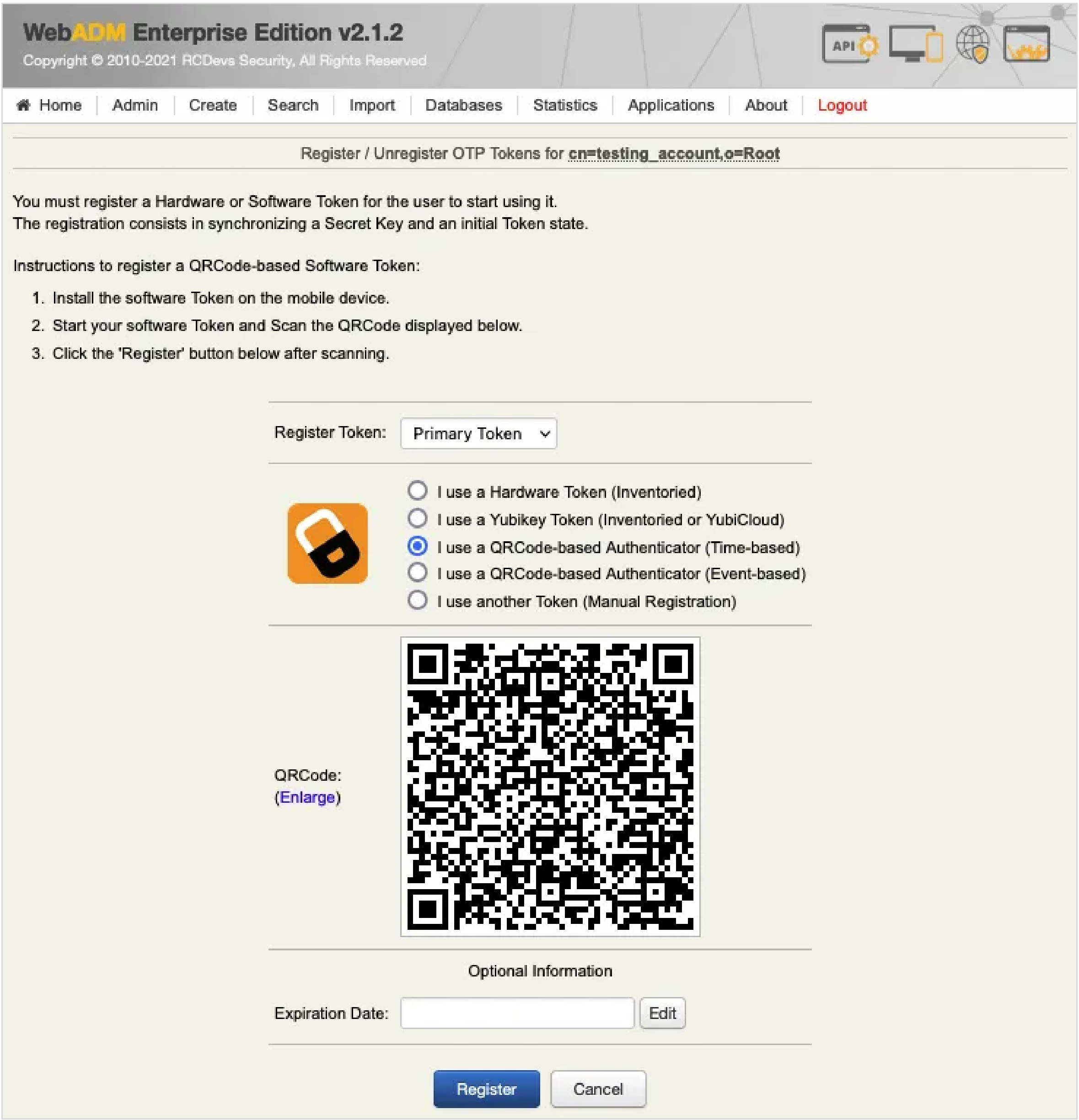
● I use a Hardware Token (Inventoried)
○ I use a Yubikey Token (Inventoried or YubiCloud)
○ I use a QRCode-based Authenticator (Time-based)
○ I use a QRCode-based Authenticator (Event-based)
○ I use another Token (Manual Registration)

Token Serial:

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.



WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Register / Unregister OTP Tokens for cn=testing_account,o=Root

You must register a Hardware or Software Token for the user to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register a QRCode-based Software Token:

1. Install the software Token on the mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. Click the 'Register' button below after scanning.

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: Edit

⚠ 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.

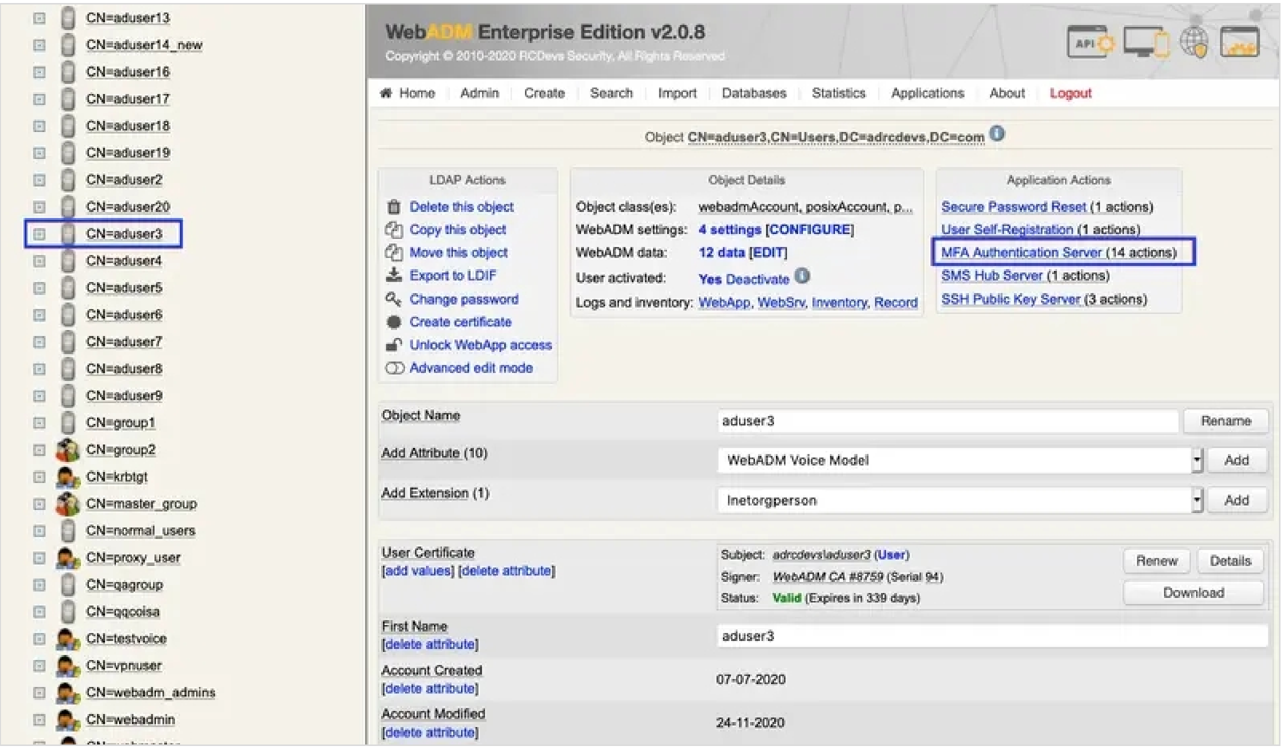
⚠ Push Token enrollment

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 log in 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`.



CN=aduser13
CN=aduser14_new
CN=aduser16
CN=aduser17
CN=aduser18
CN=aduser19
CN=aduser2
CN=aduser20
CN=aduser3
CN=aduser4
CN=aduser5
CN=aduser6
CN=aduser7
CN=aduser8
CN=aduser9
CN=group1
CN=group2
CN=krbtgt
CN=master_group
CN=normal_users
CN=proxy_user
CN=qagroup
CN=qqcoisa
CN=testvoice
CN=vpnuser
CN=webadm_admins
CN=webadmin

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

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

LDAP Actions
- Delete this object
- Copy this object
- Move this object
- Export to LDIF
- Change password
- Create certificate
- Unlock WebApp access
- Advanced edit mode

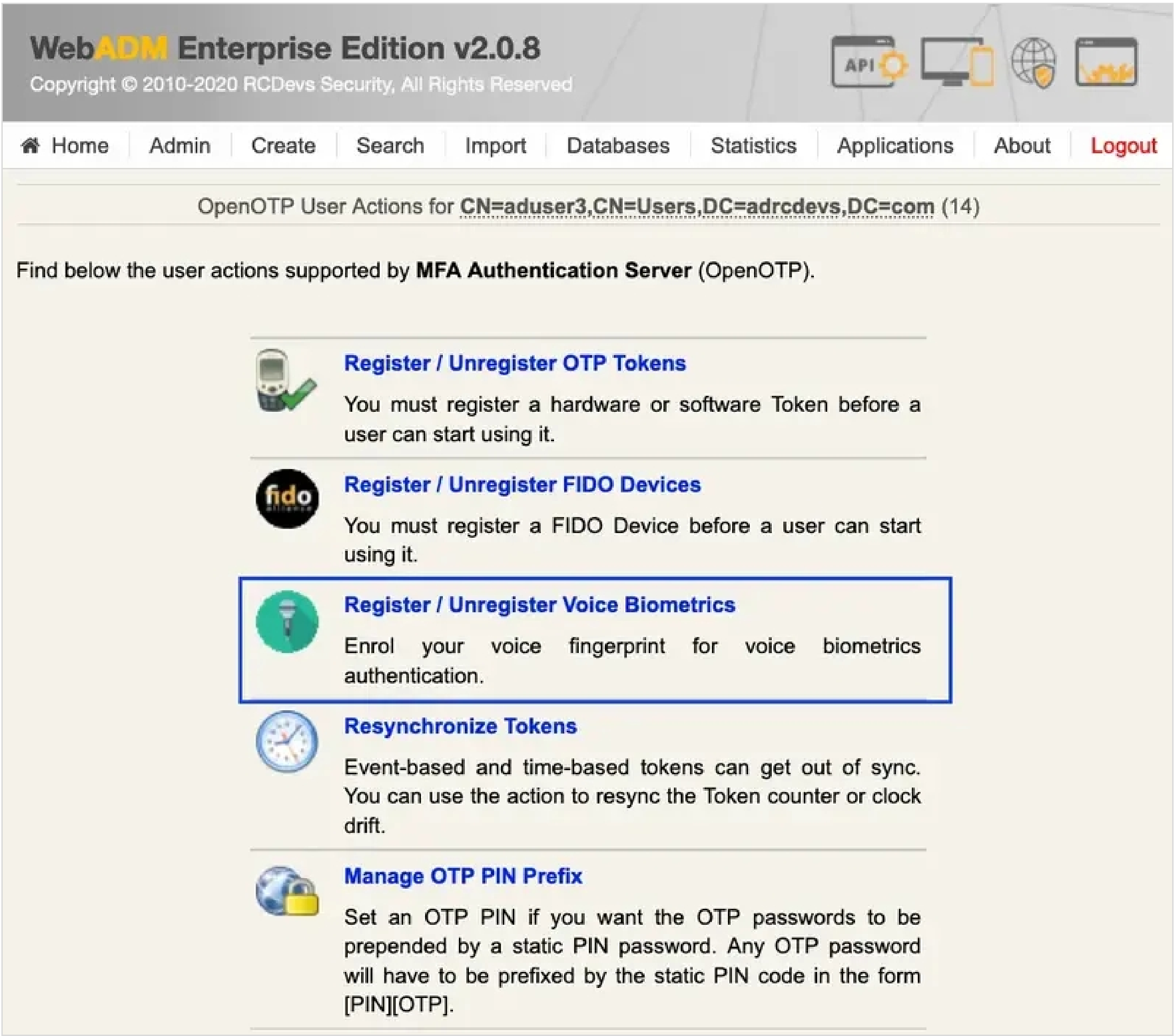
Object Details

Object class(es): webadmAccount, posixAccount, p...
WebADM settings: 4 settings [CONFIGURE]
WebADM data: 12 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)
- MFA Authentication Server (14 actions)
- SMS Hub Server (1 actions)
- SSH Public Key Server (3 actions)

Object Name	aduser3 [Rename]
Add Attribute (10)	WebADM Voice Model [Add]
Add Extension (1)	Inetorgperson [Add]
User Certificate [add values] [delete attribute]	Subject: adrcdevs\aduser3 (User) Signer: WebADM CA #8759 (Serial 94) Status: Valid (Expires in 339 days) [Renew] [Details] [Download]
First Name [delete attribute]	aduser3
Account Created [delete attribute]	07-07-2020
Account Modified [delete attribute]	24-11-2020

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


WebADM Enterprise Edition v2.0.8
Copyright © 2010-2020 RCDevs Security, All Rights Reserved
Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

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.

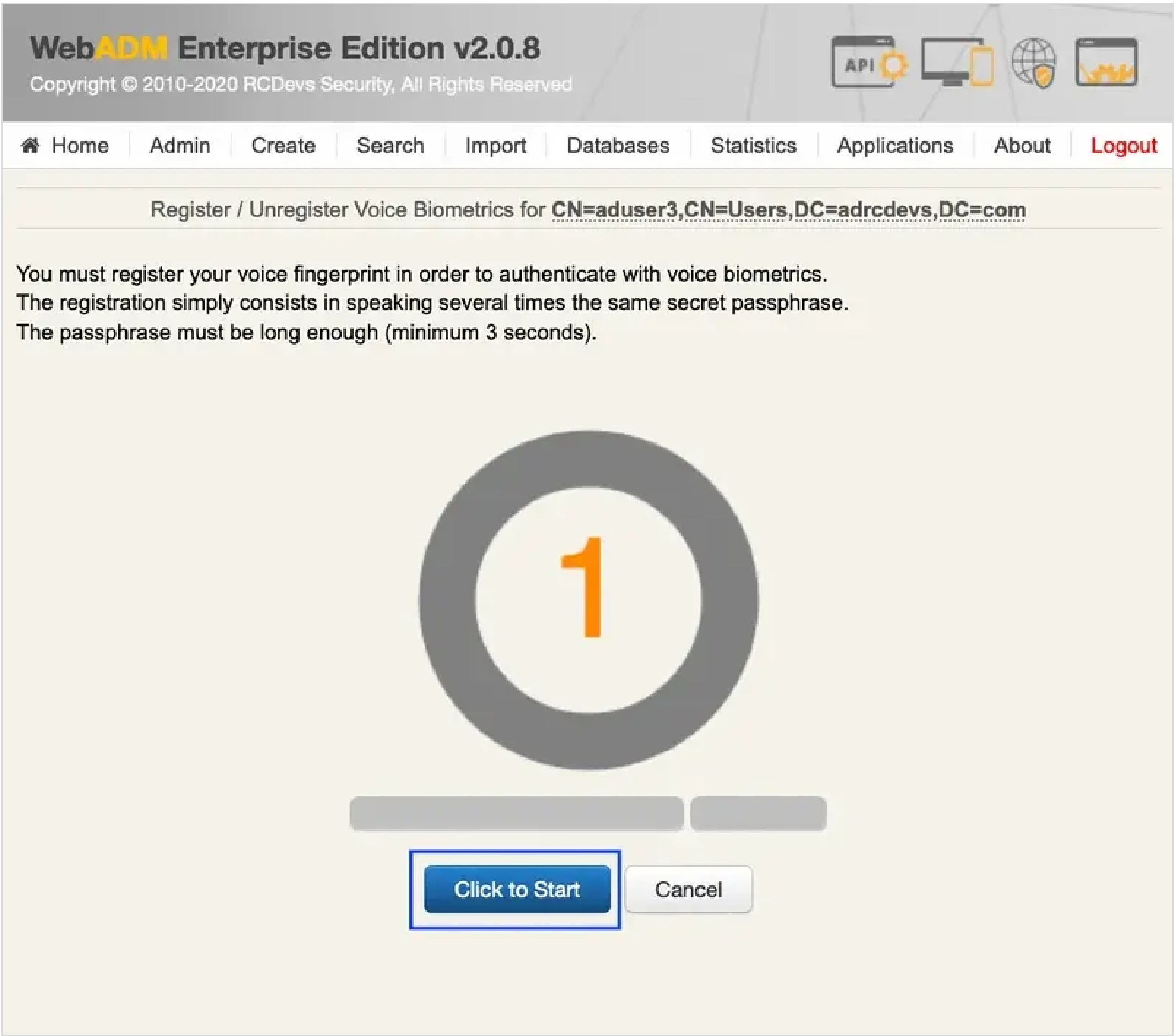
Register / Unregister FIDO Devices
You must register a FIDO Device before a user can start using it.

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].

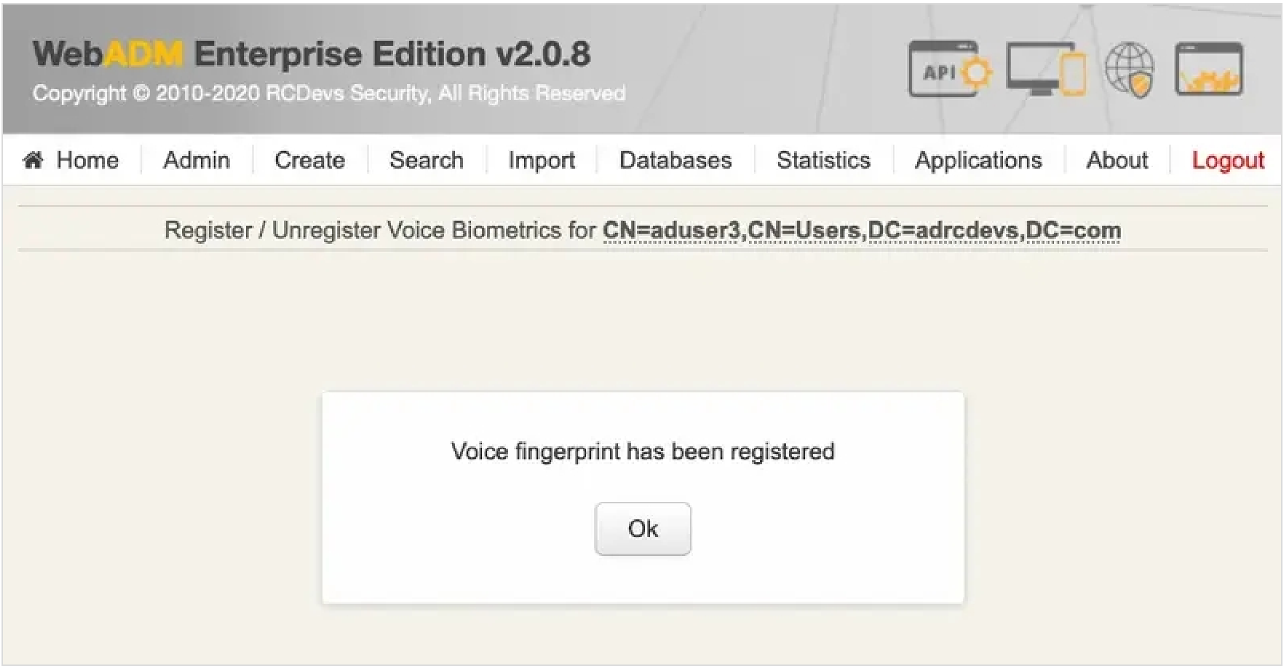
In that page, click in `Click to Start`, then record your **voice biometric**. It is recommended you use an earphone with microphone or other kind of dedicated audio input device.



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).

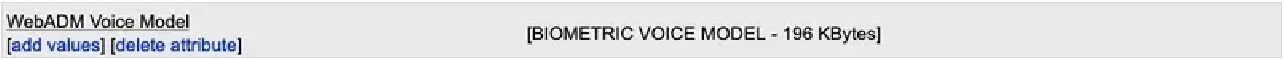
To make sure it will not be misunderstood by **OpenOTP**, you have to repeat your voice biometric 4 times and not use too short messages.


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
Ok

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 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:

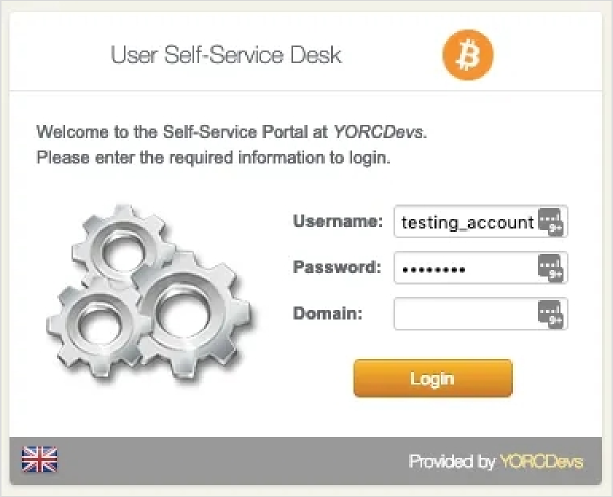
```
https://YOUR_WAPROXY/selfdesk/login_uid.php
```

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.



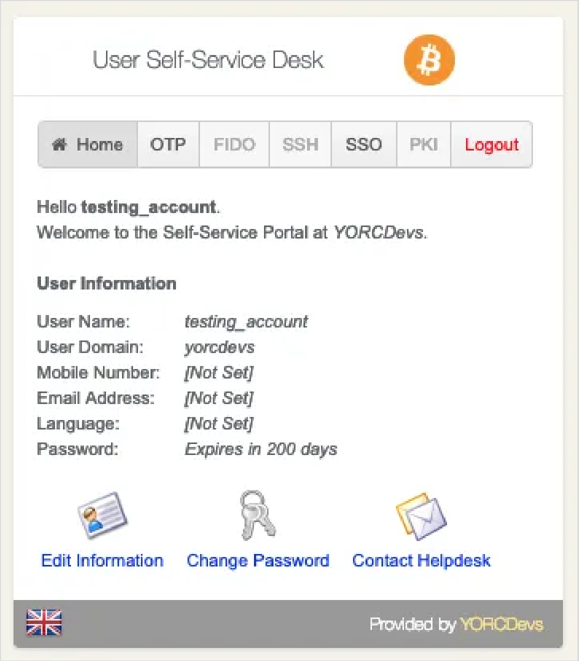
User Self-Service Desk

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

Username: testing_account

Password: ••••••••

Domain:



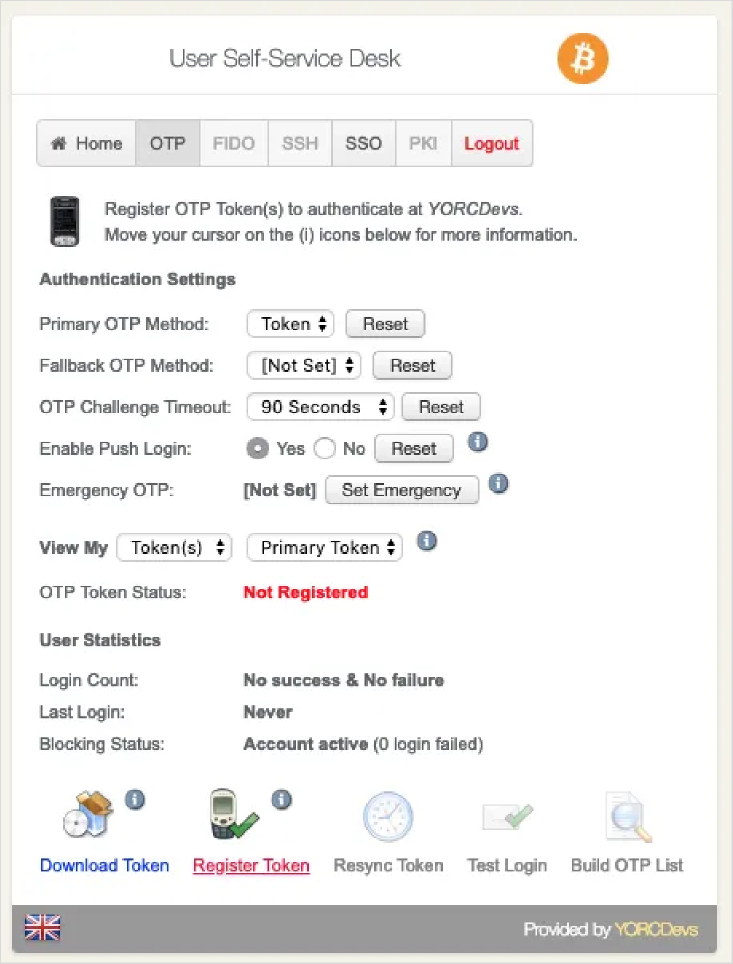
User Self-Service Desk

Hello **testing_account**.
Welcome to the Self-Service Portal at *YORCDevs*.

User Information

User Name:	*testing_account*
User Domain:	*yorcdevs*
Mobile Number:	*[Not Set]*
Email Address:	*[Not Set]*
Language:	*[Not Set]*
Password:	*Expires in 200 days*

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



User Self-Service Desk

Home | OTP | FIDO | SSH | SSO | PKI | Logout

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

Authentication Settings

Primary OTP Method:	Token ◆ Reset
Fallback OTP Method:	[Not Set] ◆ Reset
OTP Challenge Timeout:	90 Seconds ◆ Reset
Enable Push Login:	● Yes ○ No Reset (i)
Emergency OTP:	**[Not Set]** Set Emergency (i)

View My Token(s) ◆ Primary Token ◆ (i)

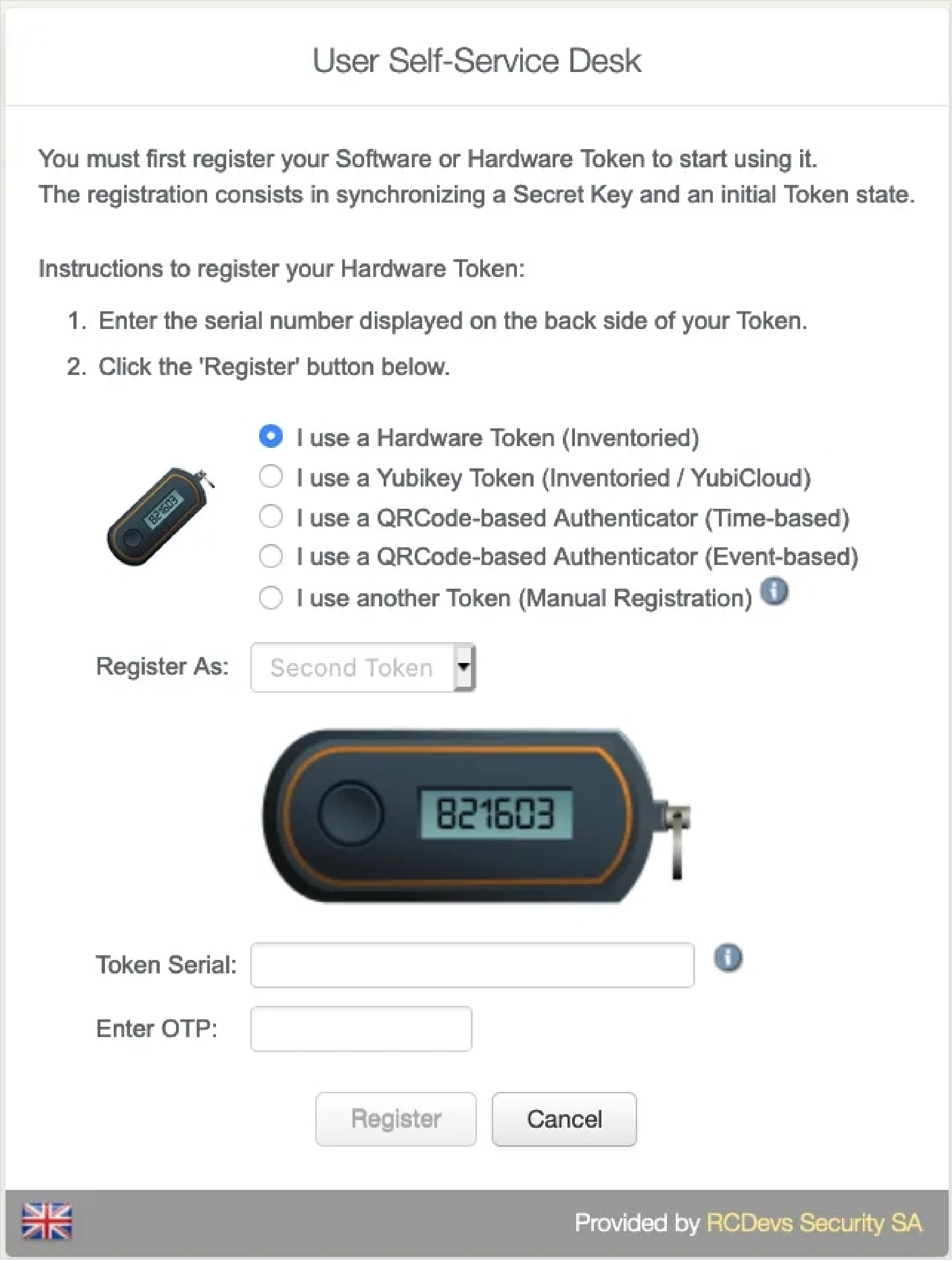
OTP Token Status:	**Not Registered**

User Statistics

Login Count:	**No success & No failure**
Last Login:	**Never**
Blocking Status:	**Account active** (0 login failed)

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.



User Self-Service Desk

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register your Hardware Token:

1. Enter the serial number displayed on the back side of your Token.
2. Click the 'Register' button below.

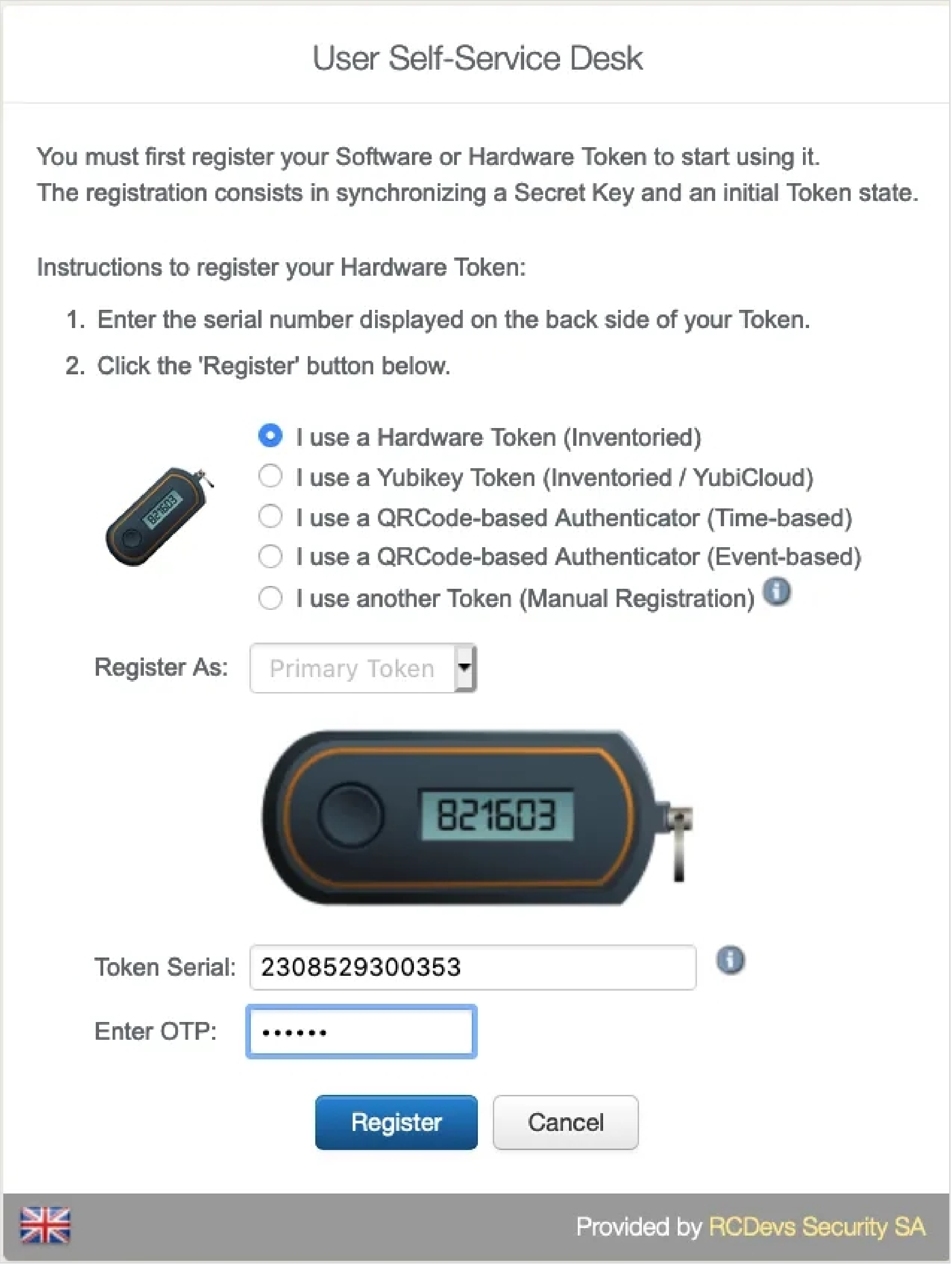
● I use a Hardware Token (Inventoried)
○ I use a Yubikey Token (Inventoried / YubiCloud)
○ I use a QRCode-based Authenticator (Time-based)
○ I use a QRCode-based Authenticator (Event-based)
○ I use another Token (Manual Registration)

Register As: Second Token

Token Serial:

Enter OTP:

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



User Self-Service Desk

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register your Hardware Token:

1. Enter the serial number displayed on the back side of your Token.
2. Click the 'Register' button below.

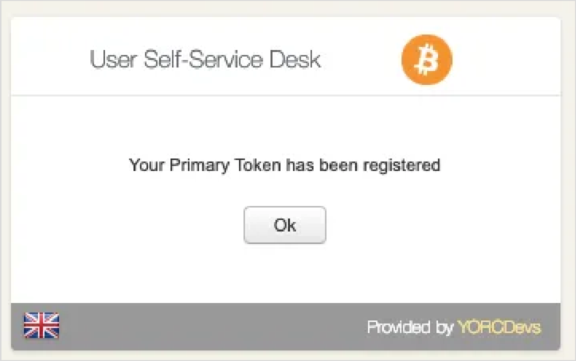
● I use a Hardware Token (Inventoried)
○ I use a Yubikey Token (Inventoried / YubiCloud)
○ I use a QRCode-based Authenticator (Time-based)
○ I use a QRCode-based Authenticator (Event-based)
○ I use another Token (Manual Registration)

Register As: Primary Token

Token Serial: 2308529300353

Enter OTP: ••••••

And click on `Register` button.



User Self-Service Desk

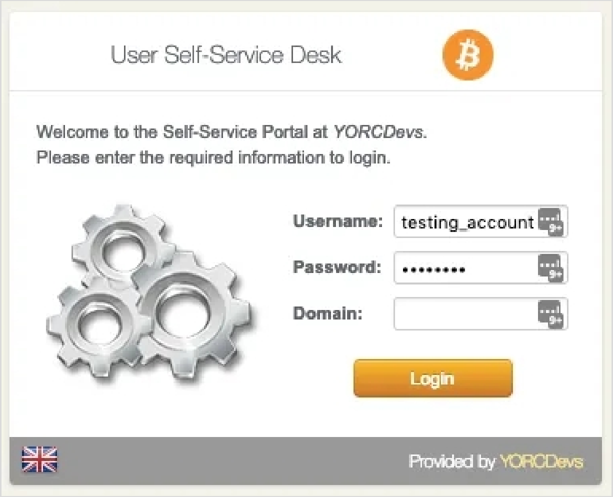
Your Primary Token has been registered

Your hardware token is now registered.

3.2.1.2 Software Token Registration

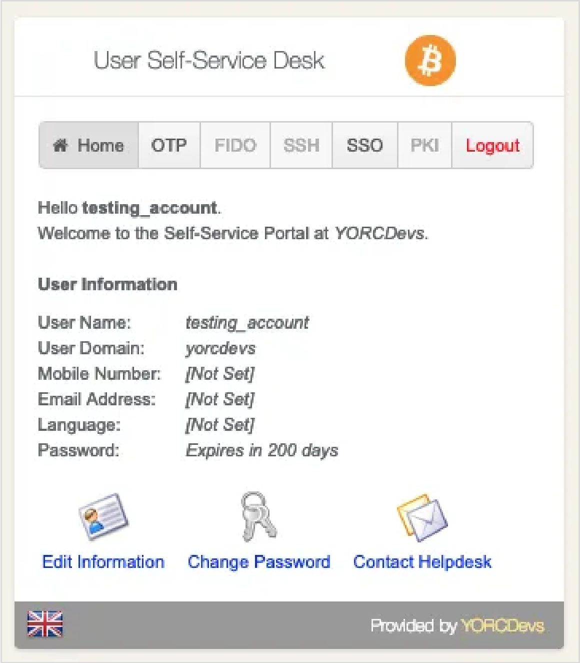
To allow the user to enroll a Software Token, you have to allow the OTP management under the Selfdesk configuration.

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



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

Username: testing_account
Password: ••••••••
Domain:

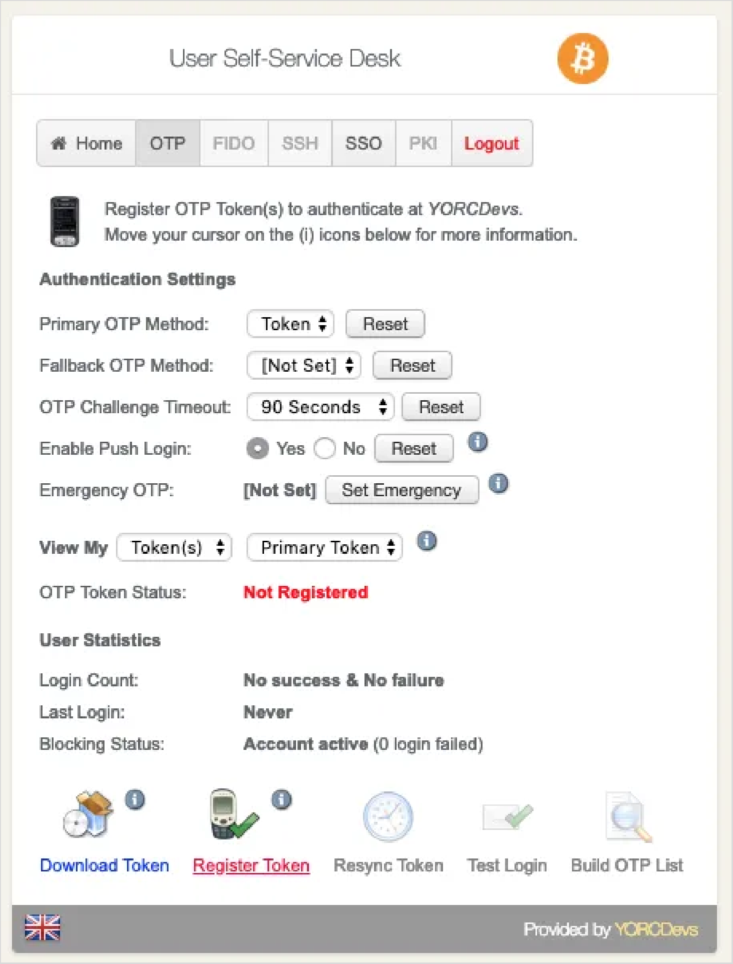


Hello **testing_account**.
Welcome to the Self-Service Portal at *YORCDevs*.

User Information

User Name:	*testing_account*
User Domain:	*yorcdevs*
Mobile Number:	*[Not Set]*
Email Address:	*[Not Set]*
Language:	*[Not Set]*
Password:	*Expires in 200 days*

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



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

Authentication Settings

Primary OTP Method:	Token
Fallback OTP Method:	[Not Set]
OTP Challenge Timeout:	90 Seconds
Enable Push Login:	● Yes ○ No
Emergency OTP:	**[Not Set]**

View My Token(s) Primary Token

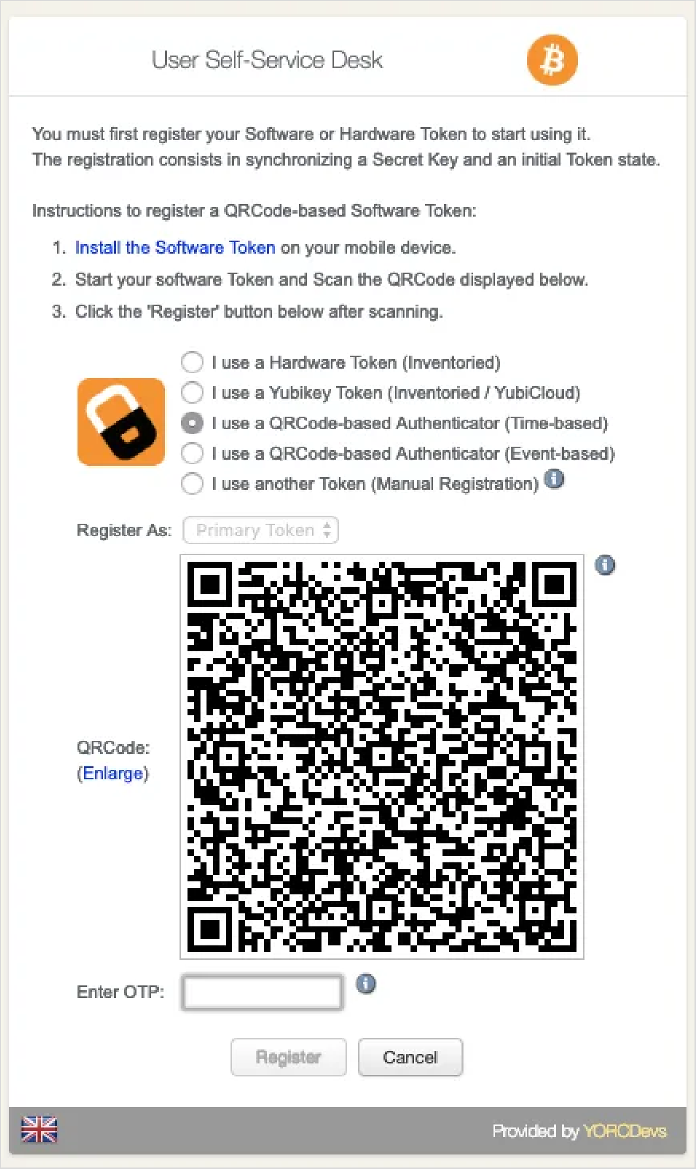
OTP Token Status: **Not Registered**

User Statistics

Login Count:	**No success & No failure**
Last Login:	**Never**
Blocking Status:	**Account active** (0 login failed)

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.



User Self-Service Desk

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register a QRCode-based Software Token:

1. Install the Software Token on your mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. Click the 'Register' button below after scanning.

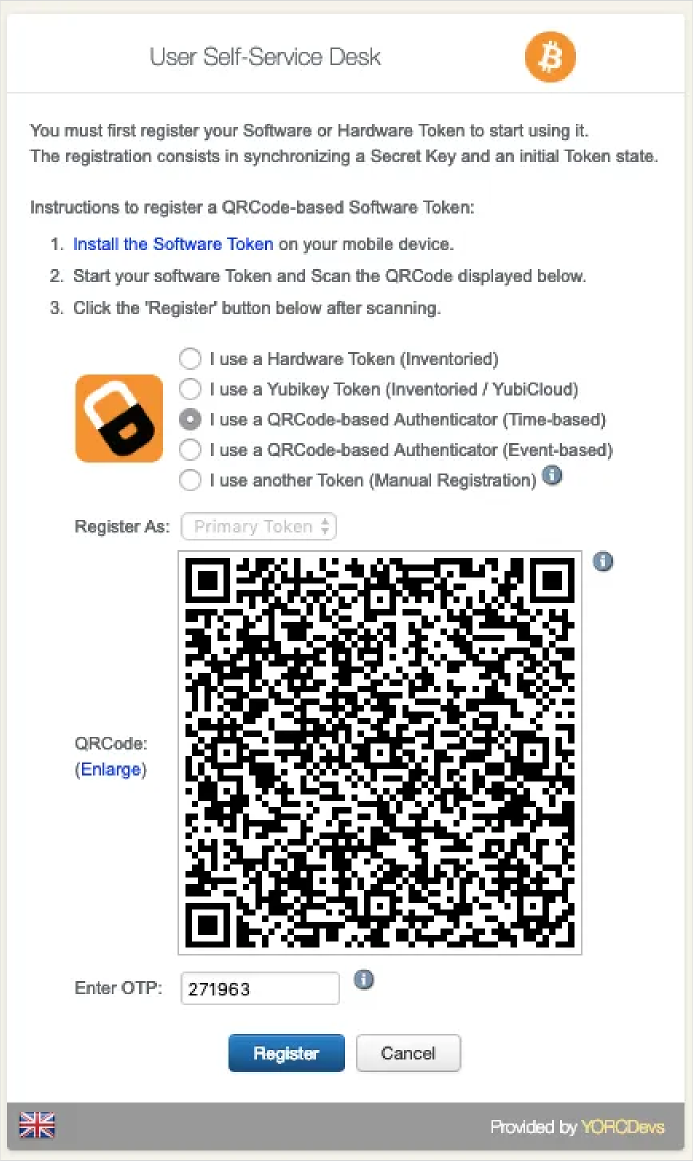
○ I use a Hardware Token (Inventoried)
○ I use a Yubikey Token (Inventoried / YubiCloud)
● I use a QRCode-based Authenticator (Time-based)
○ I use a QRCode-based Authenticator (Event-based)
○ I use another Token (Manual Registration)

Register As: Primary Token

QRCode:
(Enlarge)

Enter OTP:

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



User Self-Service Desk

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register a QRCode-based Software Token:

1. Install the Software Token on your mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. Click the 'Register' button below after scanning.

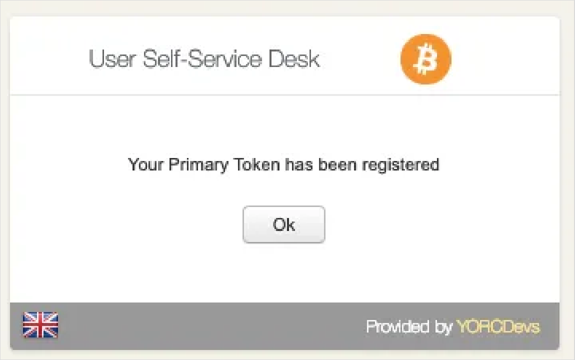
- ○ I use a Hardware Token (Inventoried)
- ○ I use a Yubikey Token (Inventoried / YubiCloud)
- ● I use a QRCode-based Authenticator (Time-based)
- ○ I use a QRCode-based Authenticator (Event-based)
- ○ I use another Token (Manual Registration)

Register As: Primary Token

QRCode: (Enlarge)

Enter OTP: 271963

And click on `Register` button.



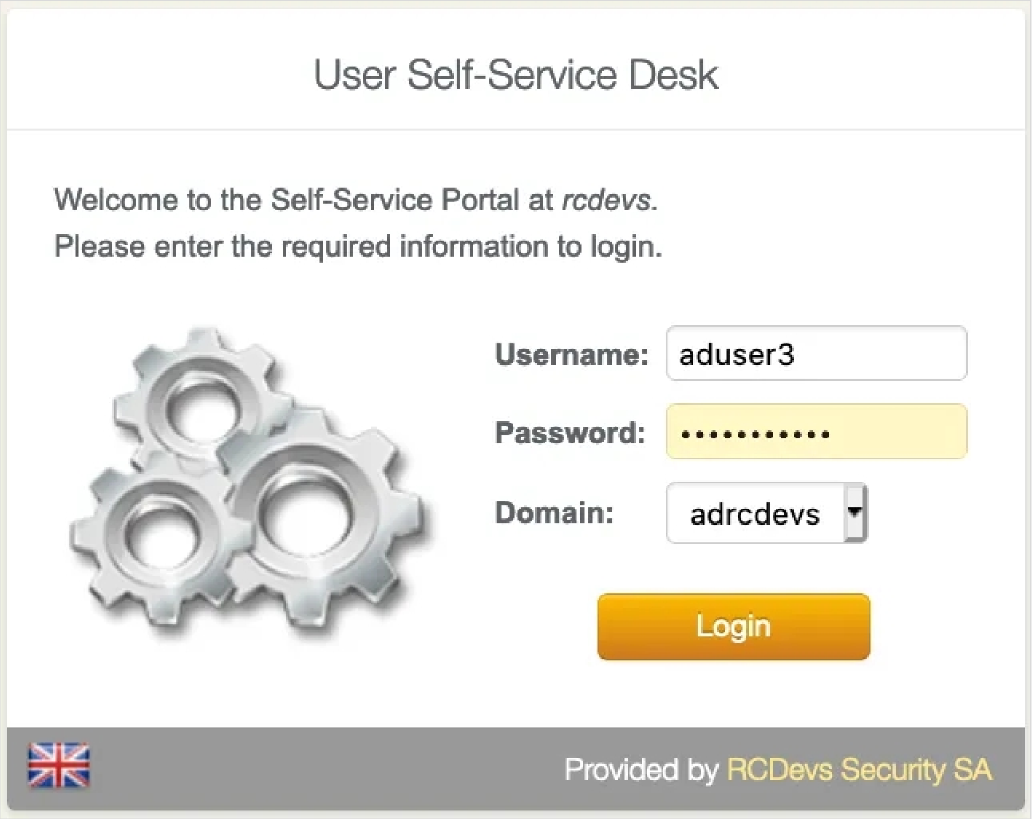
User Self-Service Desk

Your Primary Token has been registered

Your software token is now registered.

3.2.3 SelfDesk Voice Registration

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



User Self-Service Desk

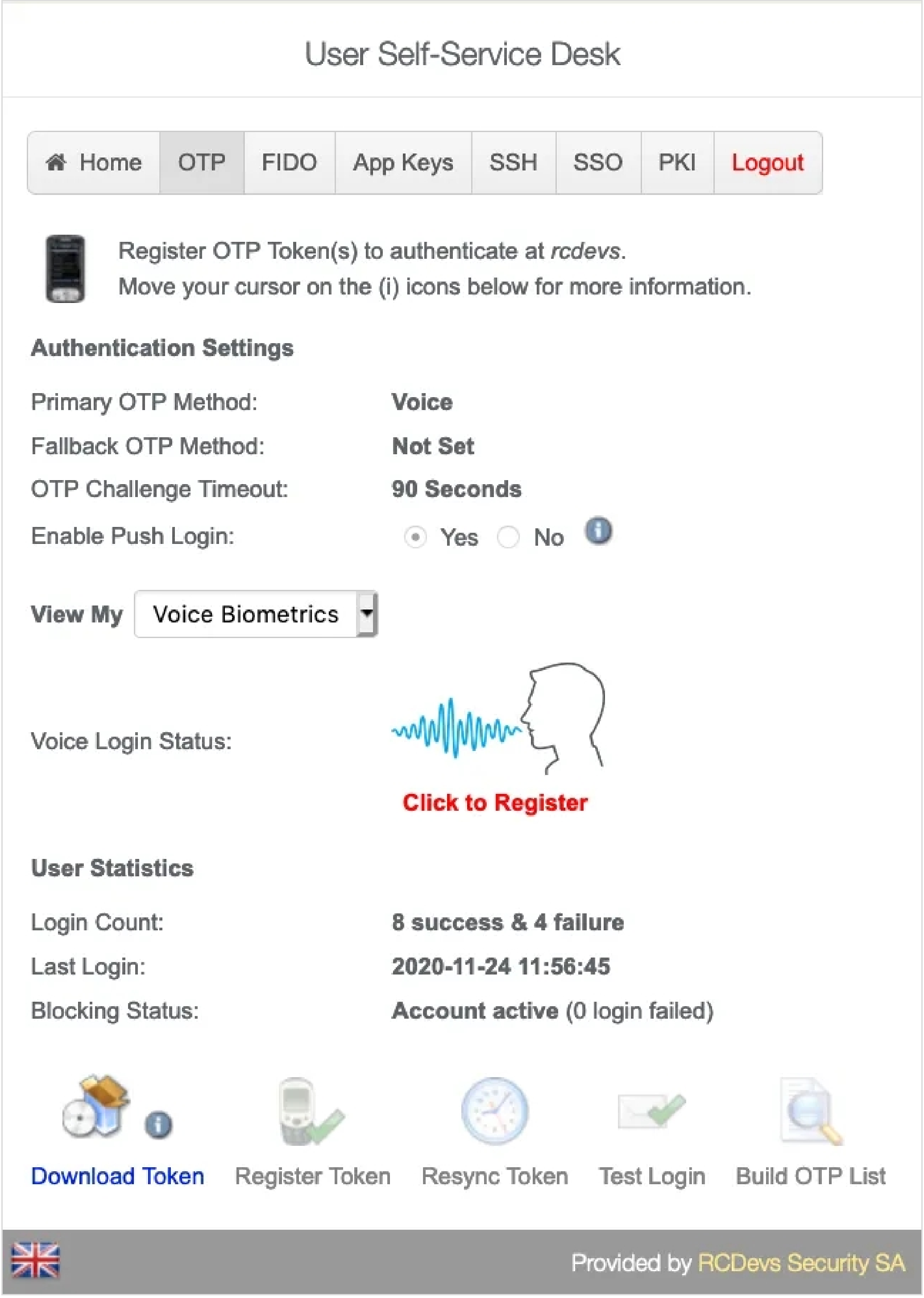
Welcome to the Self-Service Portal at *rcdevs*.
Please enter the required information to login.

Username: aduser3

Password: ••••••••••••

Domain: adrcdevs

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



User Self-Service Desk

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

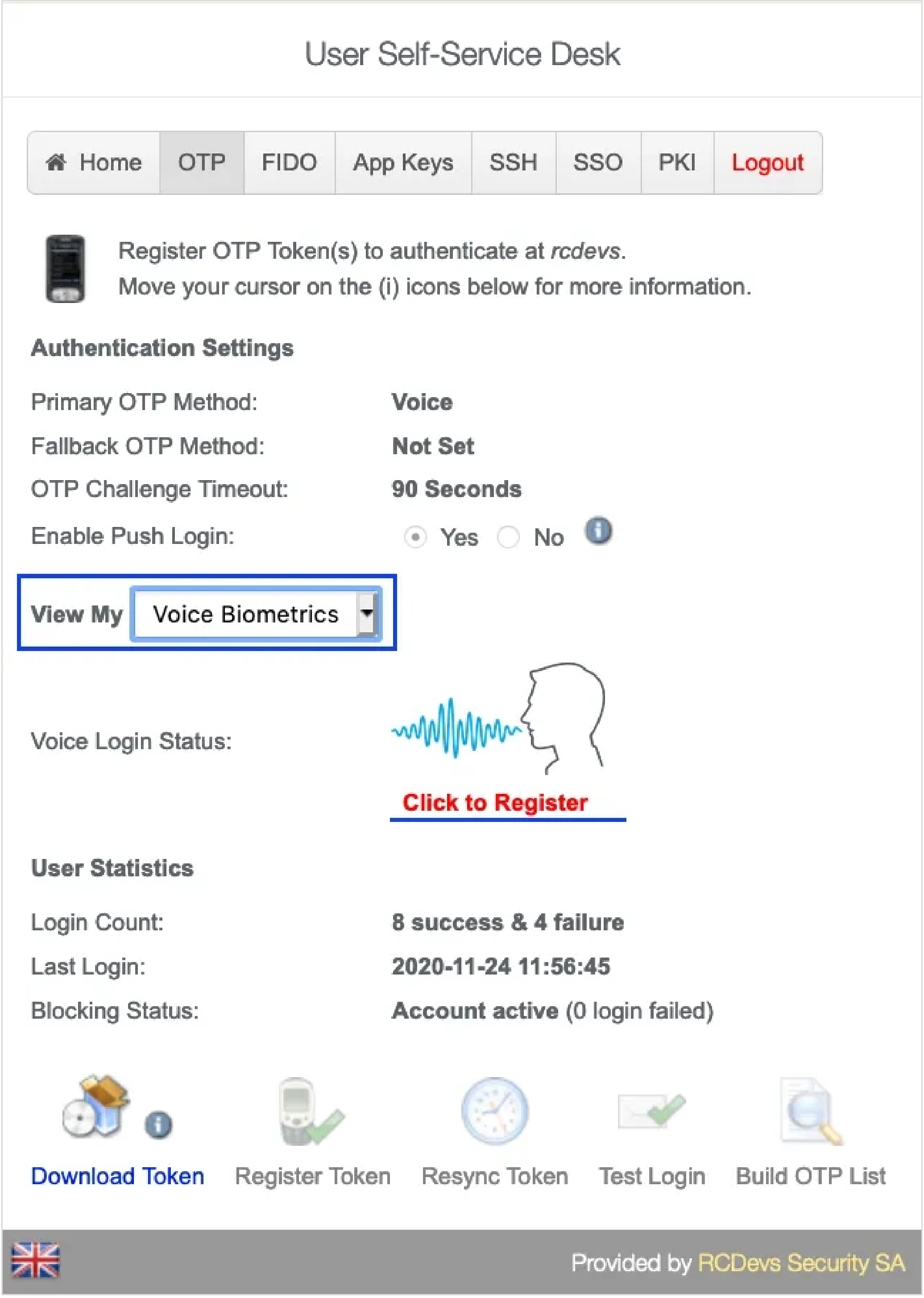
View My Voice Biometrics

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)

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



User Self-Service Desk

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

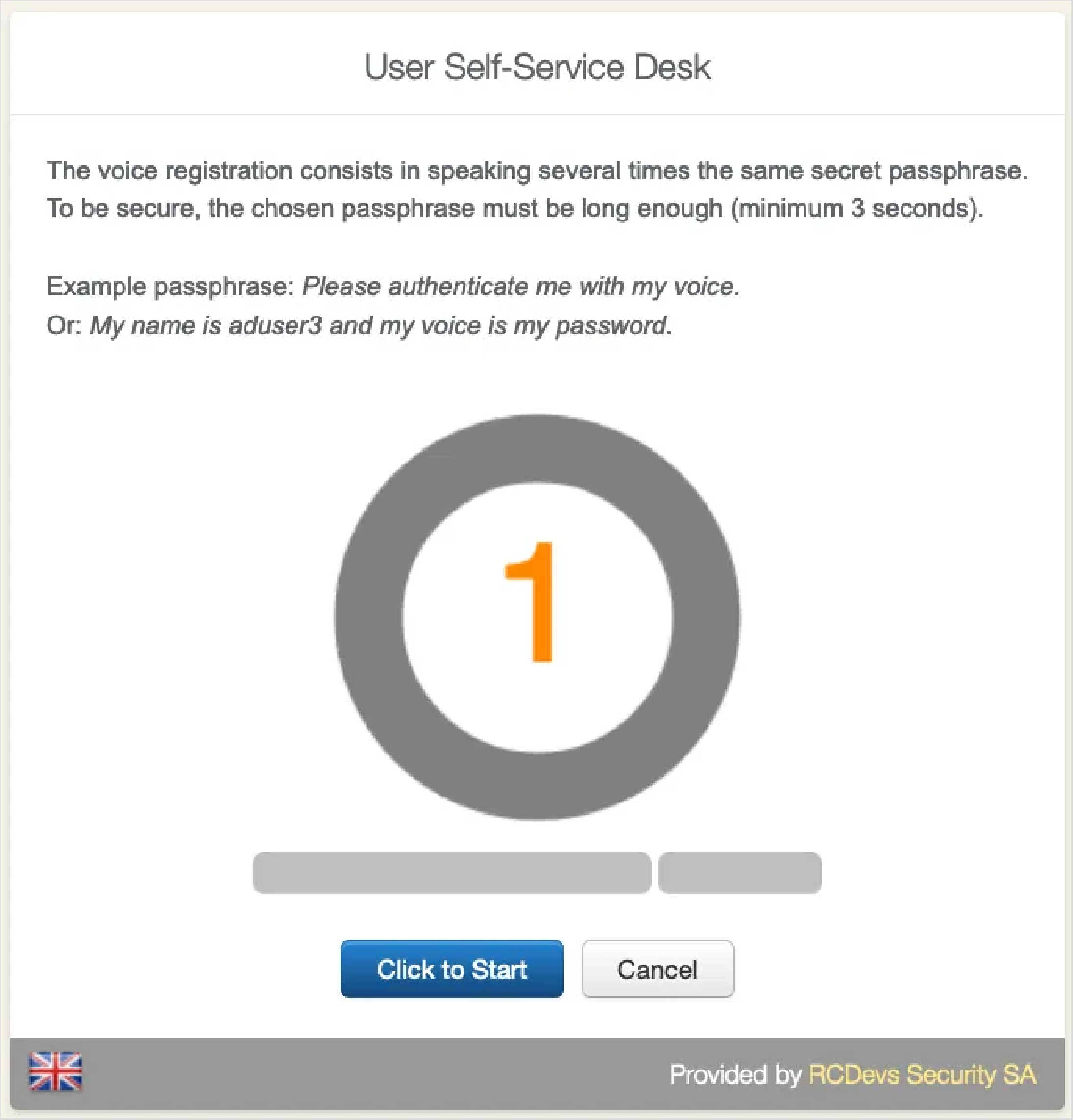
View My Voice Biometrics

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)

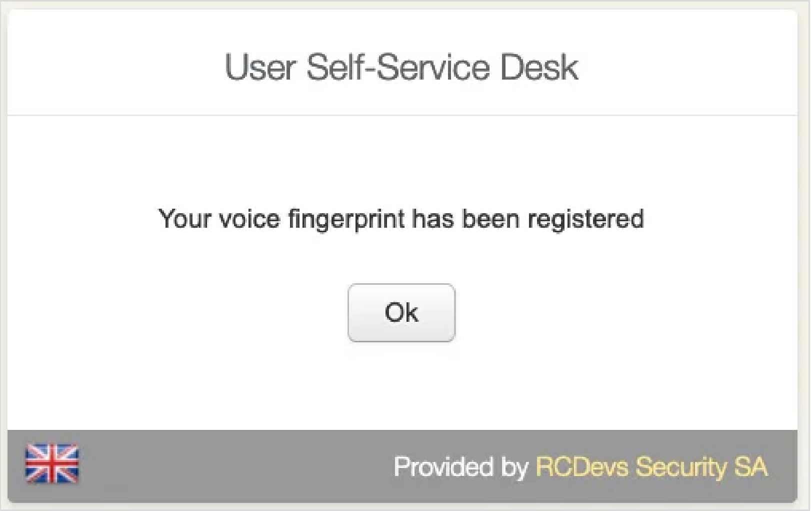
Provided by RCDevs Security SA



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.*

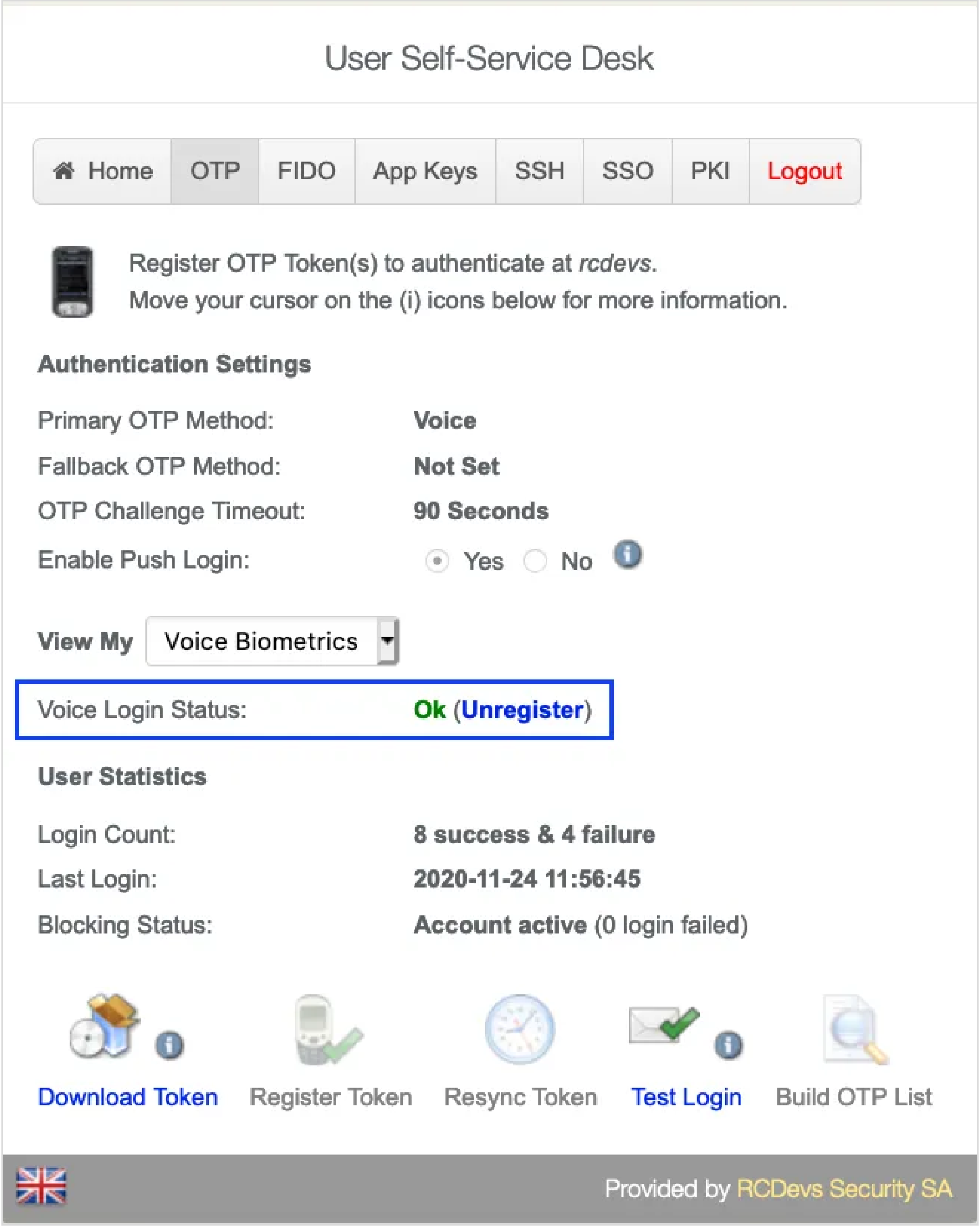


User Self-Service Desk

Your voice fingerprint has been registered

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

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:	**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)

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`

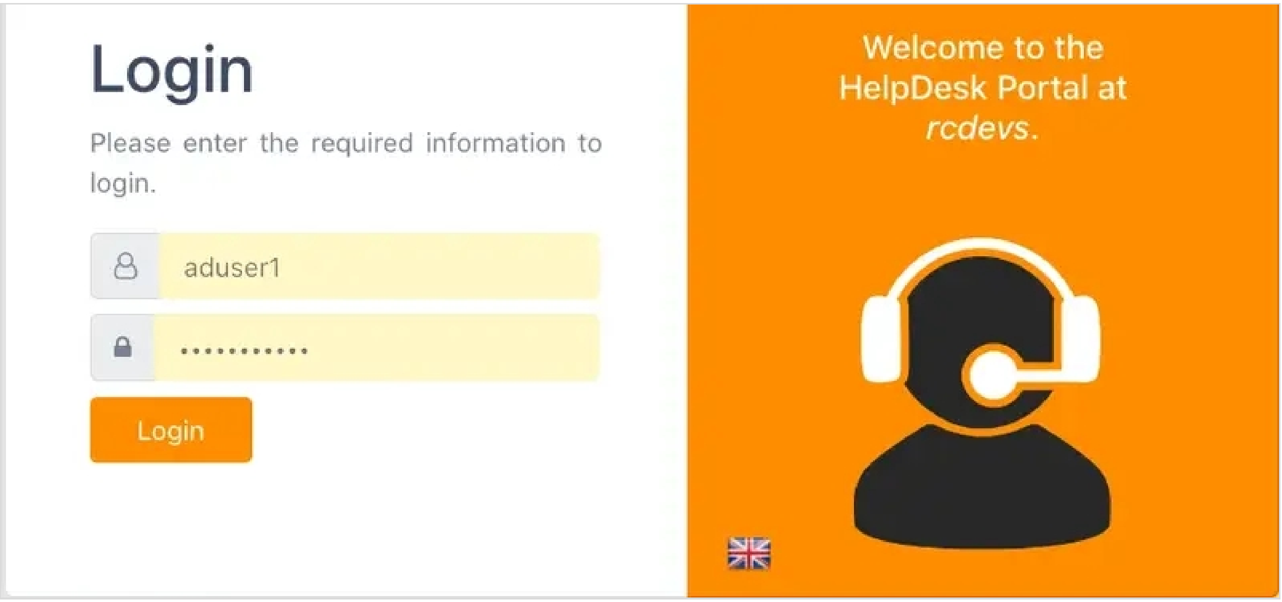
through the WAPRoxy the address is:

`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.



Login

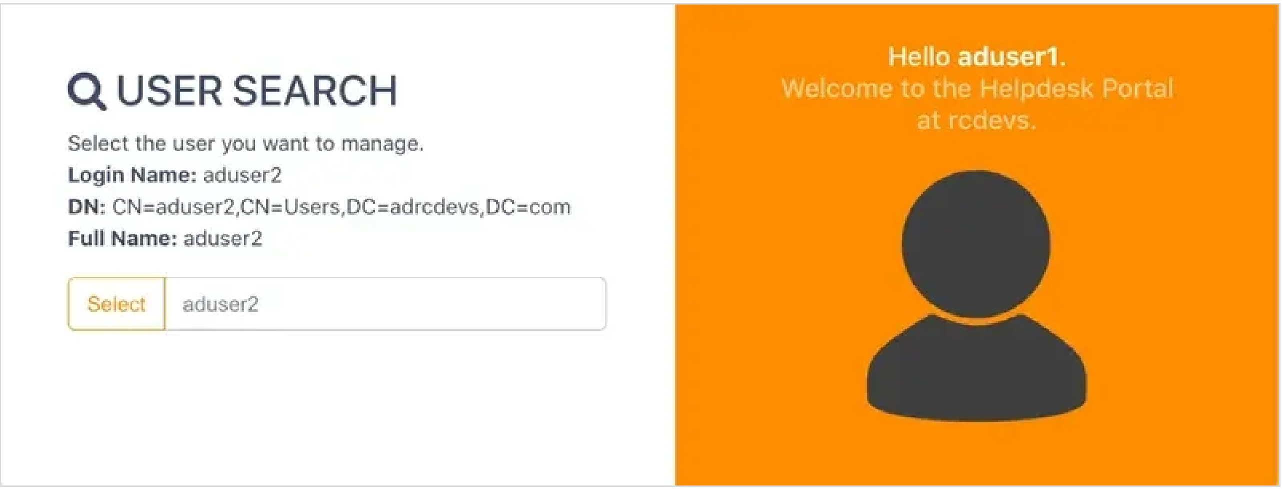
Please enter the required information to login.

aduser1

•••••••••••

Welcome to the HelpDesk Portal at *rcdevs*.

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



USER SEARCH

Select the user you want to manage.

Login Name: aduser2

DN: CN=aduser2,CN=Users,DC=adrcdevs,DC=com

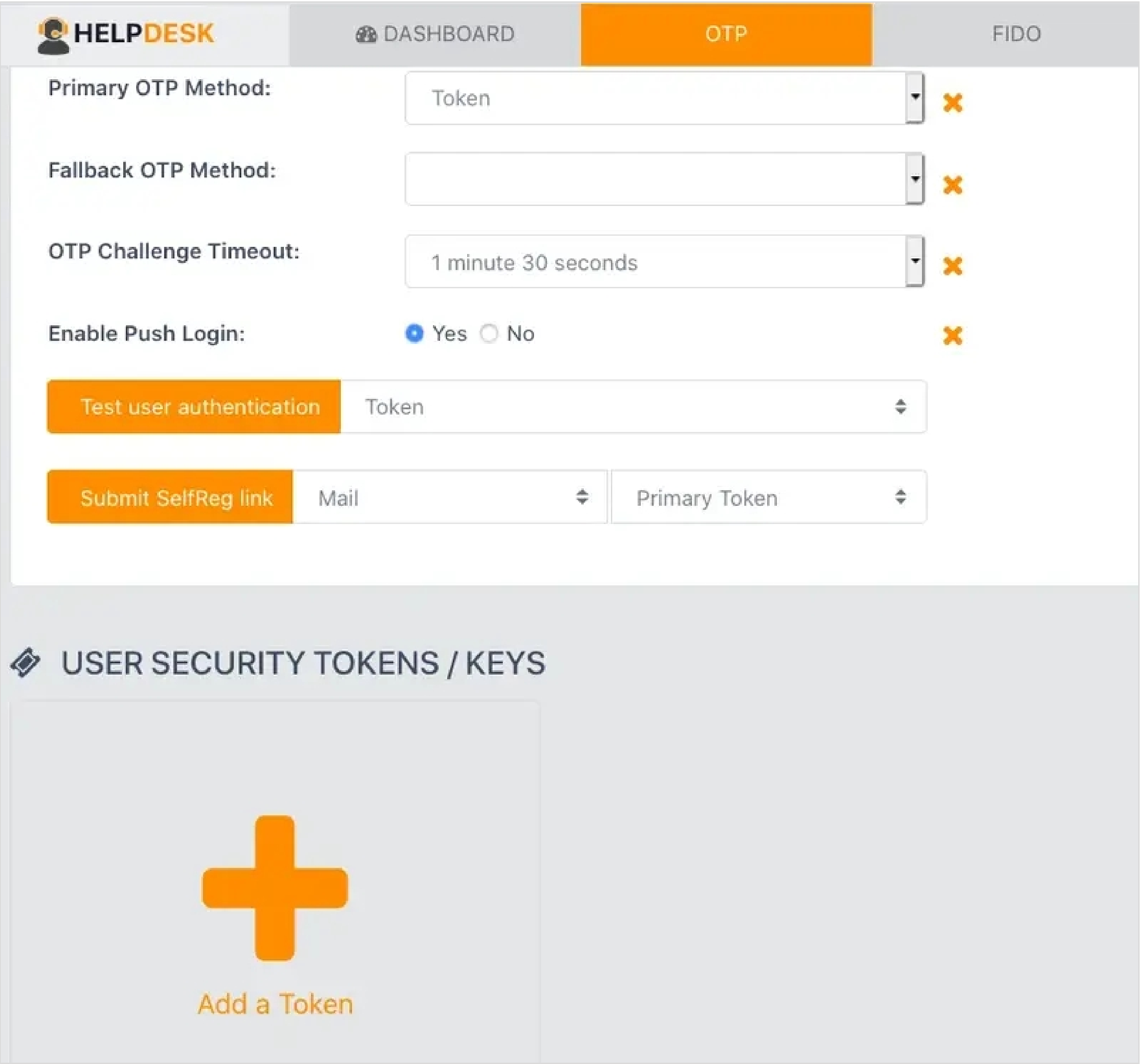
Full Name: aduser2

aduser2

Hello aduser1.

Welcome to the Helpdesk Portal at rcdevs.

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



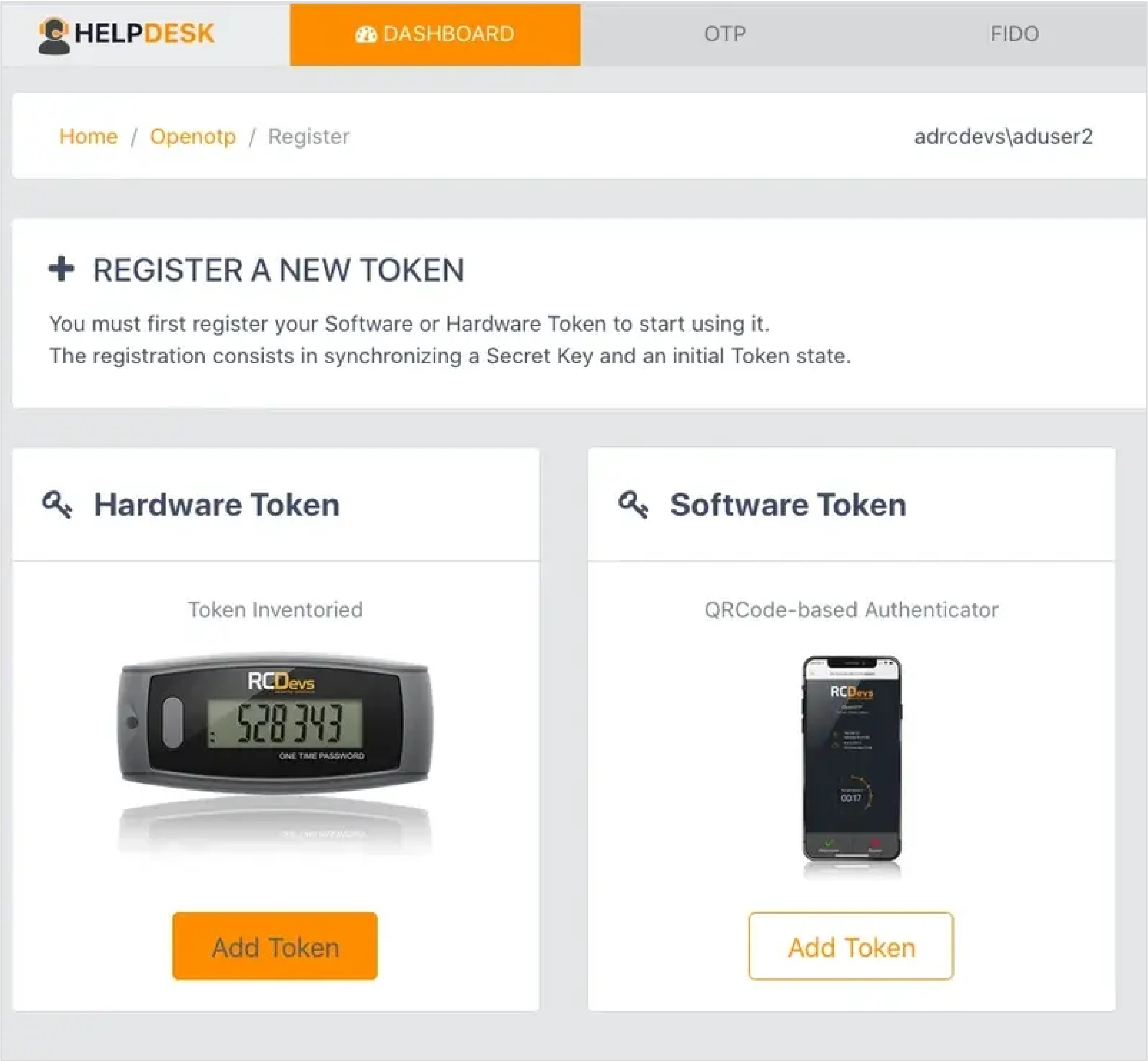
Primary OTP Method: Token

Fallback OTP Method:

OTP Challenge Timeout: 1 minute 30 seconds

Enable Push Login: ● Yes ○ No

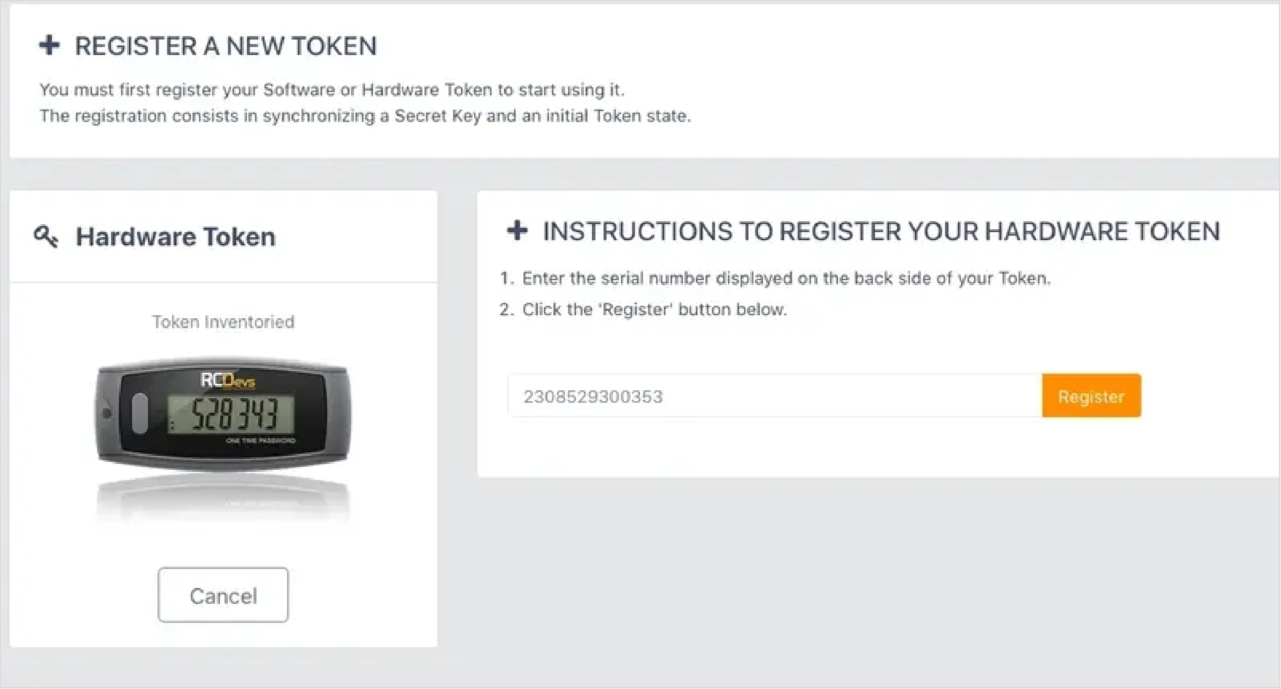
In the next page, please, click in `Hardware Token`.



REGISTER A NEW TOKEN

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

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



REGISTER A NEW TOKEN

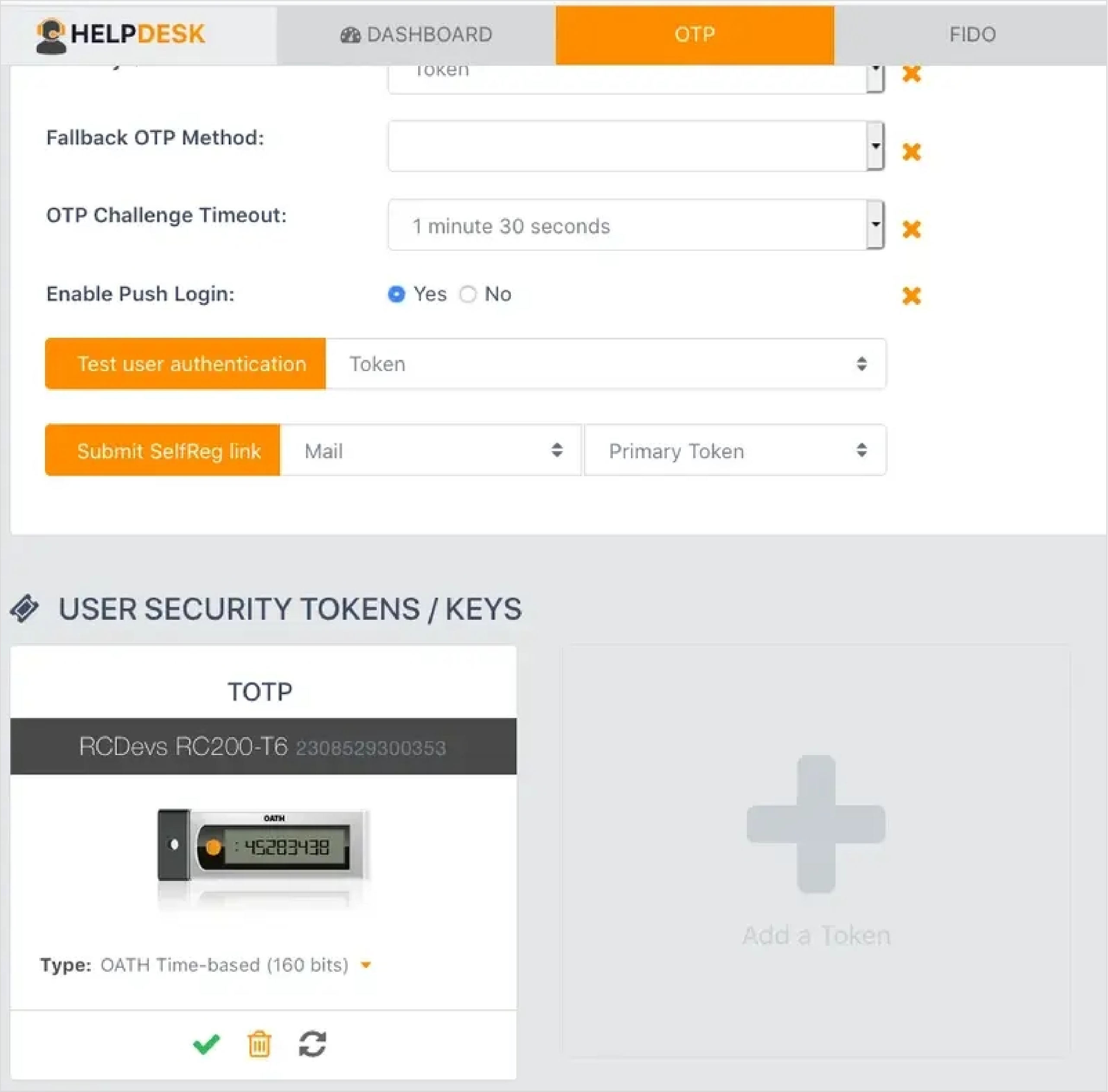
You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

INSTRUCTIONS TO REGISTER YOUR HARDWARE TOKEN

1. Enter the serial number displayed on the back side of your Token.
2. Click the 'Register' button below.

2308529300353

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



Token

Fallback OTP Method:

OTP Challenge Timeout: 1 minute 30 seconds

Enable Push Login: ● Yes ○ No

TOTP

RCDevs RC200-T6 2308529300353

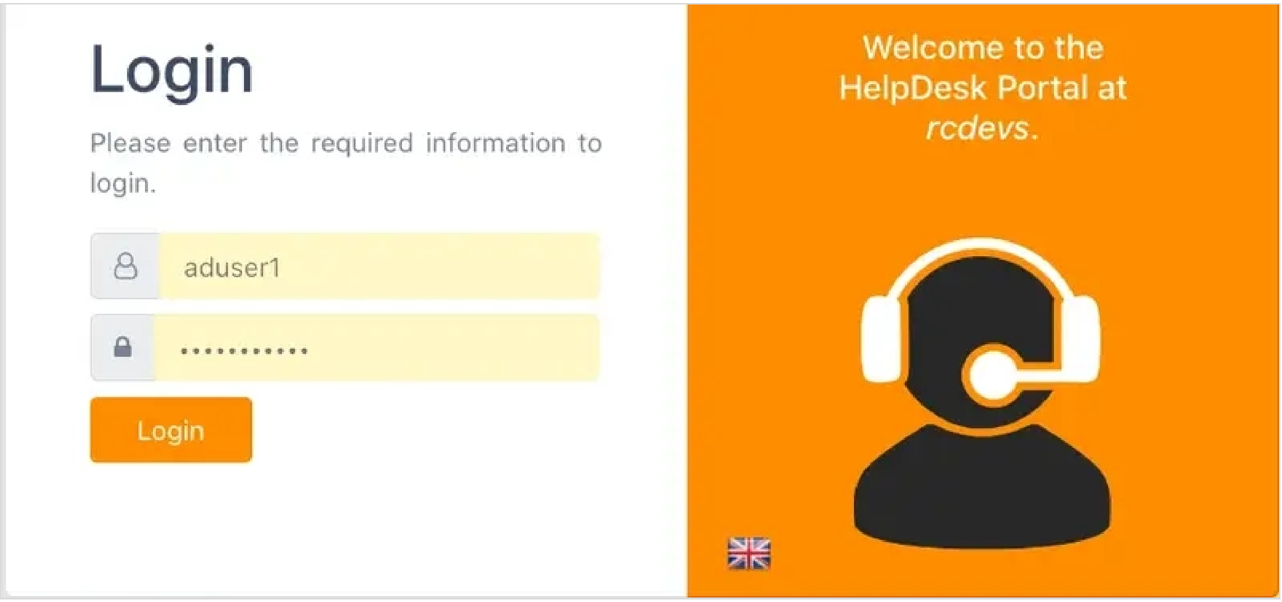
Type: OATH Time-based (160 bits)

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.



Login

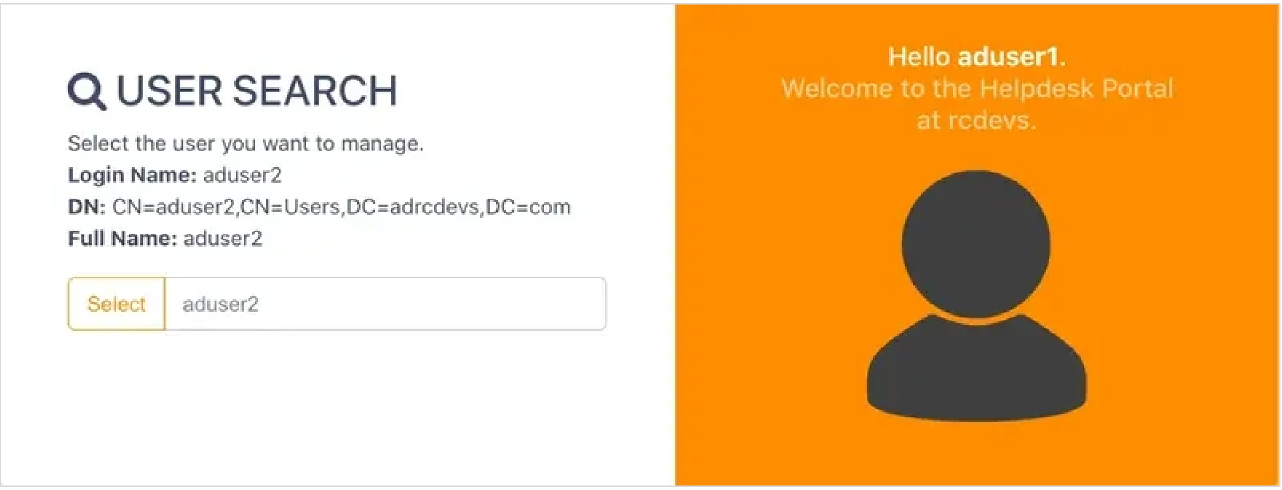
Please enter the required information to login.

aduser1

•••••••••••

Welcome to the HelpDesk Portal at *rcdevs*.

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



USER SEARCH

Select the user you want to manage.

Login Name: aduser2

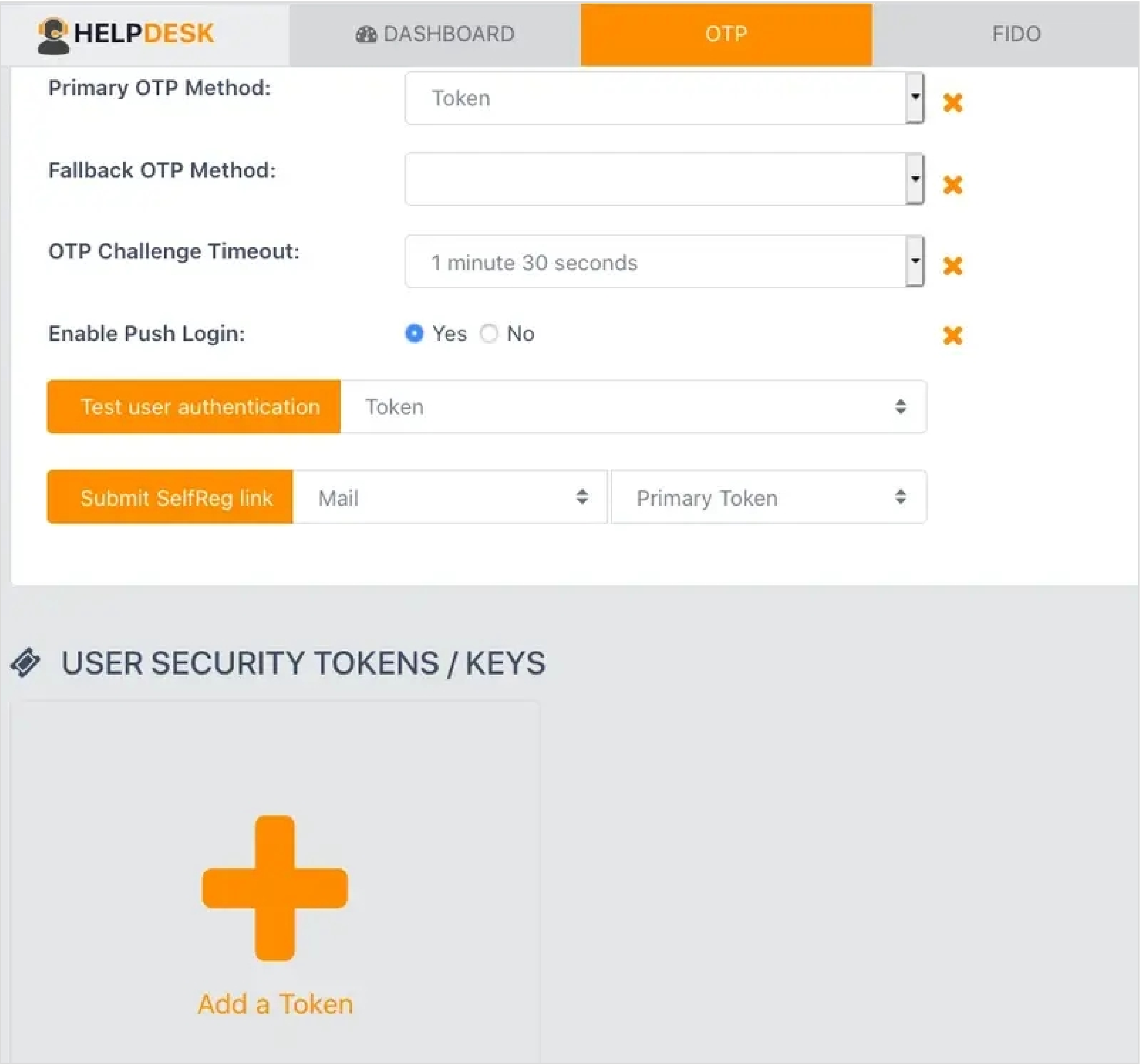
DN: CN=aduser2,CN=Users,DC=adrcdevs,DC=com

Full Name: aduser2

aduser2

Hello **aduser1**.
Welcome to the Helpdesk Portal at rcdevs.

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



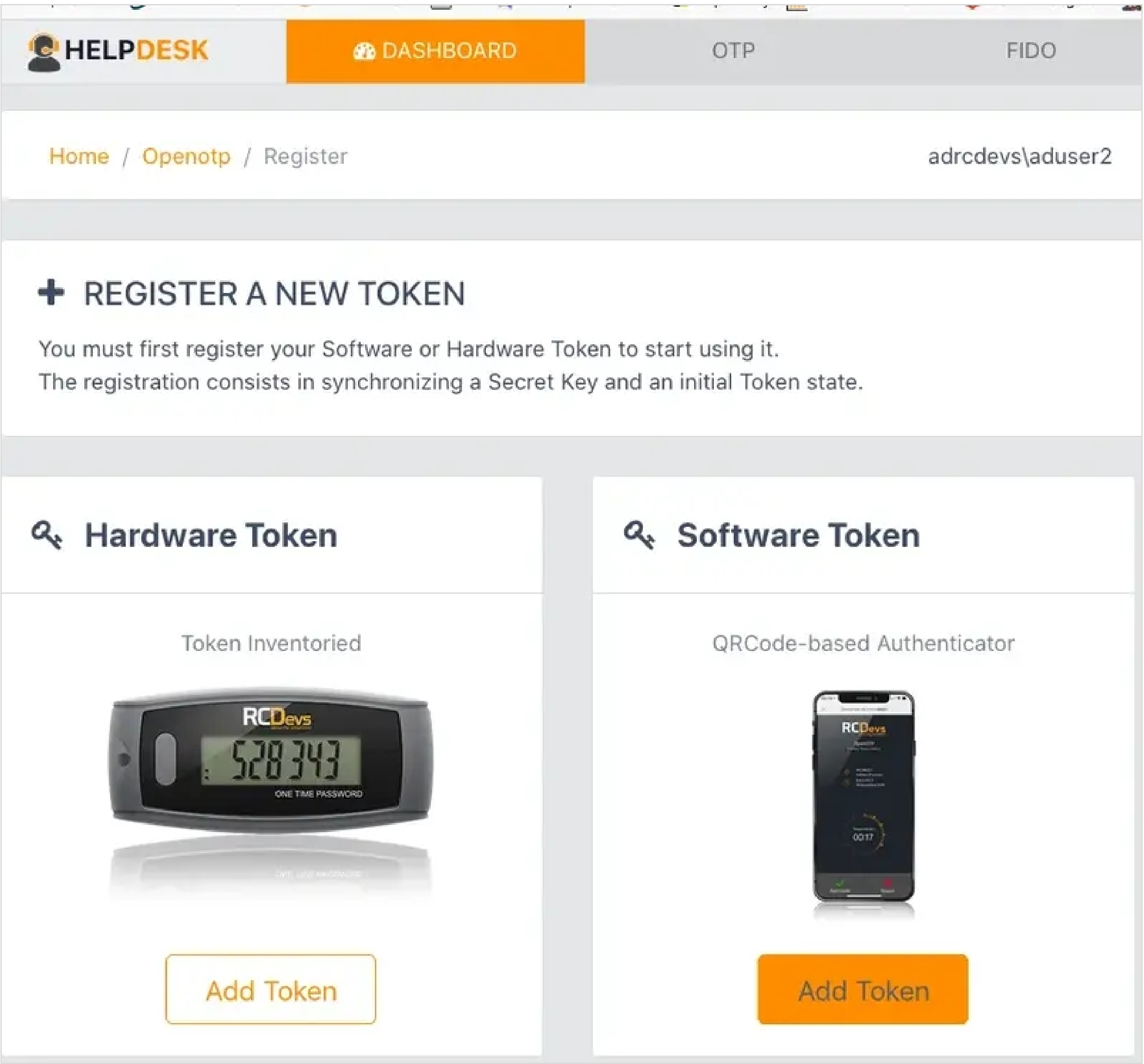
Primary OTP Method: Token

Fallback OTP Method:

OTP Challenge Timeout: 1 minute 30 seconds

Enable Push Login: ● Yes ○ No

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



Home / Openotp / Register

adrcdevs\aduser2

✚ REGISTER A NEW TOKEN

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Hardware Token

Token Inventoried

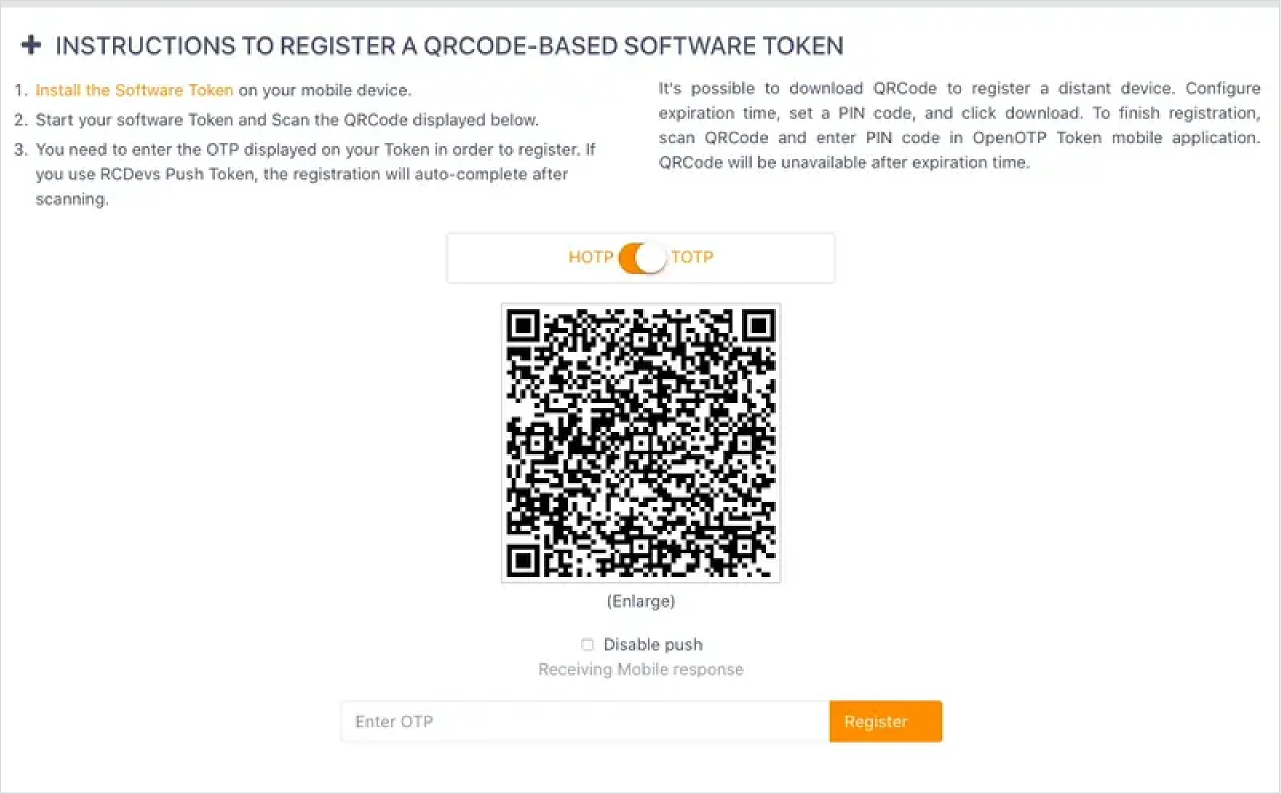
Add Token

Software Token

QRCode-based Authenticator

Add Token

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

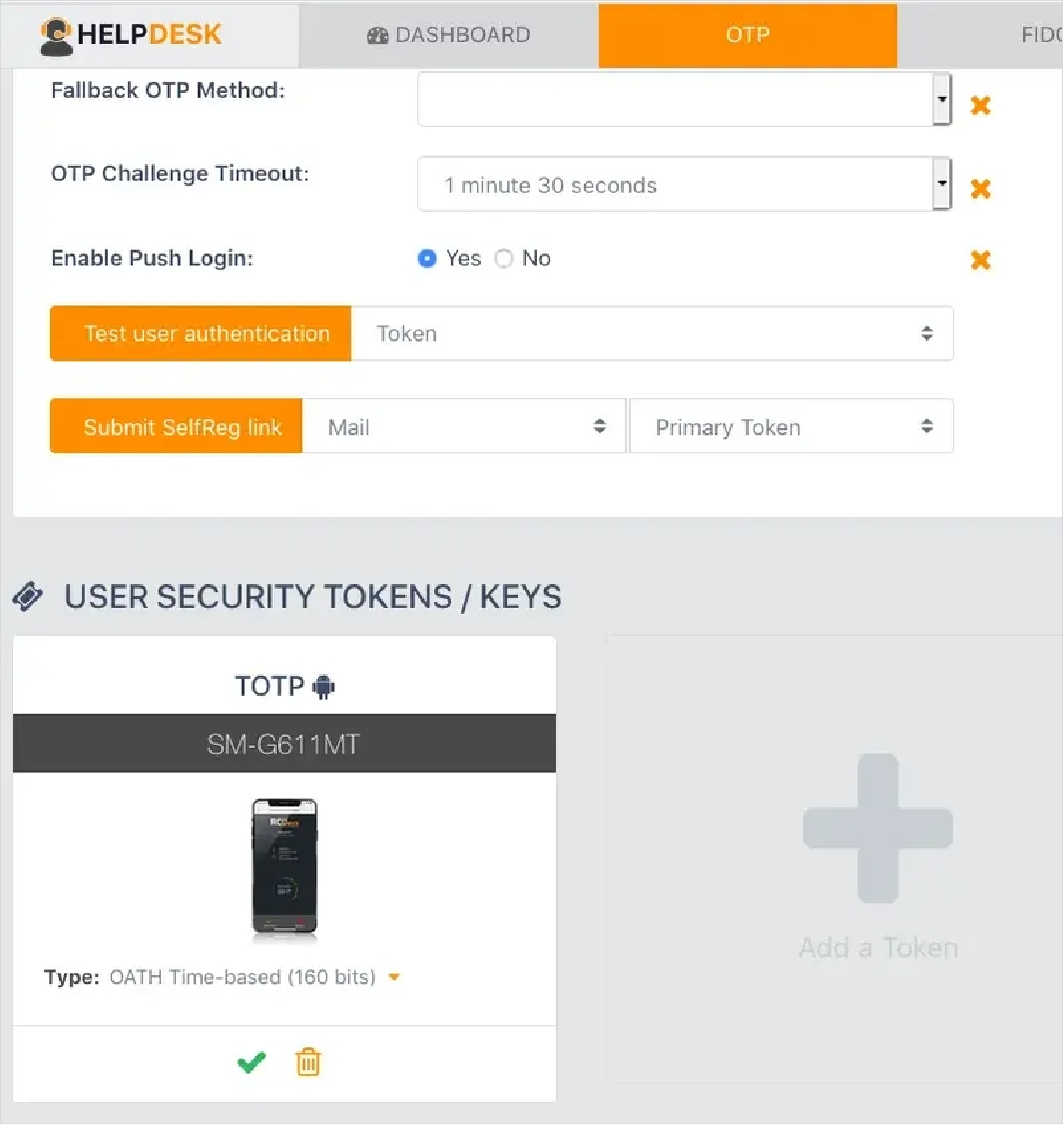


✚ INSTRUCTIONS TO REGISTER A QRCODE-BASED SOFTWARE TOKEN

1. Install the Software Token on your mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. You need to enter the OTP displayed on your Token in order to register. If you use RCDevs Push Token, the registration will auto-complete after scanning.

It's possible to download QRCode to register a distant device. Configure expiration time, set a PIN code, and click download. To finish registration, scan QRCode and enter PIN code in OpenOTP Token mobile application. QRCode will be unavailable after expiration time.

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



HELPDESK | DASHBOARD | OTP | FIDO

Fallback OTP Method:

OTP Challenge Timeout: 1 minute 30 seconds

Enable Push Login: ● Yes ○ No

Test user authentication — Token

Submit SelfReg link — Mail — Primary Token

USER SECURITY TOKENS / KEYS

TOTP

SM-G611MT

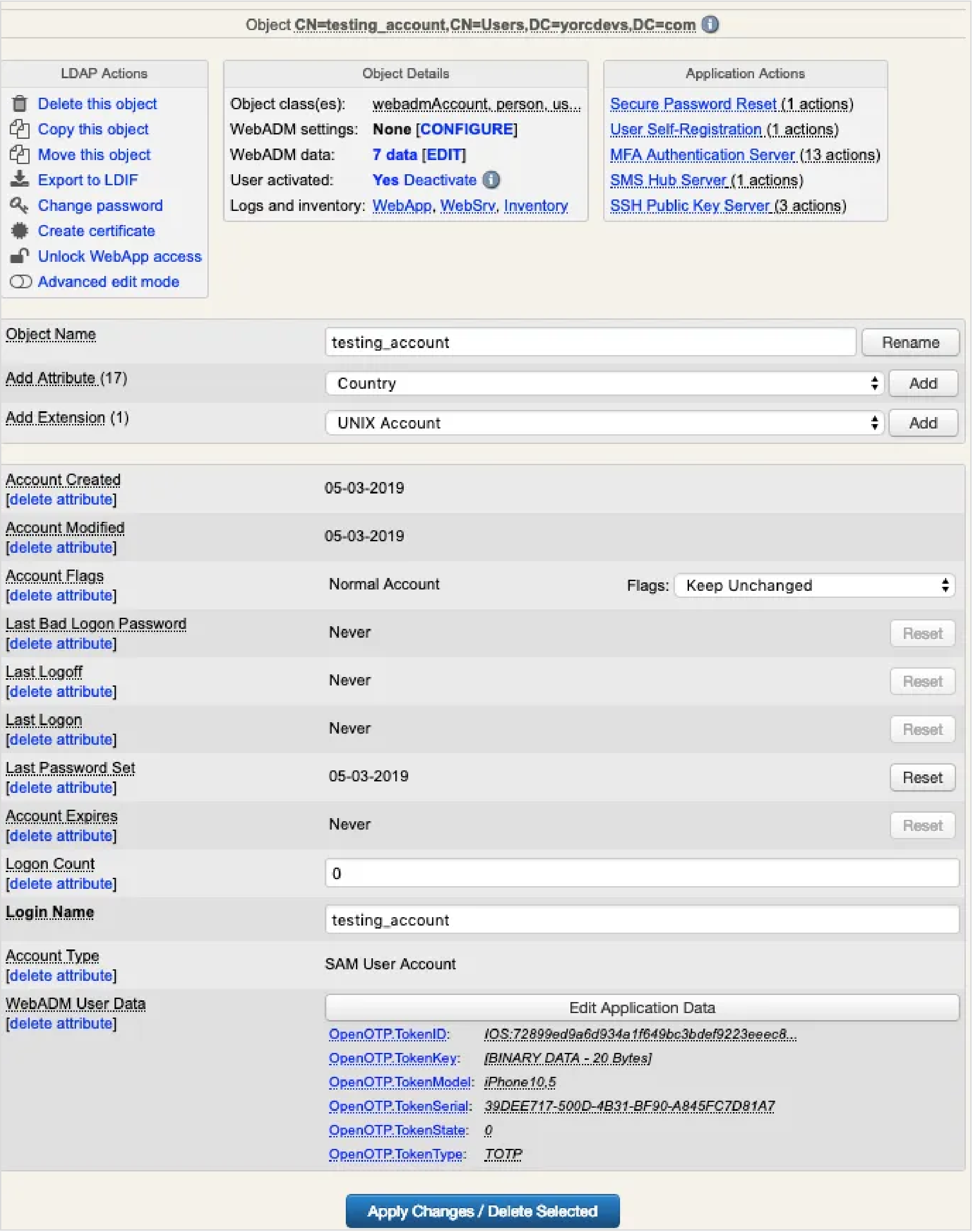
Type: OATH Time-based (160 bits)

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`



Object CN=testing_account,CN=Users,DC=yorcdevs,DC=com

Object Details

Object class(es):	webadmAccount, person, us...
WebADM settings:	None [CONFIGURE]
WebADM data:	7 data [EDIT]
User activated:	Yes Deactivate
Logs and inventory:	WebApp, WebSrv, Inventory

Application Actions

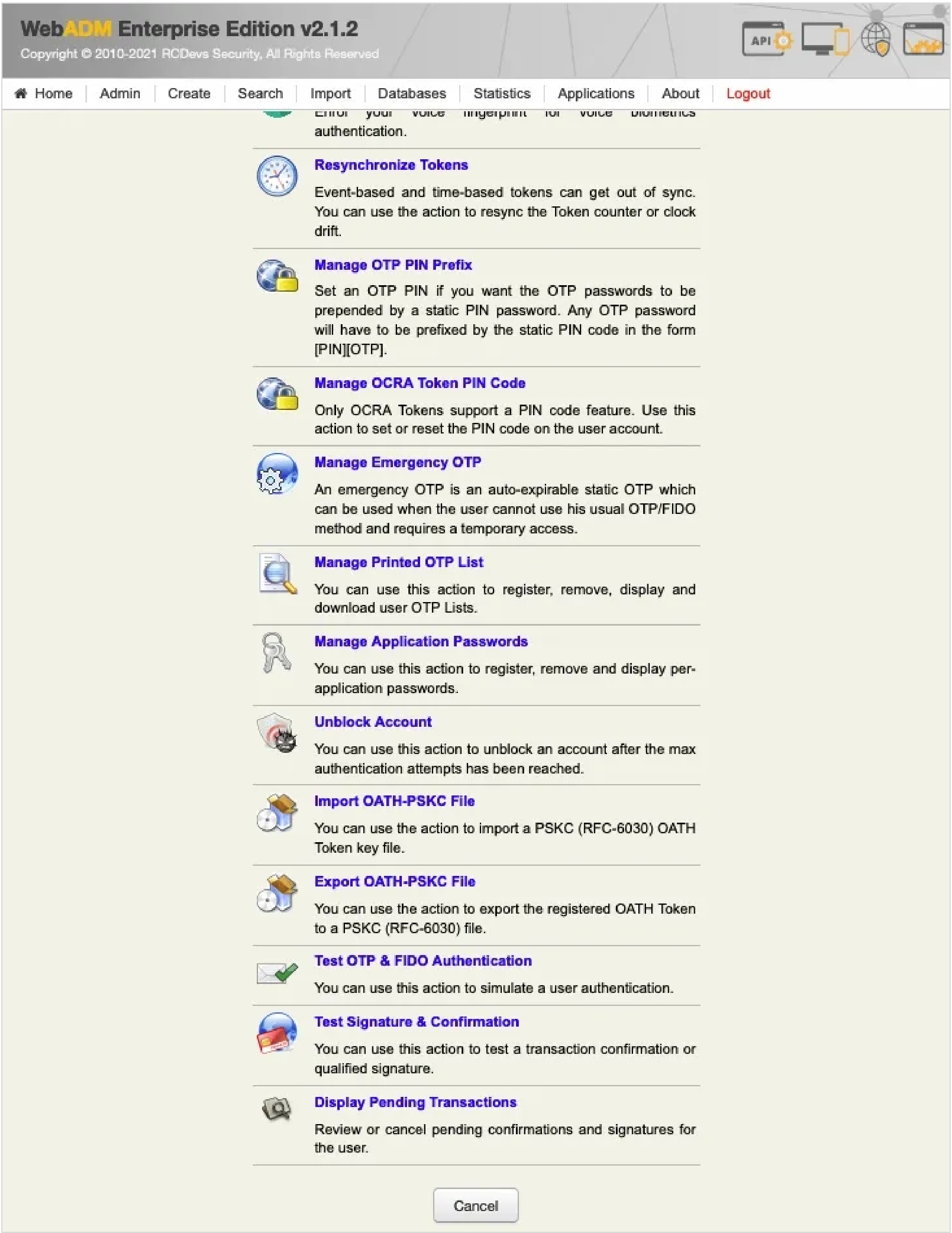
- Secure Password Reset (1 actions)
- User Self-Registration (1 actions)
- MFA Authentication Server (13 actions)
- SMS Hub Server (1 actions)
- SSH Public Key Server (3 actions)

Object Name	testing_account	Rename
Add Attribute (17)	Country	Add
Add Extension (1)	UNIX Account	Add

Account Created [delete attribute]	05-03-2019	
Account Modified [delete attribute]	05-03-2019	
Account Flags [delete attribute]	Normal Account	Flags: Keep Unchanged
Last Bad Logon Password [delete attribute]	Never	Reset
Last Logoff [delete attribute]	Never	Reset
Last Logon [delete attribute]	Never	Reset
Last Password Set [delete attribute]	05-03-2019	Reset
Account Expires [delete attribute]	Never	Reset
Logon Count [delete attribute]	0	
Login Name	testing_account	
Account Type [delete attribute]	SAM User Account	
WebADM User Data [delete attribute]	Edit Application Data	

OpenOTP.TokenID:	*IOS:72899ed9a6d934a1f649bc3bdef9223eeec8...*
OpenOTP.TokenKey:	*[BINARY DATA - 20 Bytes]*
OpenOTP.TokenModel:	*iPhone10,5*
OpenOTP.TokenSerial:	*39DEE717-500D-4B31-BF90-A845FC7D81A7*
OpenOTP.TokenState:	*0*
OpenOTP.TokenType:	*TOTP*

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



WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
API
Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

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].

Manage OCRA Token PIN Code

Only OCRA Tokens support a PIN code feature. Use this 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 OTP & FIDO Authentication

You can use this action to simulate a user authentication.

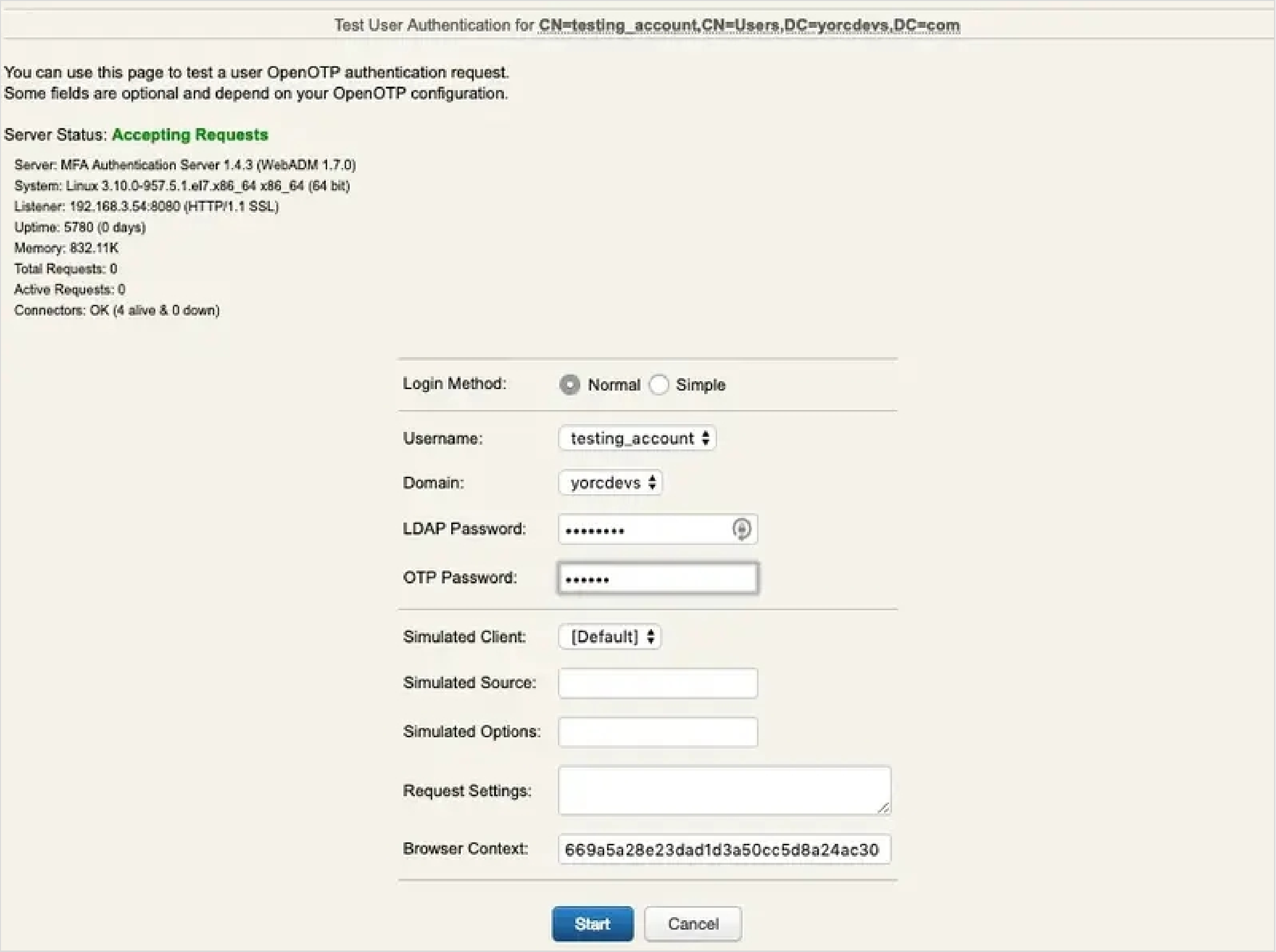
Test Signature & Confirmation

You can use this action to test a transaction confirmation or qualified signature.

Display Pending Transactions

Review or cancel pending confirmations and signatures for the user.

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



Test User Authentication for CN=testing_account,CN=Users,DC=yorcdevs,DC=com

You can use this page to test a user OpenOTP authentication request.
Some fields are optional and depend on your OpenOTP configuration.

Server Status: Accepting Requests

```
Server: MFA Authentication Server 1.4.3 (WebADM 1.7.0)
System: Linux 3.10.0-957.5.1.el7.x86_64 x86_64 (64 bit)
Listener: 192.168.3.54:8080 (HTTP/1.1 SSL)
Uptime: 5780 (0 days)
Memory: 832.11K
Total Requests: 0
Active Requests: 0
Connectors: OK (4 alive & 0 down)
```

Login Method: ● Normal ○ Simple

Username: testing_account

Domain: yorcdevs

LDAP Password: ••••••••

OTP Password: ••••••

Simulated Client: [Default]

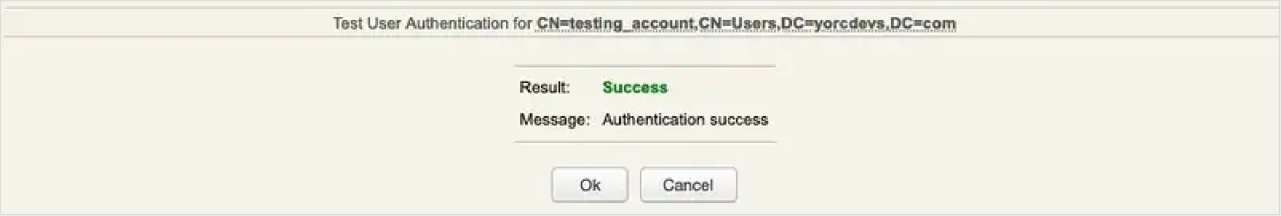
Simulated Source:

Simulated Options:

Request Settings:

Browser Context: 669a5a28e23dad1d3a50cc5d8a24ac30

We are authenticated!



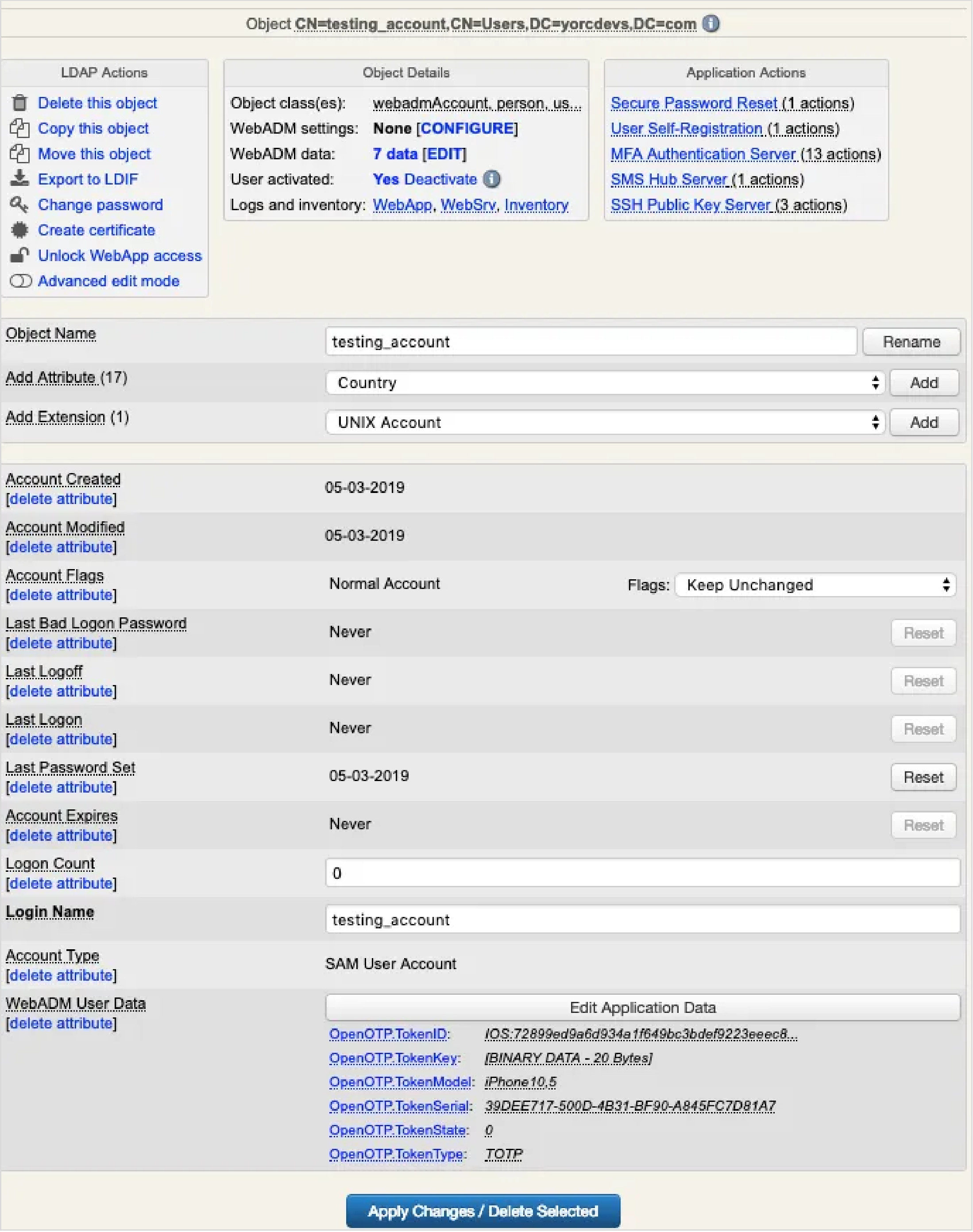
Test User Authentication for CN=testing_account,CN=Users,DC=yorcdevs,DC=com

Result: Success

Message: Authentication success

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`



Object CN=testing_account,CN=Users,DC=yorcdevs,DC=com

Object Details

Object class(es):	webadmAccount, person, us...
WebADM settings:	None [CONFIGURE]
WebADM data:	7 data [EDIT]
User activated:	Yes Deactivate
Logs and inventory:	WebApp, WebSrv, Inventory

Application Actions

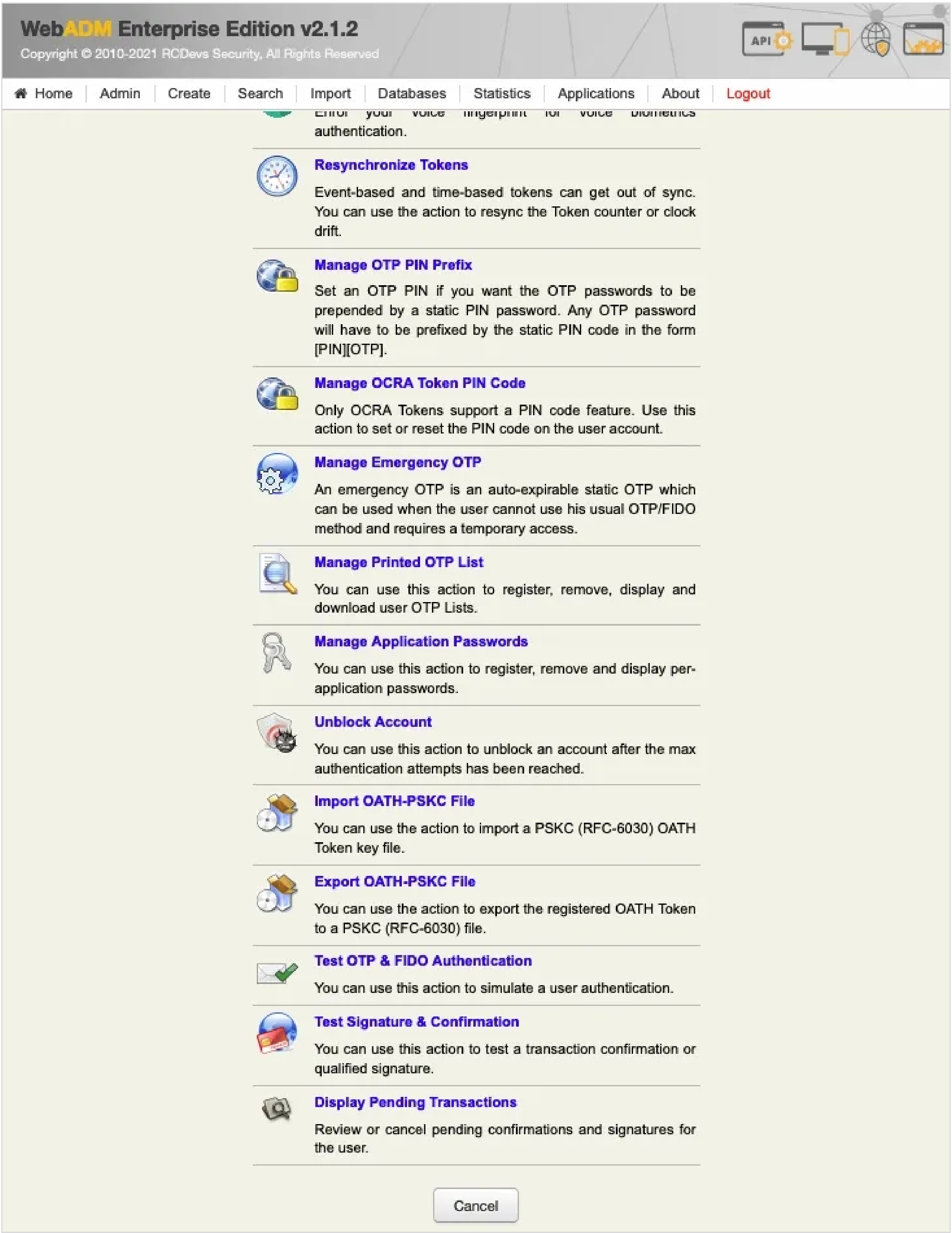
- Secure Password Reset (1 actions)
- User Self-Registration (1 actions)
- MFA Authentication Server (13 actions)
- SMS Hub Server (1 actions)
- SSH Public Key Server (3 actions)

Object Name	testing_account	Rename
Add Attribute (17)	Country	Add
Add Extension (1)	UNIX Account	Add

Account Created [delete attribute]	05-03-2019	
Account Modified [delete attribute]	05-03-2019	
Account Flags [delete attribute]	Normal Account	Flags: Keep Unchanged
Last Bad Logon Password [delete attribute]	Never	Reset
Last Logoff [delete attribute]	Never	Reset
Last Logon [delete attribute]	Never	Reset
Last Password Set [delete attribute]	05-03-2019	Reset
Account Expires [delete attribute]	Never	Reset
Logon Count [delete attribute]	0	
Login Name	testing_account	
Account Type [delete attribute]	SAM User Account	
WebADM User Data [delete attribute]	Edit Application Data	

OpenOTP.TokenID:	*IOS:72899ed9a6d934a1f649bc3bdef9223eeec8...*
OpenOTP.TokenKey:	*[BINARY DATA - 20 Bytes]*
OpenOTP.TokenModel:	*iPhone10,5*
OpenOTP.TokenSerial:	*39DEE717-500D-4B31-BF90-A845FC7D81A7*
OpenOTP.TokenState:	*0*
OpenOTP.TokenType:	*TOTP*

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



WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
API
Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

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].

Manage OCRA Token PIN Code

Only OCRA Tokens support a PIN code feature. Use this 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 OTP & FIDO Authentication

You can use this action to simulate a user authentication.

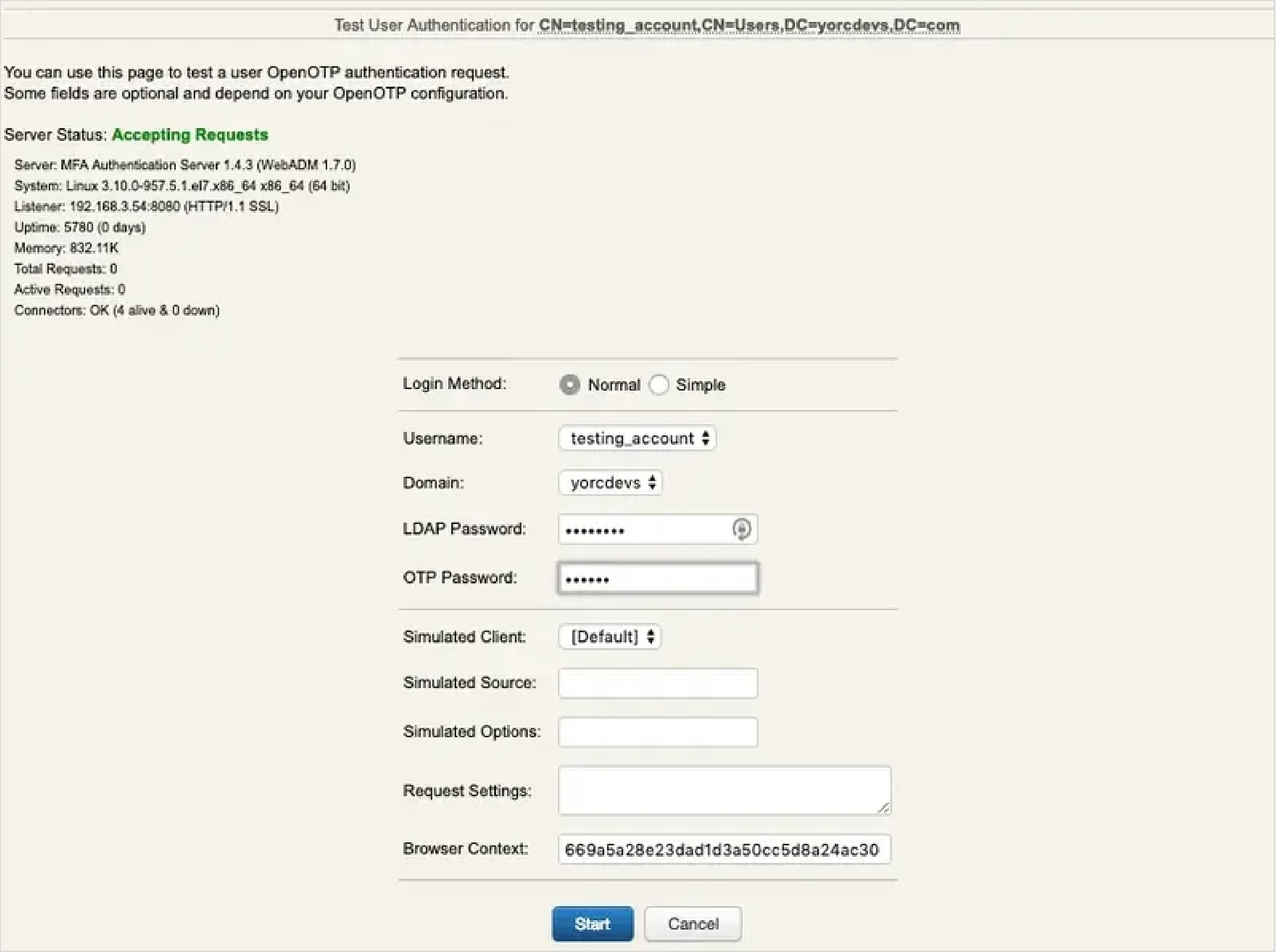
Test Signature & Confirmation

You can use this action to test a transaction confirmation or qualified signature.

Display Pending Transactions

Review or cancel pending confirmations and signatures for the user.

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`:



Test User Authentication for CN=testing_account,CN=Users,DC=yorcdevs,DC=com

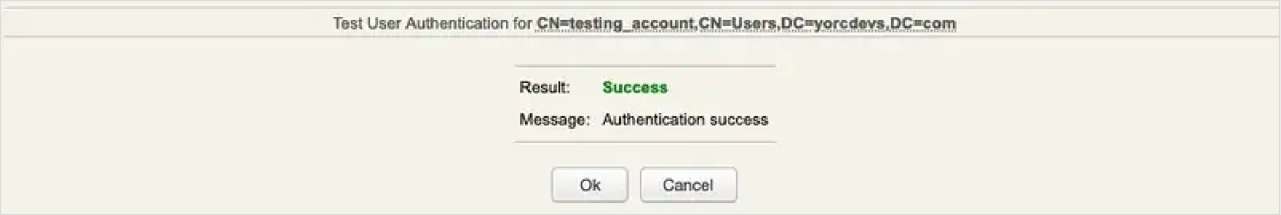
You can use this page to test a user OpenOTP authentication request.
Some fields are optional and depend on your OpenOTP configuration.

Server Status: Accepting Requests

Server: MFA Authentication Server 1.4.3 (WebADM 1.7.0)
System: Linux 3.10.0-957.5.1.el7.x86_64 x86_64 (64 bit)
Listener: 192.168.3.54:8080 (HTTP/1.1 SSL)
Uptime: 5780 (0 days)
Memory: 832.11K
Total Requests: 0
Active Requests: 0
Connectors: OK (4 alive & 0 down)

Login Method:	● Normal ○ Simple
Username:	testing_account
Domain:	yorcdevs
LDAP Password:	••••••••
OTP Password:	••••••
Simulated Client:	[Default]
Simulated Source:	
Simulated Options:	
Request Settings:	
Browser Context:	669a5a28e23dad1d3a50cc5d8a24ac30

We are authenticated!

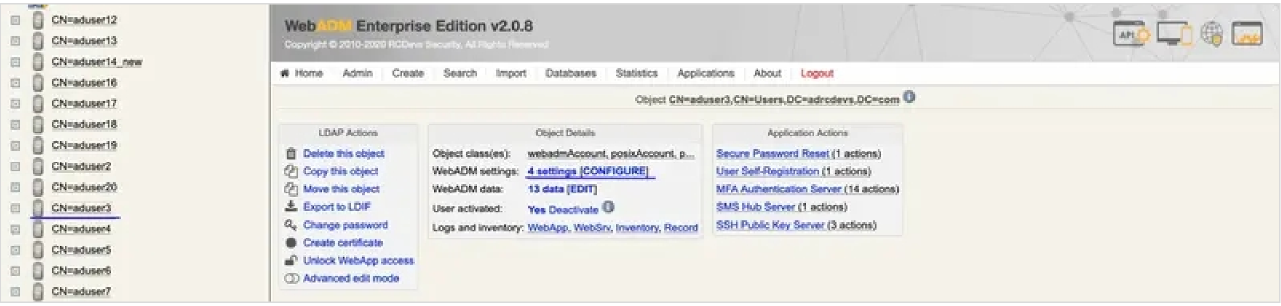


Test User Authentication for CN=testing_account,CN=Users,DC=yorcdevs,DC=com

Result:	Success
Message:	Authentication success

4.3 Voice Login

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

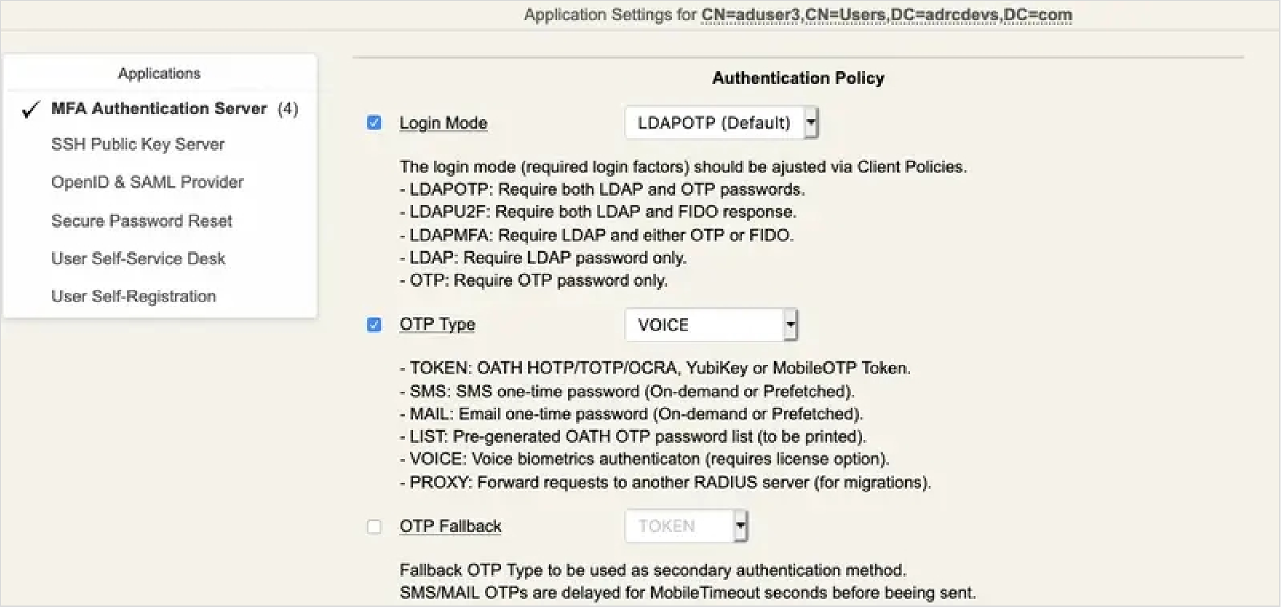


Object CN=aduser3,CN=Users,DC=adrcdevs,DC=com

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

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 ajusted 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).

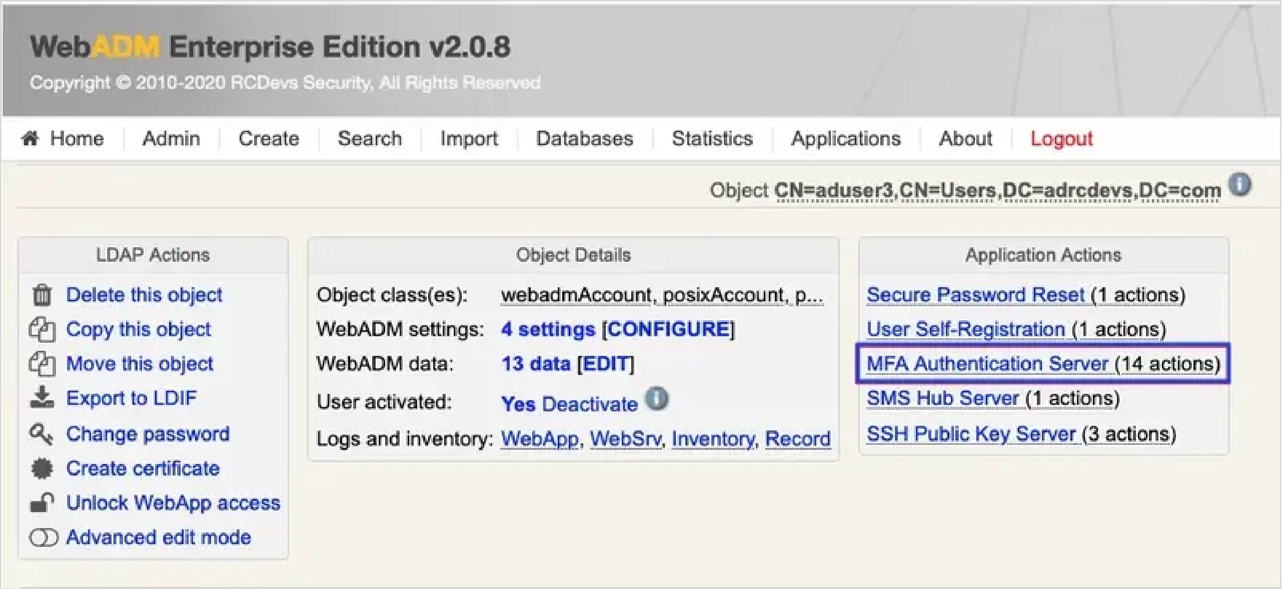
□ OTP Fallback: TOKEN

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

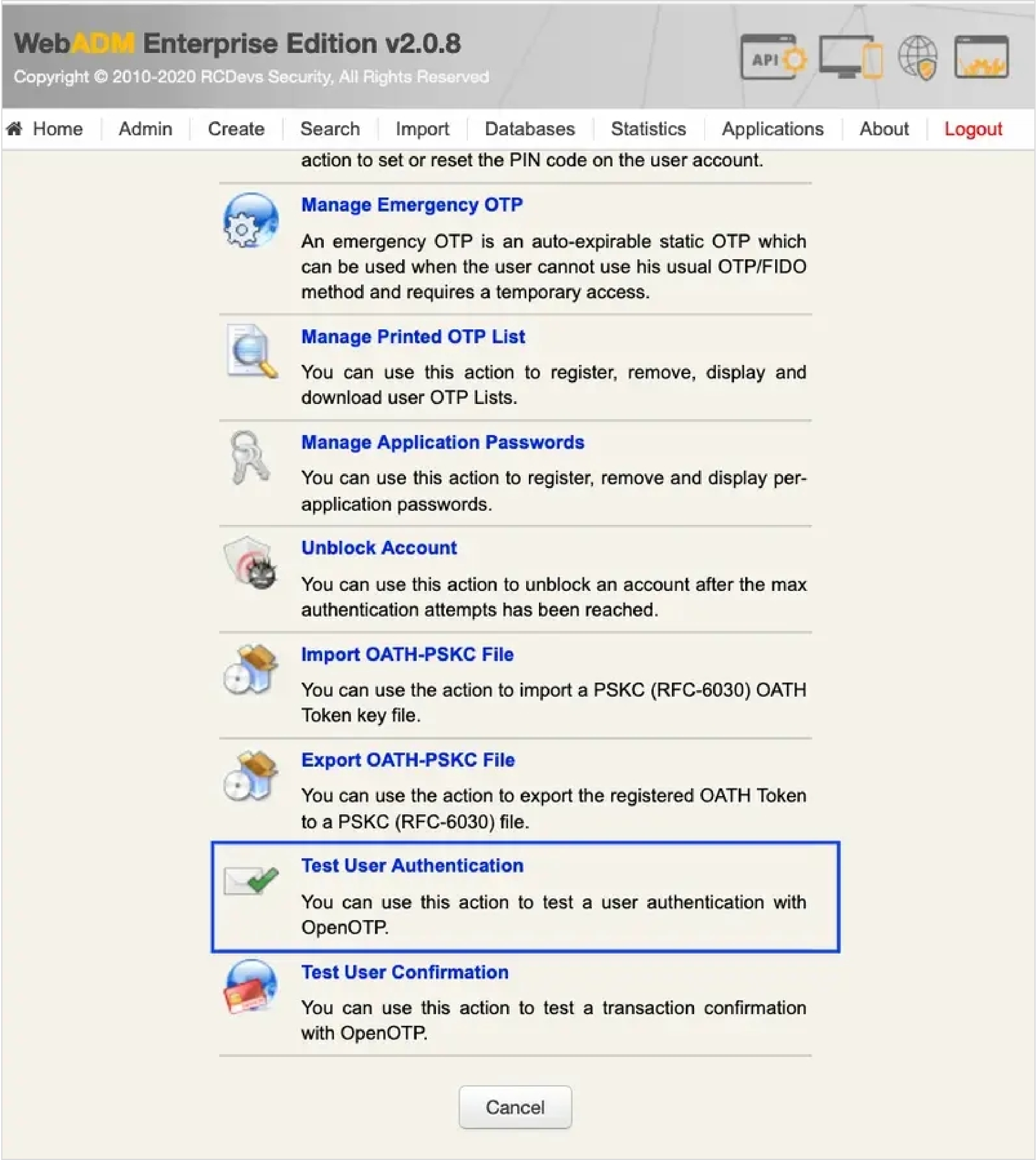
LDAP Actions
- Delete this object
- Copy this object
- Move this object
- Export to LDIF
- Change password
- Create certificate
- Unlock WebApp access
- Advanced edit mode

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)
- 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`:



WebADM Enterprise Edition v2.0.8
Copyright © 2010-2020 RCDevs Security, All Rights Reserved
Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

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.

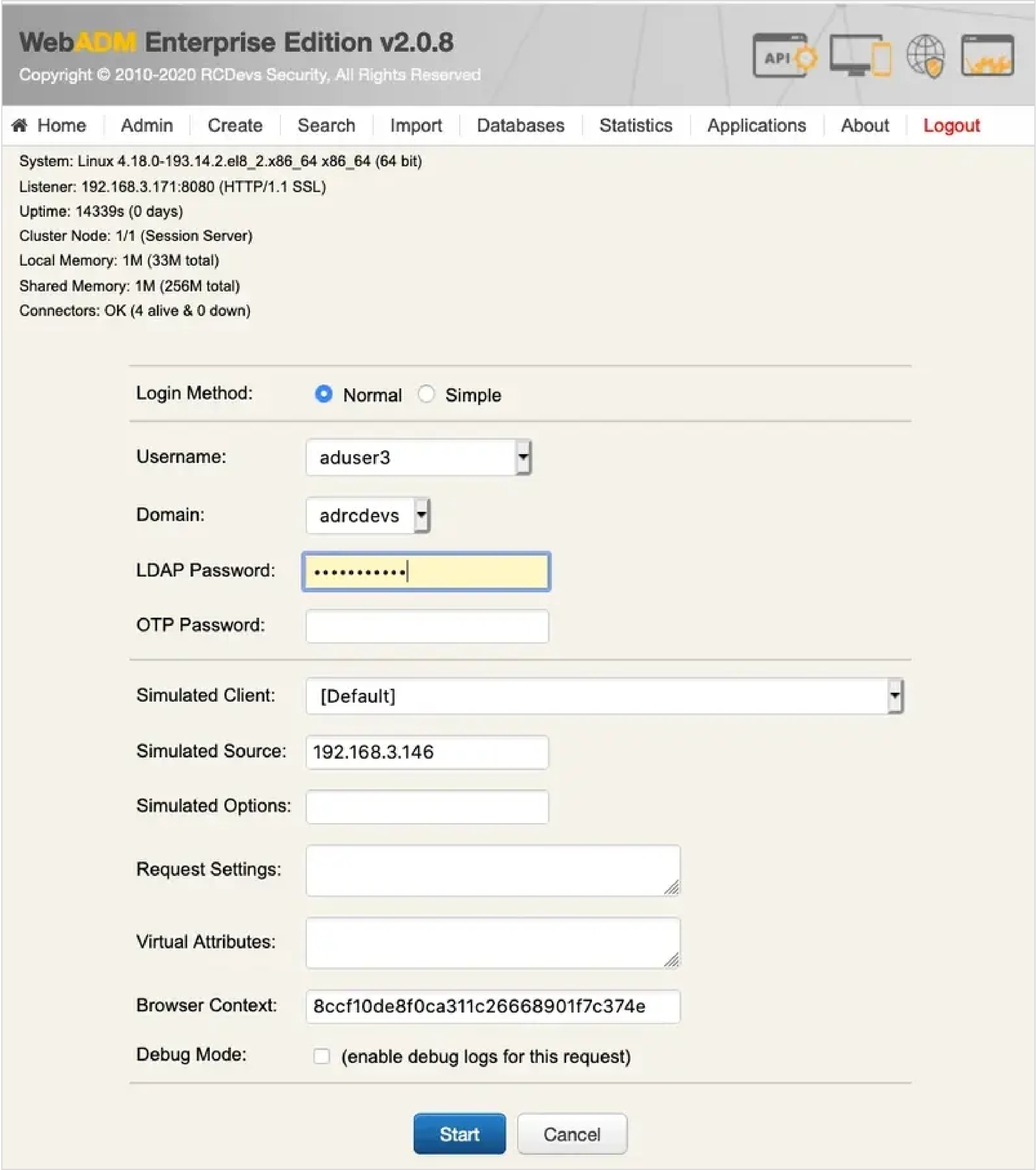
Test User Authentication

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.

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



WebADM Enterprise Edition v2.0.8

Copyright © 2010-2020 RCDevs Security, All Rights Reserved

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: aduser3

Domain: adrcdevs

LDAP Password: •••••••••••

OTP Password:

Simulated Client: [Default]

Simulated Source: 192.168.3.146

Simulated Options:

Request Settings:

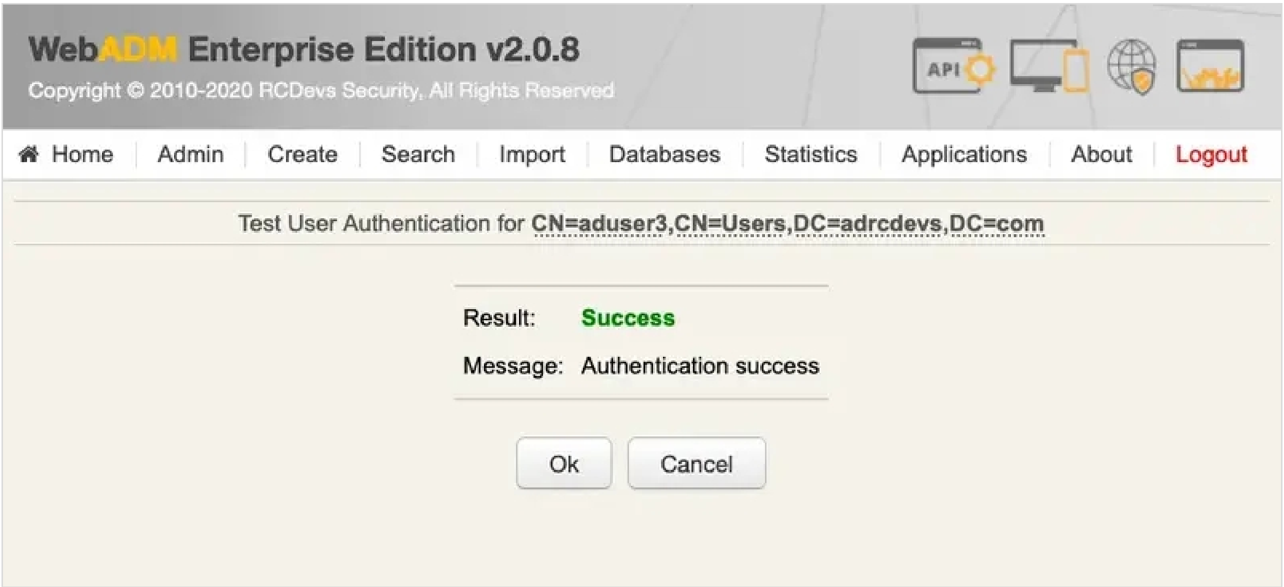
Virtual Attributes:

Browser Context: 8ccf10de8f0ca311c26668901f7c374e

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. Otherwise, you will be asked to enter your **Voice biometrics** in the test page.

We are authenticated!


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
Ok
Cancel

Test User Authentication for CN=aduser3,CN=Users,DC=adrcdevs,DC=com

Result: Success

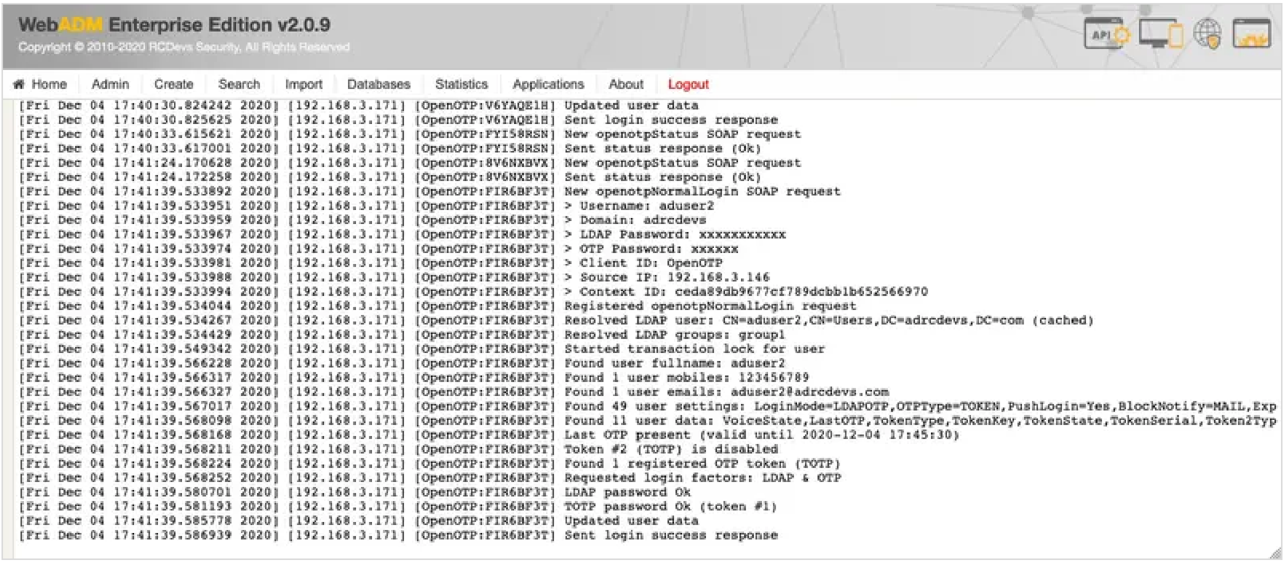
Message: Authentication success

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:


WebADM Enterprise Edition v2.0.9
Copyright © 2010-2020 RCDevs Security, All Rights Reserved
API
Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

```
[Fri Dec 04 17:40:30.824242 2020] [192.168.3.171] [OpenOTP:V6YAQE1H] Updated user data
[Fri Dec 04 17:40:30.825625 2020] [192.168.3.171] [OpenOTP:V6YAQE1H] Sent login success response
[Fri Dec 04 17:40:33.615621 2020] [192.168.3.171] [OpenOTP:FYI58RSN] New openotpStatus SOAP request
[Fri Dec 04 17:40:33.617001 2020] [192.168.3.171] [OpenOTP:FYI58RSN] Sent status response (Ok)
[Fri Dec 04 17:41:24.170628 2020] [192.168.3.171] [OpenOTP:8V6NXBVX] New openotpStatus SOAP request
[Fri Dec 04 17:41:24.172258 2020] [192.168.3.171] [OpenOTP:8V6NXBVX] Sent status response (Ok)
[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,OTPType=TOKEN,PushLogin=Yes,BlockNotify=MAIL,Exp
[Fri Dec 04 17:41:39.568098 2020] [192.168.3.171] [OpenOTP:FIR6BF3T] Found 11 user data: VoiceState,LastOTP,TokenType,TokenKey,TokenState,TokenSerial,Token2Typ
[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
```

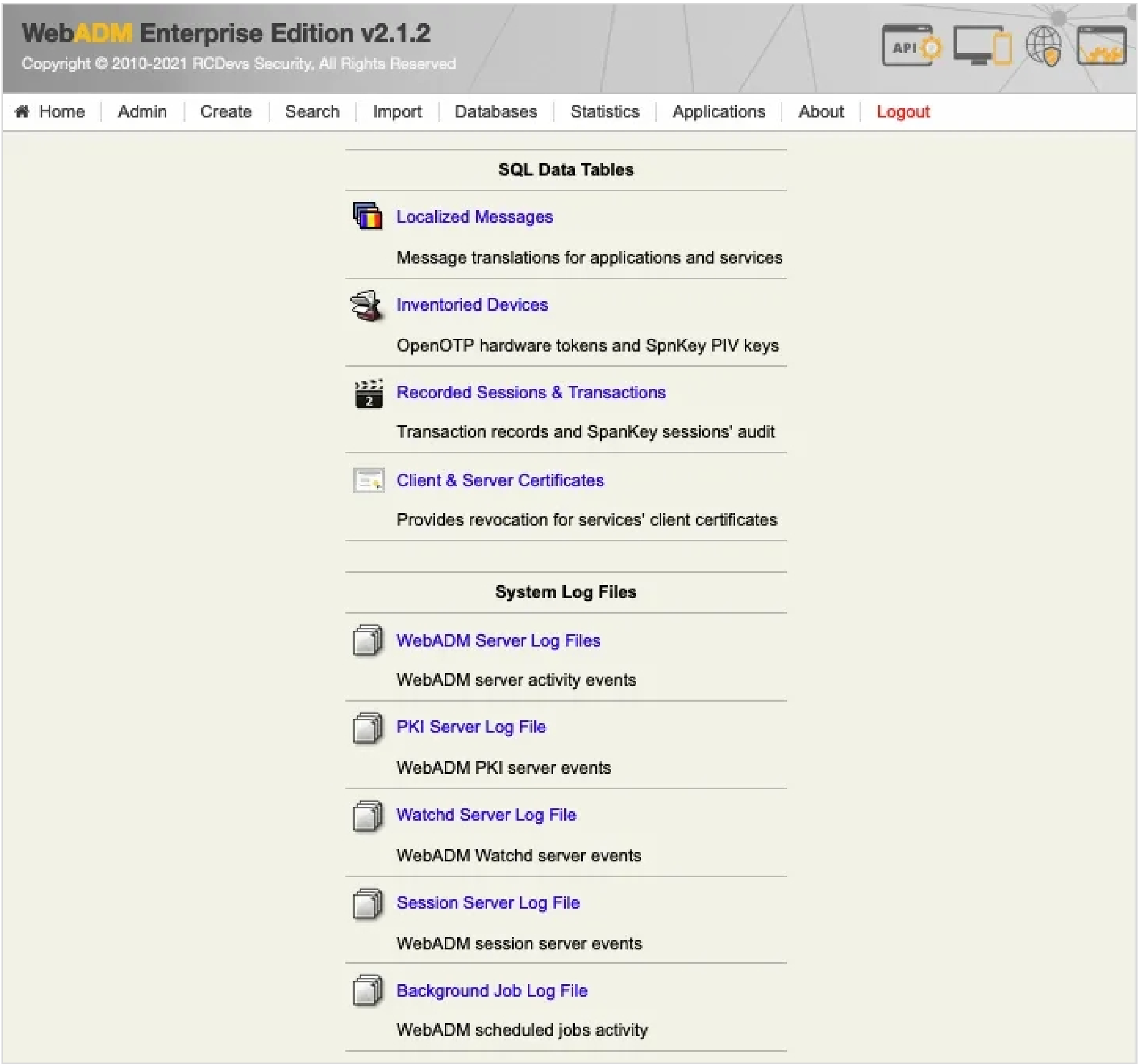
Each authentication is identified by an ID. Here, it is **FIR6BF3T**.

```
[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,OTPType=TOKEN,PushLogin=Yes,BlockNotify=MAIL,ExpireNotify=MAIL,ChallengeMode
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,Token2State,Toke

[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:



WebADM Enterprise Edition v2.1.2
Copyright © 2010-2021 RCDevs Security, All Rights Reserved
Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

SQL Data Tables

Localized Messages
Message translations for applications and services

Inventoried Devices
OpenOTP hardware tokens and SpnKey PIV keys

Recorded Sessions & Transactions
Transaction records and SpanKey sessions' audit

Client & Server Certificates
Provides revocation for services' client certificates

System Log Files

WebADM Server Log Files
WebADM server activity events

PKI Server Log File
WebADM PKI server events

Watchd Server Log File
WebADM Watchd server events

Session Server Log File
WebADM session server events

Background Job Log File
WebADM scheduled jobs activity

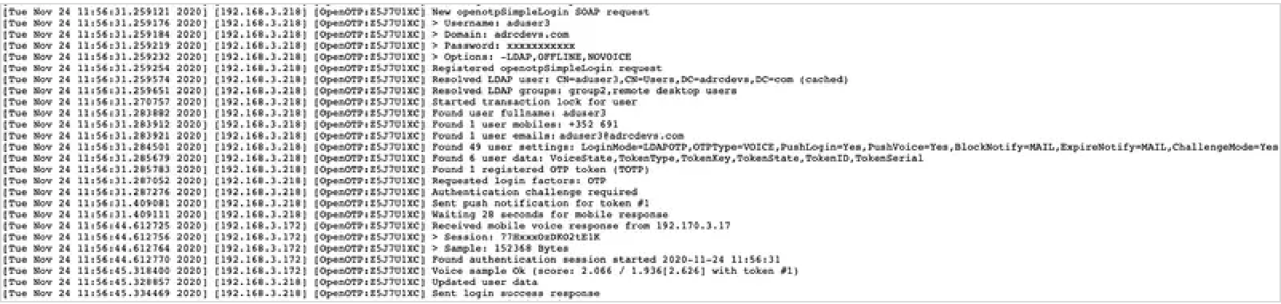
Each authentication is identified by an ID. Here, it is **JTLYVX0O**.

```
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] New openotpNormalLogin SOAP request
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] > Username: testing_account
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] > Domain: yorcdevs
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] > LDAP Password: xxxxxxxx
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] > OTP Password: xxxxxx
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] > Client ID: OpenOTP
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] > Source IP: 192.168.3.54
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] > Context ID:
669a5a28e23dad1d3a50cc5d8a24ac30
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Registered openotpNormalLogin request
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Resolved LDAP user:
CN=testing_account,CN=Users,DC=yorcdevs,DC=com
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Started transaction lock for user
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Found user fullname: testing_account
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Found 43 user settings:
LoginMode=LDAPOTP,OTPType=TOKEN,OTPLength=6,ChallengeMode=Yes,ChallengeTimeout=90,MobileTim
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,PrefetchExpire=10,

[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Found 5 user data:
TokenType,TokenKey,TokenState,TokenID,TokenSerial
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Found 1 registered OTP token (TOTP)
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Requested login factors: LDAP & OTP
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] LDAP password Ok
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] TOTP password Ok (token #1)
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Updated user data
[2019-03-08 14:39:09] [192.168.3.54] [OpenOTP:JTLYVX0O] Sent success response
```

5.3 Voice Biometrics Logs

Now, we can check the logs using Voice Biometrics. Ze 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: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: +352 691
[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,ExpireNotify=MAIL,ChallengeMode=Yes
[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[2.624] 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
```

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,OTPType=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.