# FIDO2 AND PASSKEYS AUTHENTICATION WITH OPENOTP

# FIDO2 and Passkeys authentication with OpenOTP

FIDO2 TMP Passkeys WebAuthn iOS Android Security keys

## 1. Overview

OpenOTP supports FIDO2 standard from the FIDO Alliance for user authentication and Passkeys provided by Google or Apple. If you intend to use OpenOTP with FIDO2 or Passkeys, please read this document which explains how to enable and use it with your integrations.

### 1.1 FIDO2

FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP).

FIDO2 cryptographic login credentials are unique across every website, never leave the user's device and are never stored on a server. This security model eliminates the risks of phishing, all forms of password theft and replay attacks.

Users unlock cryptographic login credentials with simple built-in methods such as fingerprint readers or cameras on their devices, or by leveraging easy-to-use FIDO security keys. Consumers can select the device that best fits their needs.

Because FIDO cryptographic keys are unique for each internet site, they cannot be used to track users across sites. Plus, biometric data, when used, never leaves the user's device.

Websites can enable FIDO2 through a simple JavaScript API call that is supported across leading browsers and platforms on billions of devices consumers use every day.

**Note**

Read more about FIDO on the Alliance website : https://fidoalliance.org.

U2F APIs are now deprecated in favor of FIDO2. From WebADM v2.2, U2F support has been removed from OpenOTP Security Suite and its integration. It means, you are not able to register U2F devices anymore, but you can still use them if they have been registered on previous WebADM/OpenOTP versions. RCDevs implemented in OpenOTP the possibility to enroll a deprecated U2F device in FIDO2 mode. That way, you don't need to buy new security keys to switch to FIDO2 technology. There is no configuration to enable that feature, it is fully automatic and managed by WebADM.

### 1.2 Passkeys

Passkeys, also known as Web Authentication (WebAuthn), are a new and promising technology that aims to replace passwords as the primary method of online authentication. Passkeys offer several advantages over passwords, including:

- Enhanced security: Passkeys are based on cryptography and are resistant to phishing attacks, which can be used to steal

passwords.

- Ease of use: Passkeys are stored on your device and can be signed in with your fingerprint, face ID, or a PIN. This eliminates the need to remember and manage multiple passwords.
- Cross-platform compatibility: Passkeys are supported by all major web browsers and operating systems. This means that you can use the same set of passkeys to sign in to websites and apps on your computer, phone, and tablet.
- Privacy: Passkeys do not share your personal information with websites or apps. This makes them a more privacy-friendly authentication method.

Here are some of the key benefits of using passkeys:

- Improved security: Passkeys are much more difficult to hack than passwords. This is because they are based on cryptography and are not stored on websites or apps.
- Reduced password fatigue: Passkeys eliminate the need to remember and manage multiple passwords. This can save users time and frustration.
- Increased productivity: Passkeys can make it easier to sign in to websites.
- Reduced risk of phishing attacks: Passkeys are resistant to phishing attacks, which can be used to steal passwords.
- Improved user experience: Passkeys can provide a more seamless and secure sign-in experience for users.

Have a look on Apple and Google websites for more information about their Passkeys technology and support across devices, accounts, passkeys sharing…

## 2. Integrations Supported by RCDevs Solutions

### 2.1 FIDO2 Technology (security keys)

RCDevs is supporting FIDO2 authentication on the following integrations:

- RCDevs Identity Provider (OpenID/SAML IDP);
- OpenOTP Credential Provider for Windows;
- OpenOTP Credential Provider for macOS;
- MFAVPN with Viscosity VPN client;
- OpenOTP Plugin for Nextcloud;
- OpenOTP Plugin for ADFS;
- OpenOTP Plugin for RDWeb;
- Spankey SSH key authentication (2nd factor);
- Authentication on RCDevs Web Applications like Selfdesk, SelfReg and Helpdesk.

> **Note for Windows and MAC Credential Providers**
>
> The FIDO2 challenge is not supported through Remote Desktop Protocol (RDP). FIDO2 keys can be used for offline logins on these 2 integrations.

FIDO2 has been designed to be used with a single origin, and the public key registered during the enrollment process is associated with that origin. If you wish to use it across multiple origins, the key must be registered multiple times, once for each origin.

### 2.2 Passkey Technology

RCDevs is supporting Passkeys authentications on the following integrations:

- RCDevs Identity Provider (OpenID/SAML IDP);
- Authentication on RCDevs Web Applications like Selfdesk, SelfReg and Helpdesk;
- OpenOTP Plugin for Nextcloud;
- OpenOTP Plugin for ADFS;
- OpenOTP Plugin for RDWeb;

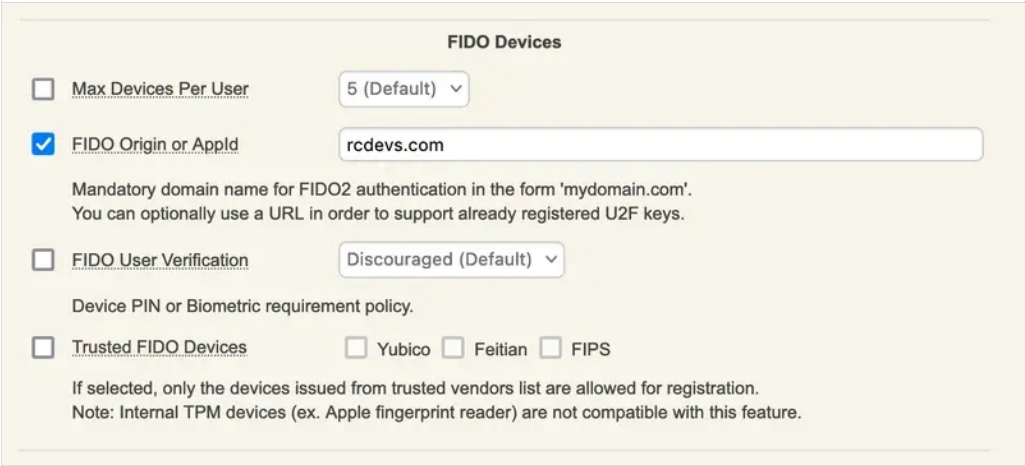
The registration of Passkeys devices with the RCDevs solutions is facilitated through FIDO2 Token registration via the WebADM Admin Portal or any other Self-Services portals offered by RCDevs, accessible under the FIDO tab.

## 3. FIDO Configuration in OpenOTP

To enable FIDO2 or Passkeys authentication with the RCDevs solutions, you need to edit your OpenOTP configuration under the `Applications` tab in WebADM and scroll down to the `FIDO Devices` section.

You must configure the FIDO origin or AppID setting, which should match the base DNS name of your domain. In this example, rcdevs.com is configured as the domain name for the FIDO origin. It is crucial to configure this setting correctly for the feature to work as intended. If, for any reason, the domain name of your organization changes (e.g: rcdevs.eu), registered FIDO2 devices will need to be re-registered with the new origin.

In other words, changing the origin used during enrollment will disrupt the authentication for FIDO2 devices registered with the old origin/base domain.




Other settings allow you to limit how many devices can be registered per user. You can optionnaly request the `FIDO User verification` by the FIDO2 device in order to use it during the authentication process.

To finish, you can also choose which `Trusted devices` are allowed in your organization. For Passkeys, that option should not be enabled.

**⚠ Note**

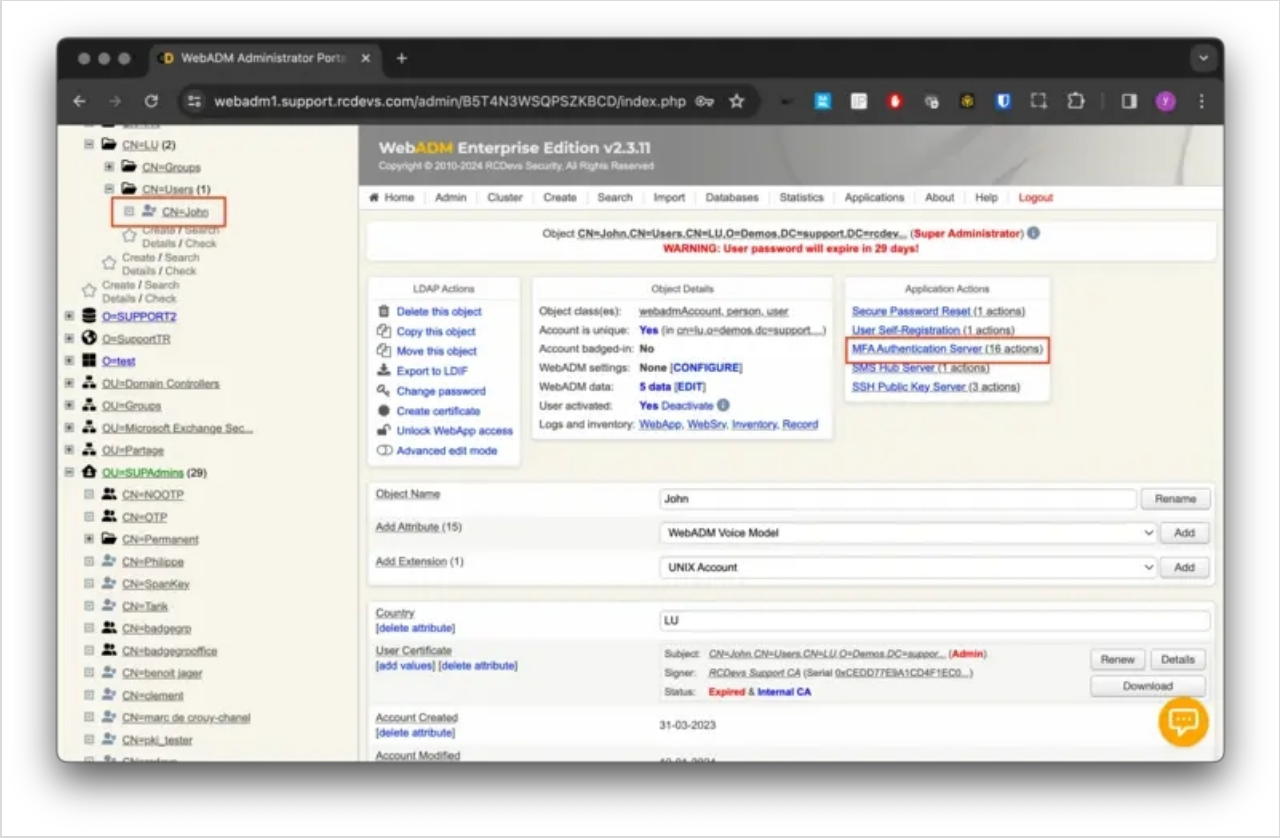
If you change the domain you must register the tokens again and also change the domain in FIDO Origin, otherwise you will have this warrning: The DNS domain in the FIDO Origin does not match the current URL domain .Please use an enrolment URL under the configured FIDO Origin

# 4. Register FIDO Devices

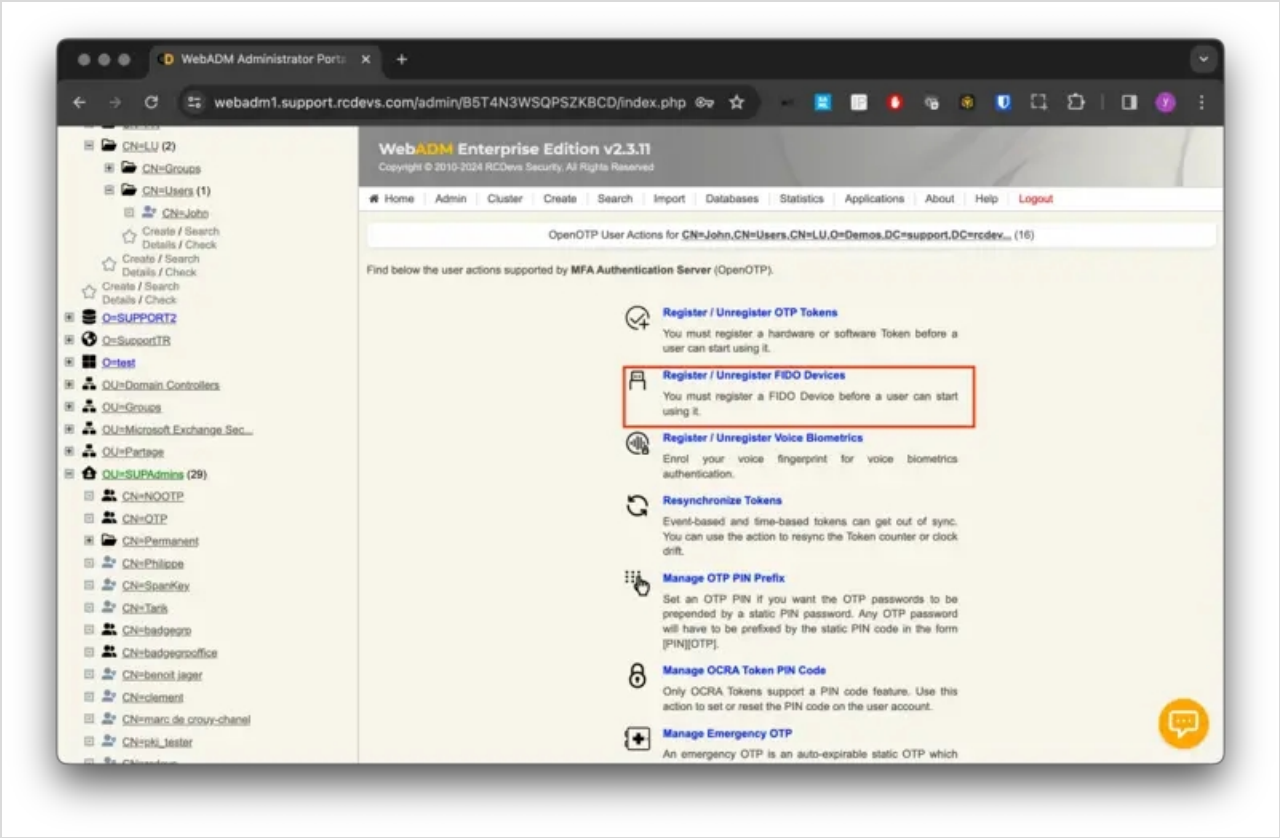
## 4.1 FIDO2 security key

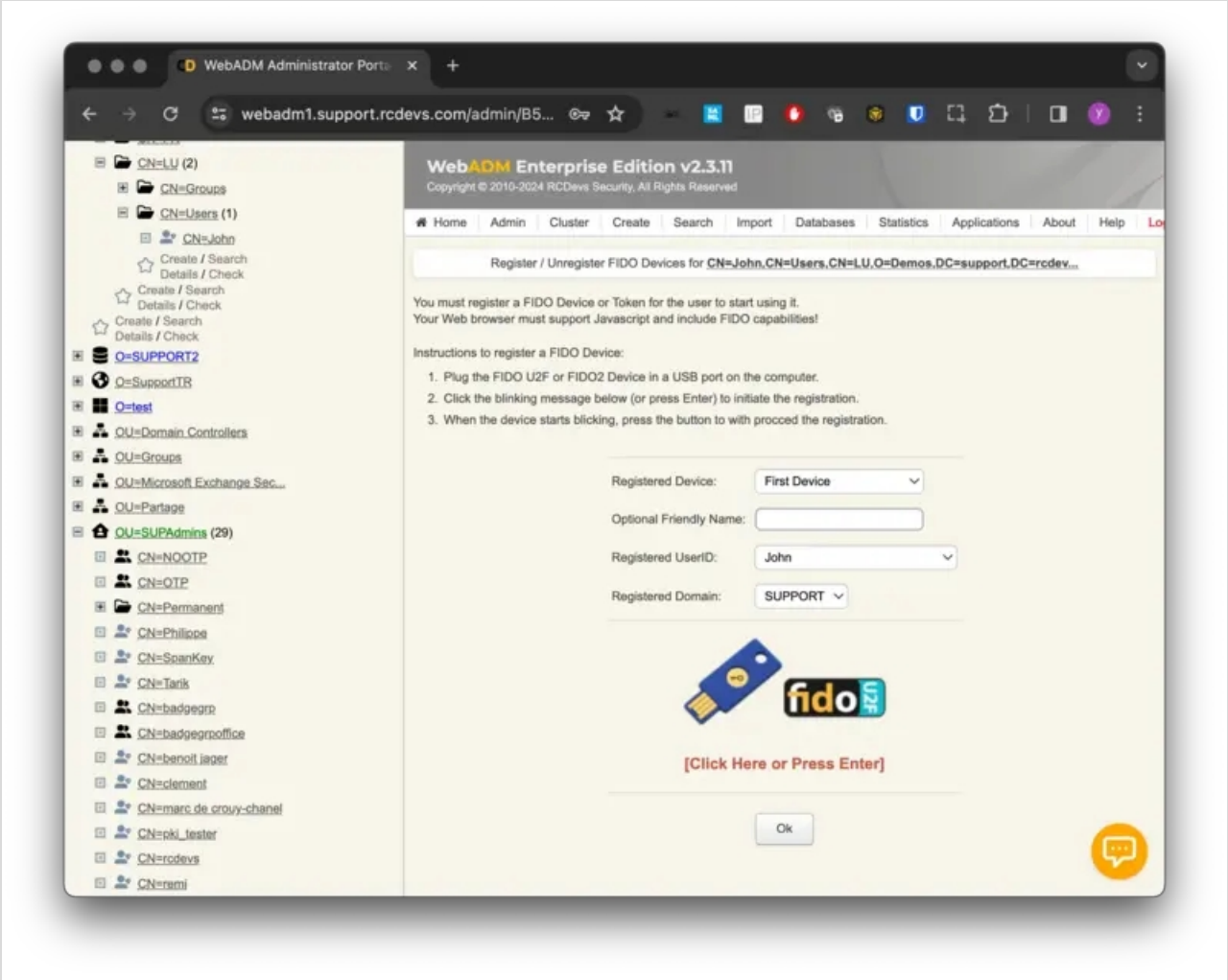
### 4.1.1 From WebADM Admin GUI

FIDO2 keys must undergo a registration process before they can be utilized for authentication.

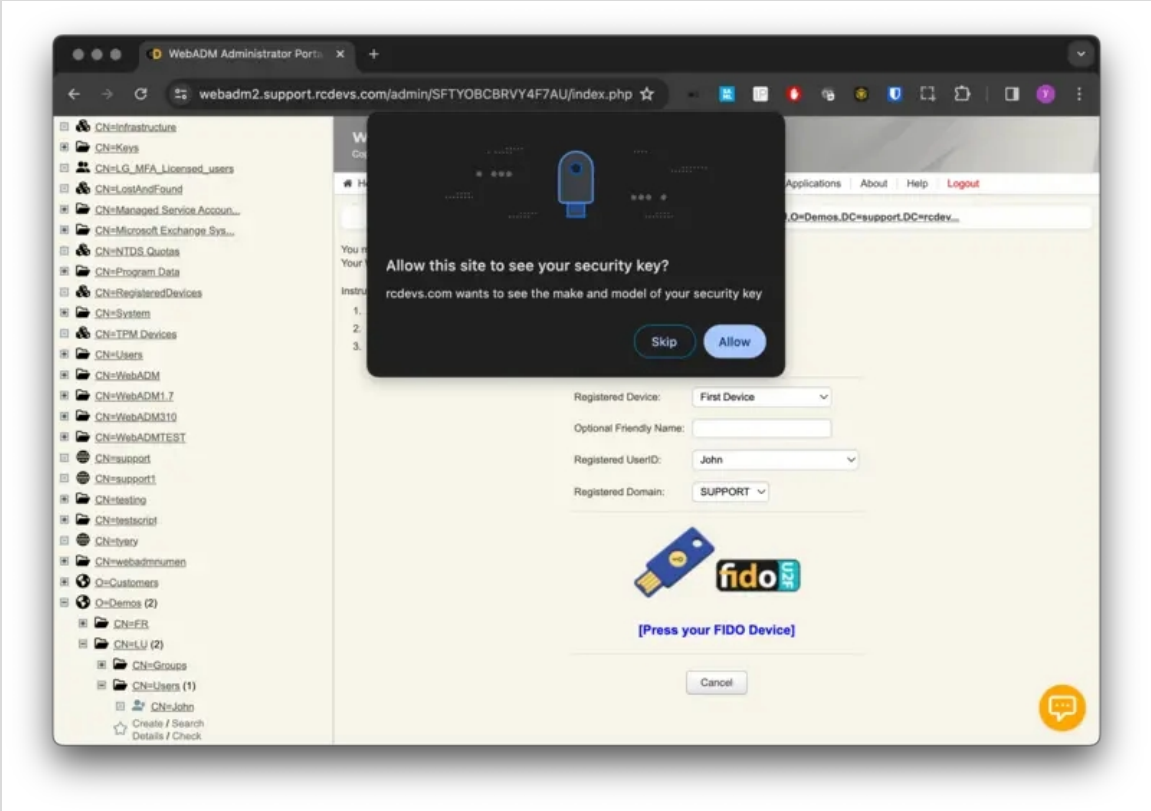



Now click on `Register / Unregister FIDO Devices`

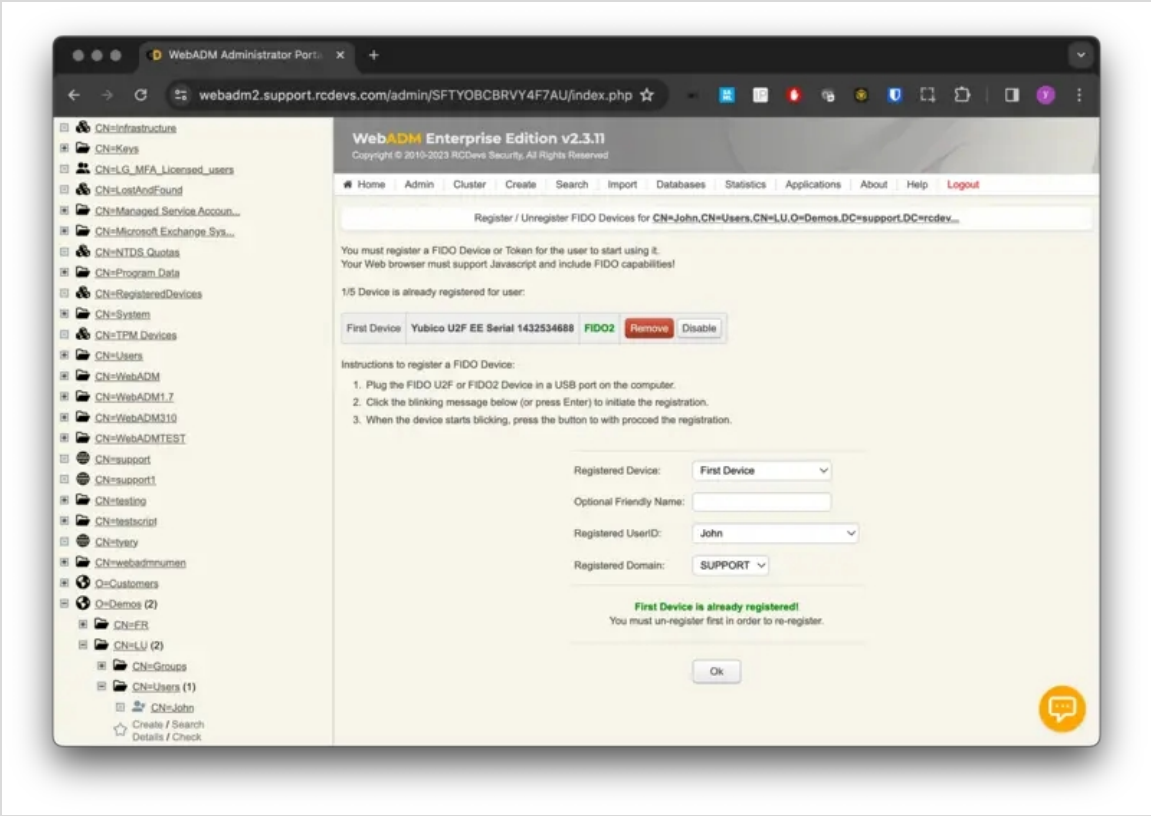





Click on the red message which is blinking to start the registration process. You are then invited to press your FIDO2 device and allow the site to access your security key.

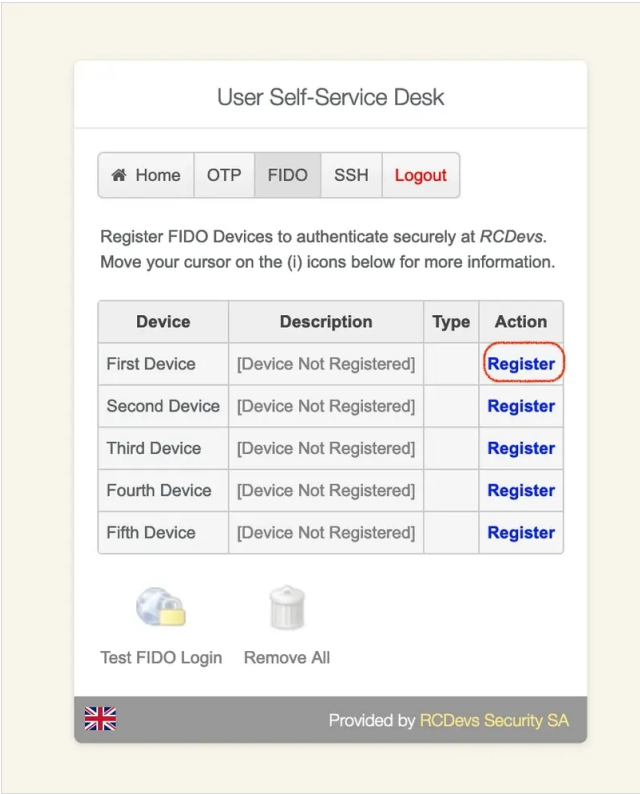


Once done, the registration is performed and you should have a screen similar to the one below:

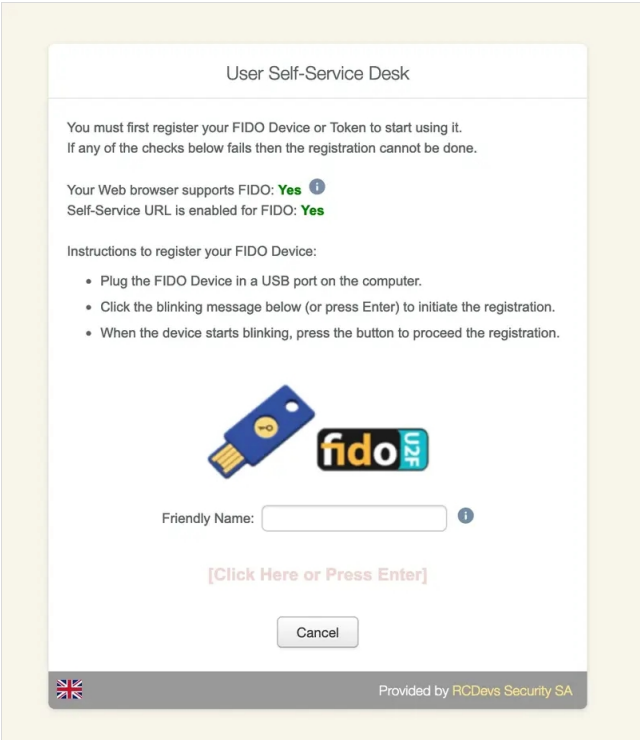



### 4.1.2 From User Self-Service Desk or User Self Registration applications

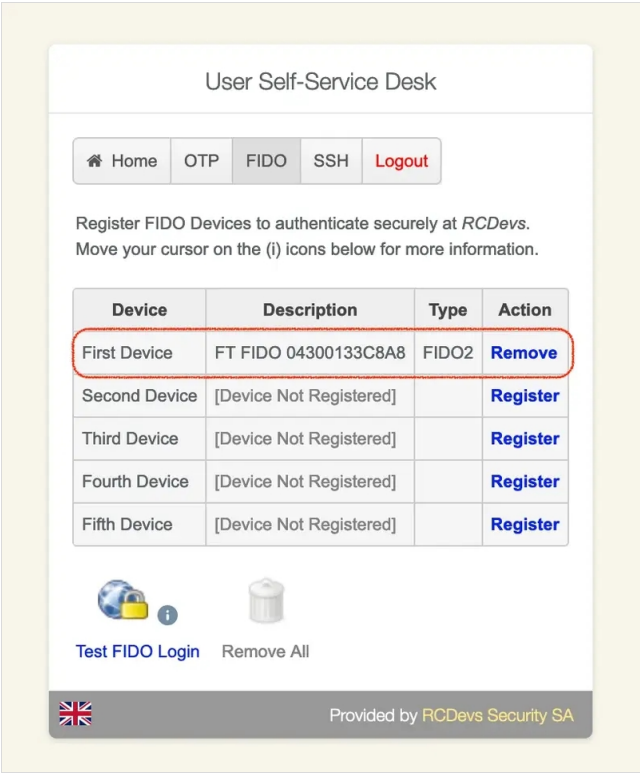
Here, we demonstrate FIDO2 enrollment using the SelfDesk application, but the process is the same for the SelfReg application. Before proceeding, ensure that FIDO2 enrollment is enabled in the configurations of SelfDesk or SelfReg. This enables users to access the FIDO tab after authentication on the self-services platform. Click on the `FIDO`, select the desired token slot, and click the Register button to initiate the enrollment process.




Once you clicked on `Register`, you are prompted for the following screen:

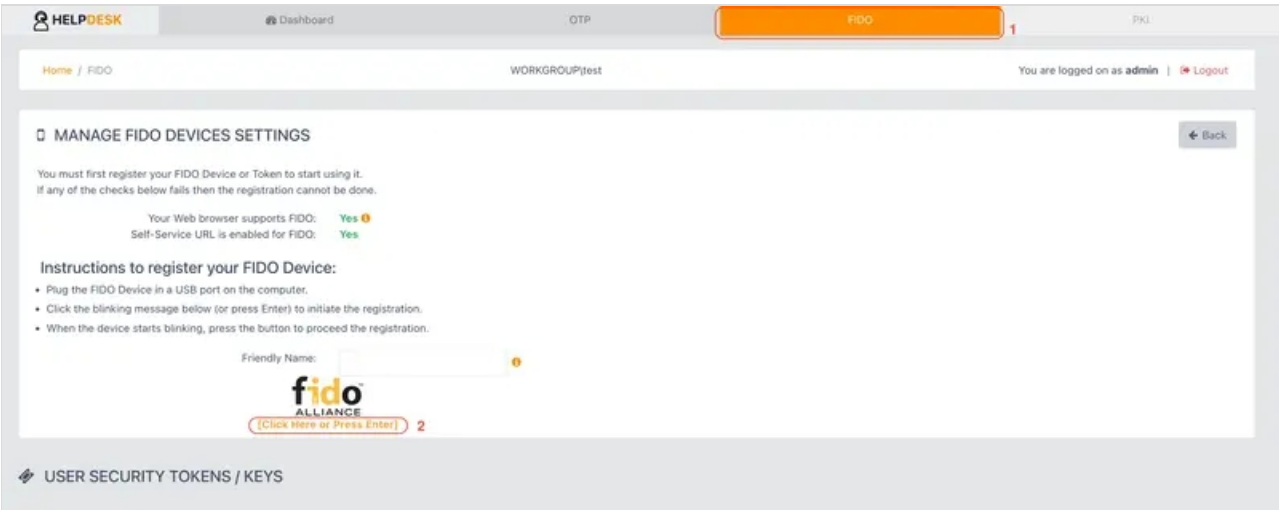



Click on the red message which is blinking to start the registration process. You are then invited to press your FIDO2 device. Press it and the registration should be done. On the next screen, you see the device enrolled.

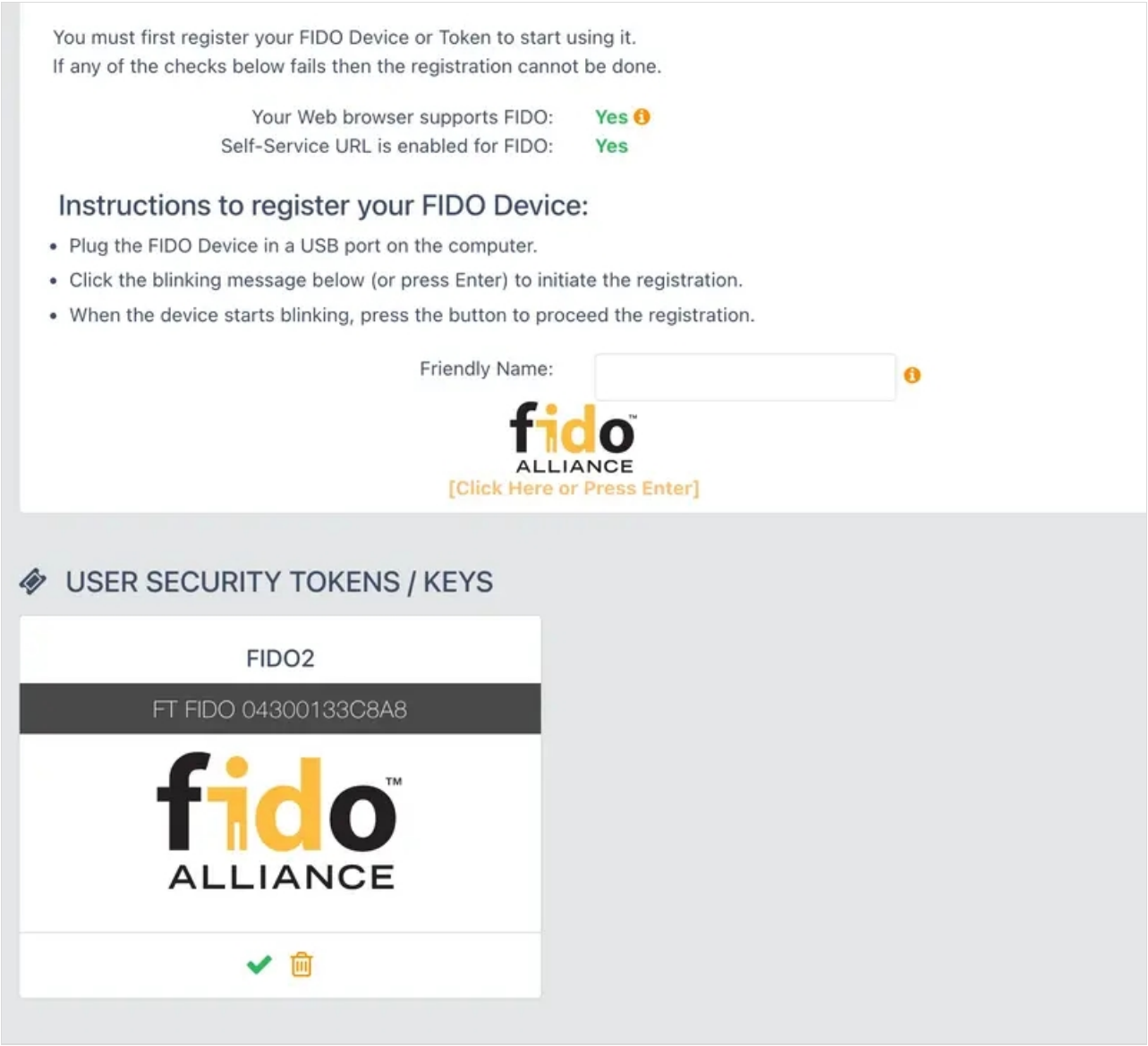



### 4.1.3 From HelpDesk application

Let's register your FIDO2 device from Helpdesk. Before doing it, you must enable the FIDO2 enrollment from Helpdesk configuration in order for your Helpdesk users to access the FIDO tab below. Once arrived at that page, click on the orange message to start the registration.




You are then invited to press your FIDO2 key. Press it and the enrollment is finished.




## 5. Register Passkeys

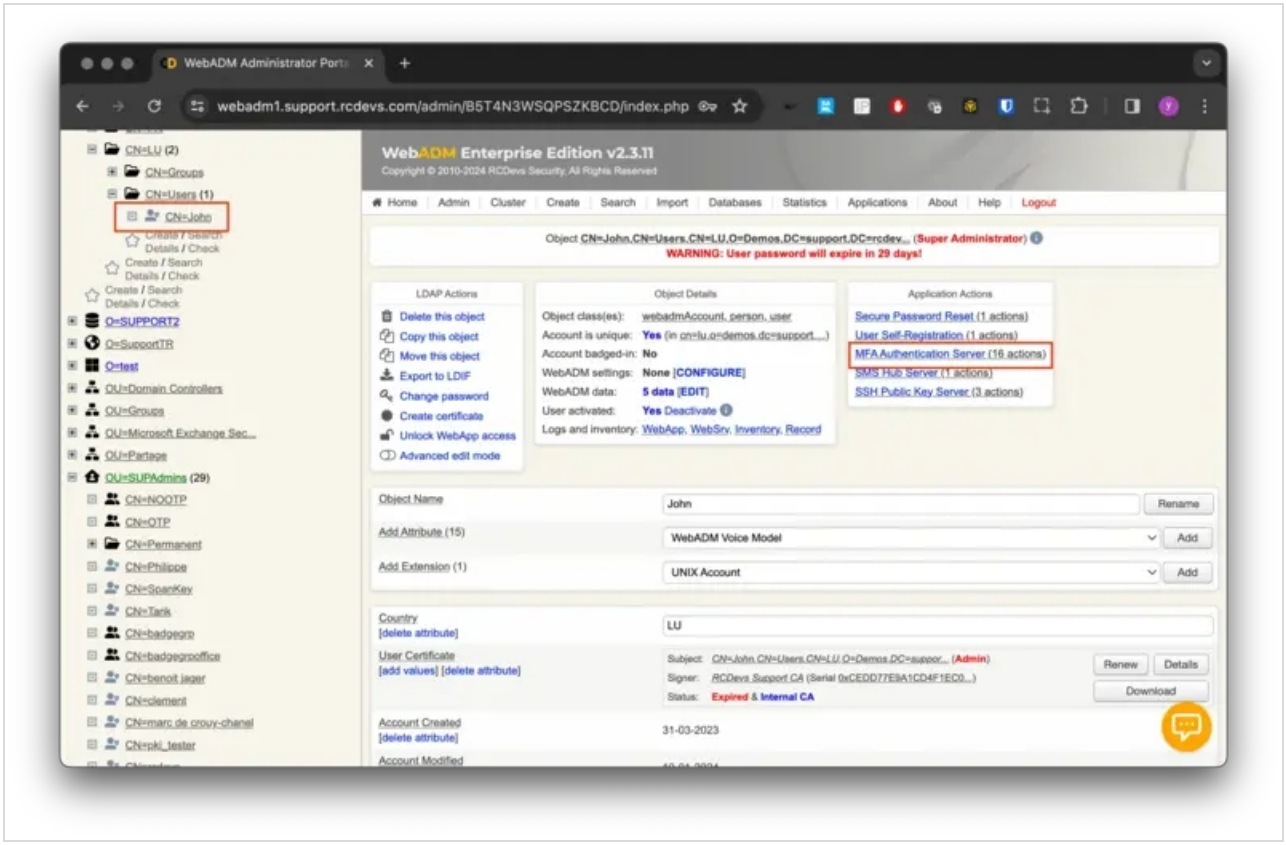
There are multiple ways to register a passkey:

- Store the Passkey in your iCloud Keychain from a compatible Apple device. This enables you to use the Passkey across all devices connected to the same iCloud account.
- Use an iPhone, iPad, or Android device. This method allows you to register and use the passkey from a device with a camera.
- Use a security key. This is typically the way to register a FIDO2 key.
- From Google Chrome, you have the option to register a Passkey in your Chrome profile.

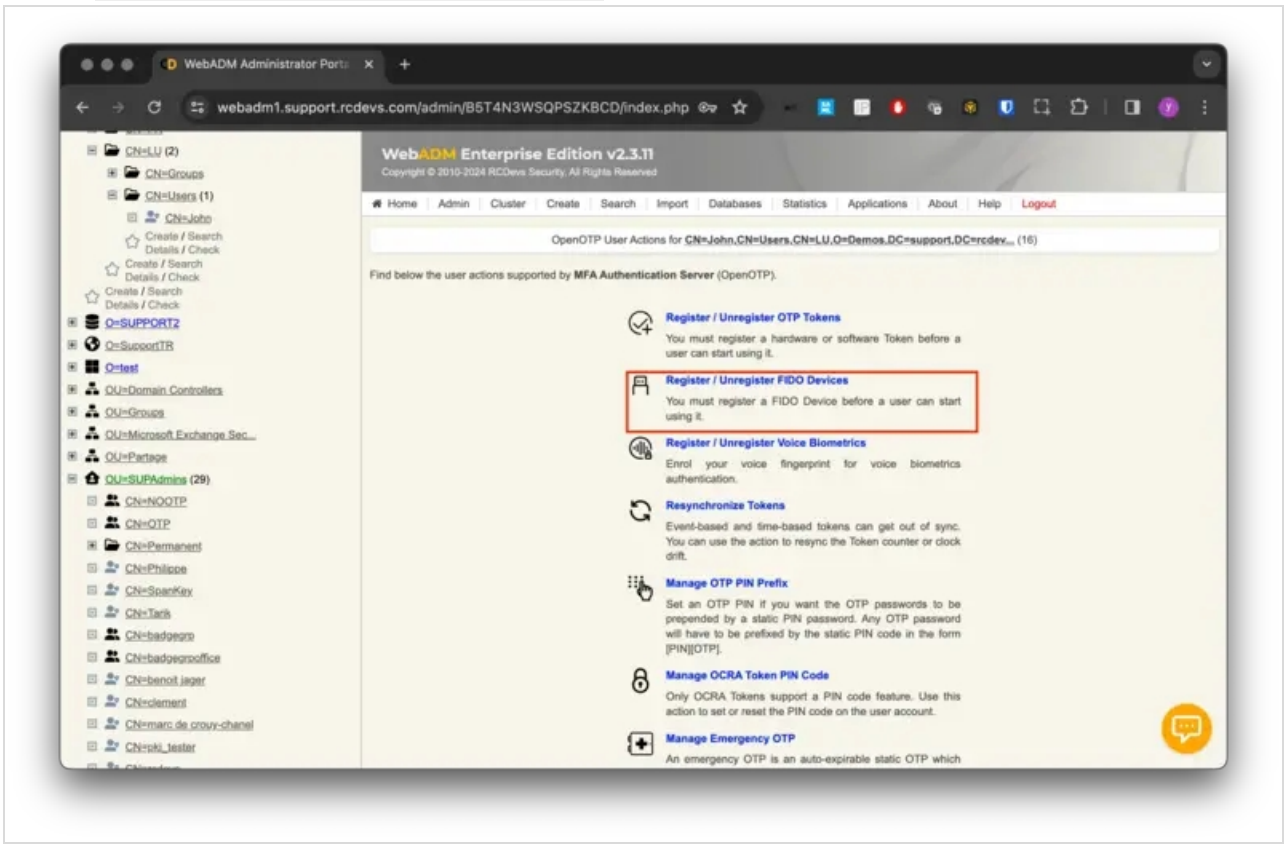
Select the method that best suits your preferences and aligns with the prerequisites set by Apple/Google and your company. Follow the provided instructions to complete the enrollment process.

The enrollments demonstrated below are conducted through the WebADM Admin GUI. It's important to note that the same enrollment options are available through various self-service web applications provided by RCDevs under the FIDO tab. Users can access these enrollment features from different self-service portals for a seamless and consistent experience.

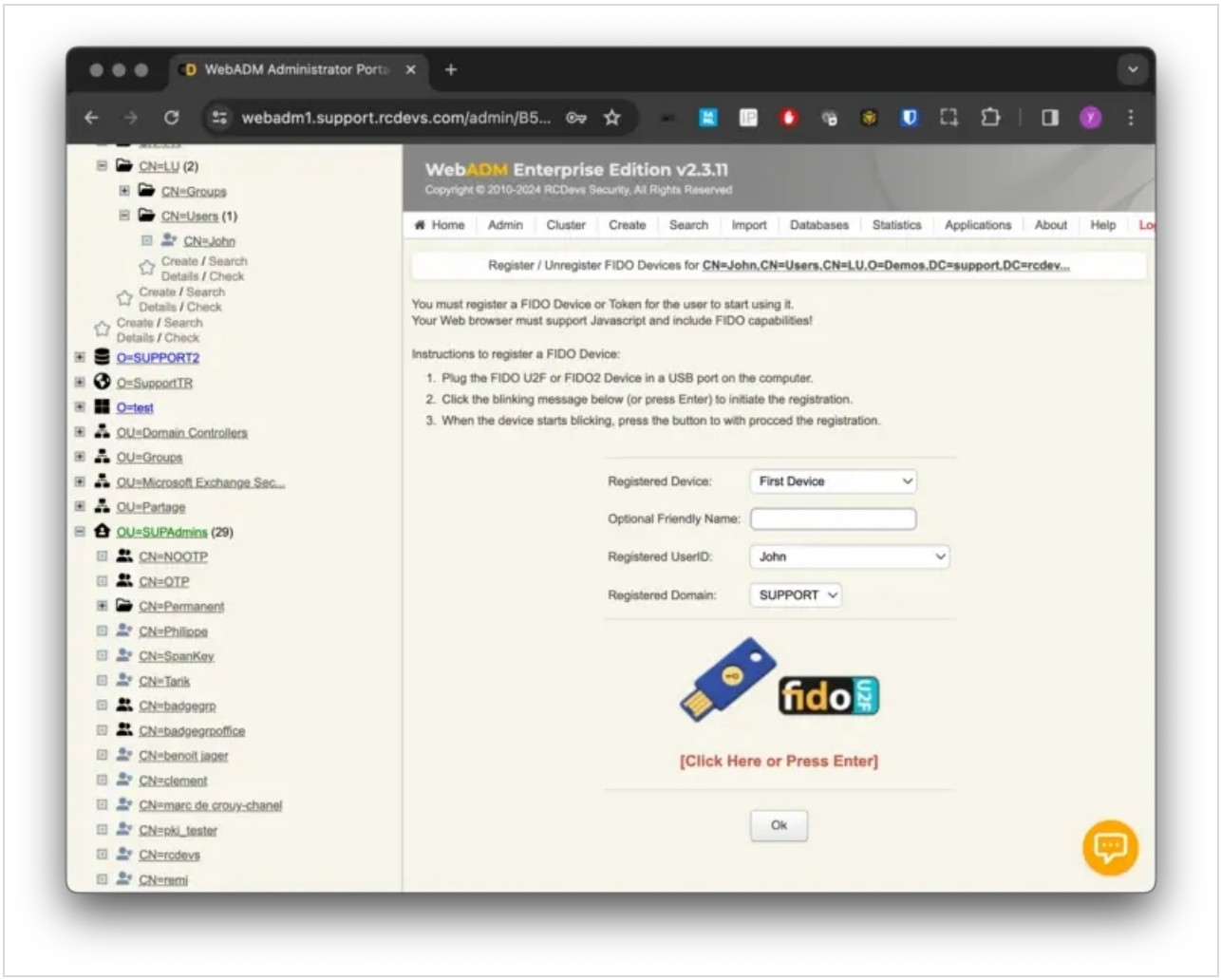
Passkeys must undergo a registration process before they can be utilized for authentication. Let's proceed with the registration, select the user account you want to register a passkeys and in `Application Actions` box, select `MFA Authentication Server`:




Now click on `Register/Unregister FIDO Devices`



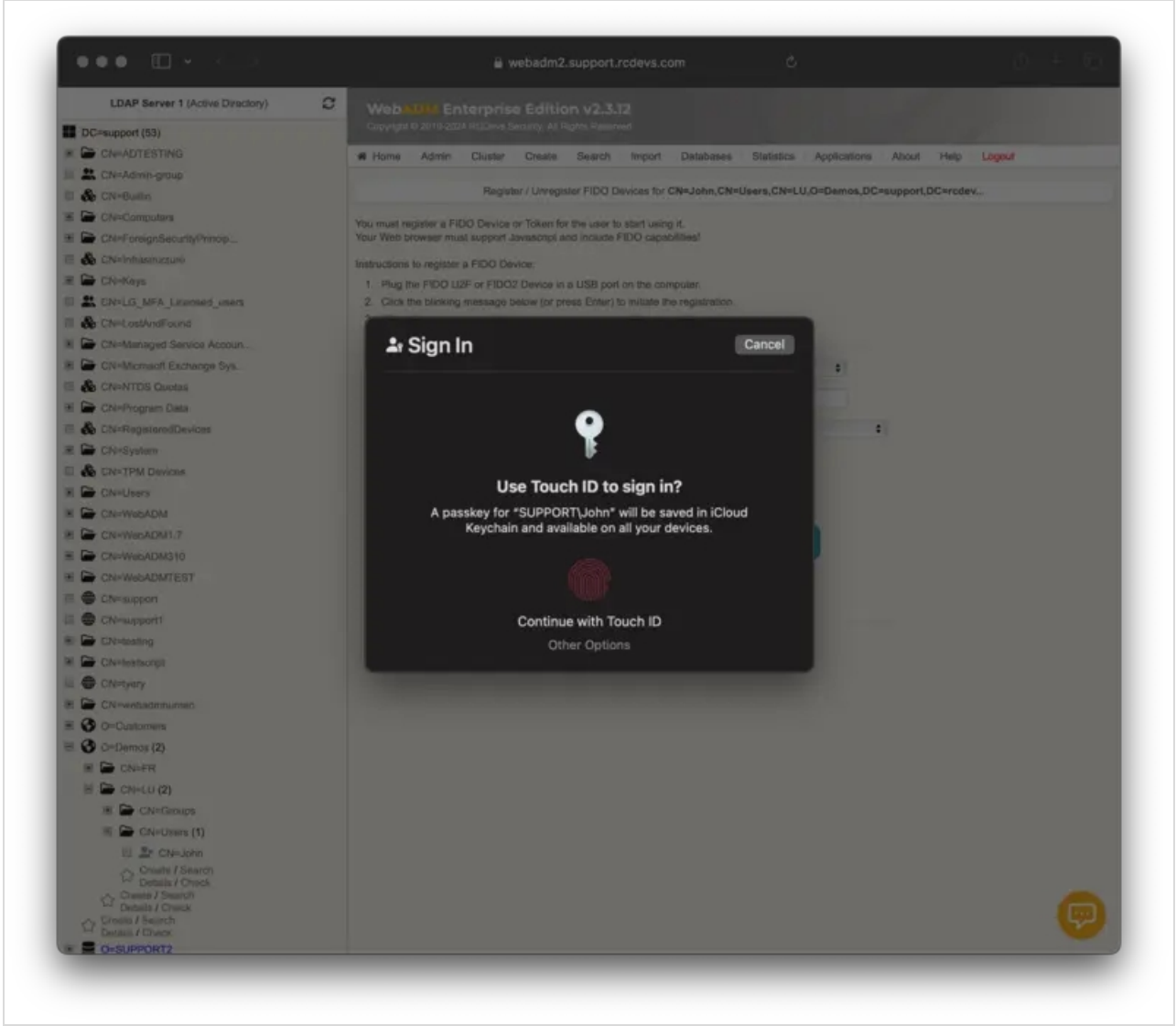

The FIDO/Passkeys registration page is prompted:



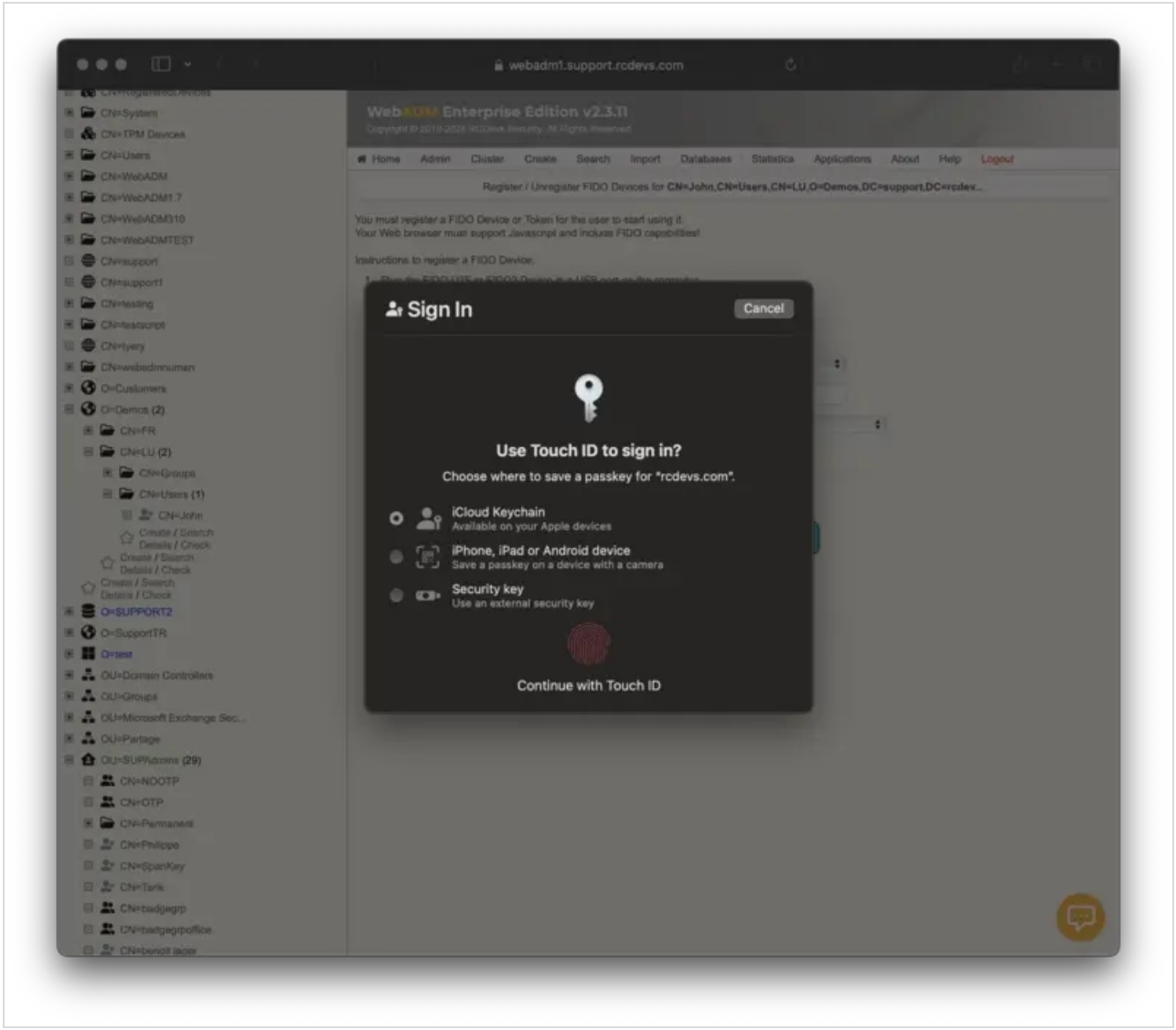

Click on the blinking red message, and you will be prompted to proceed with the enrollment process

## 5.1 From Safari and Apple Devices

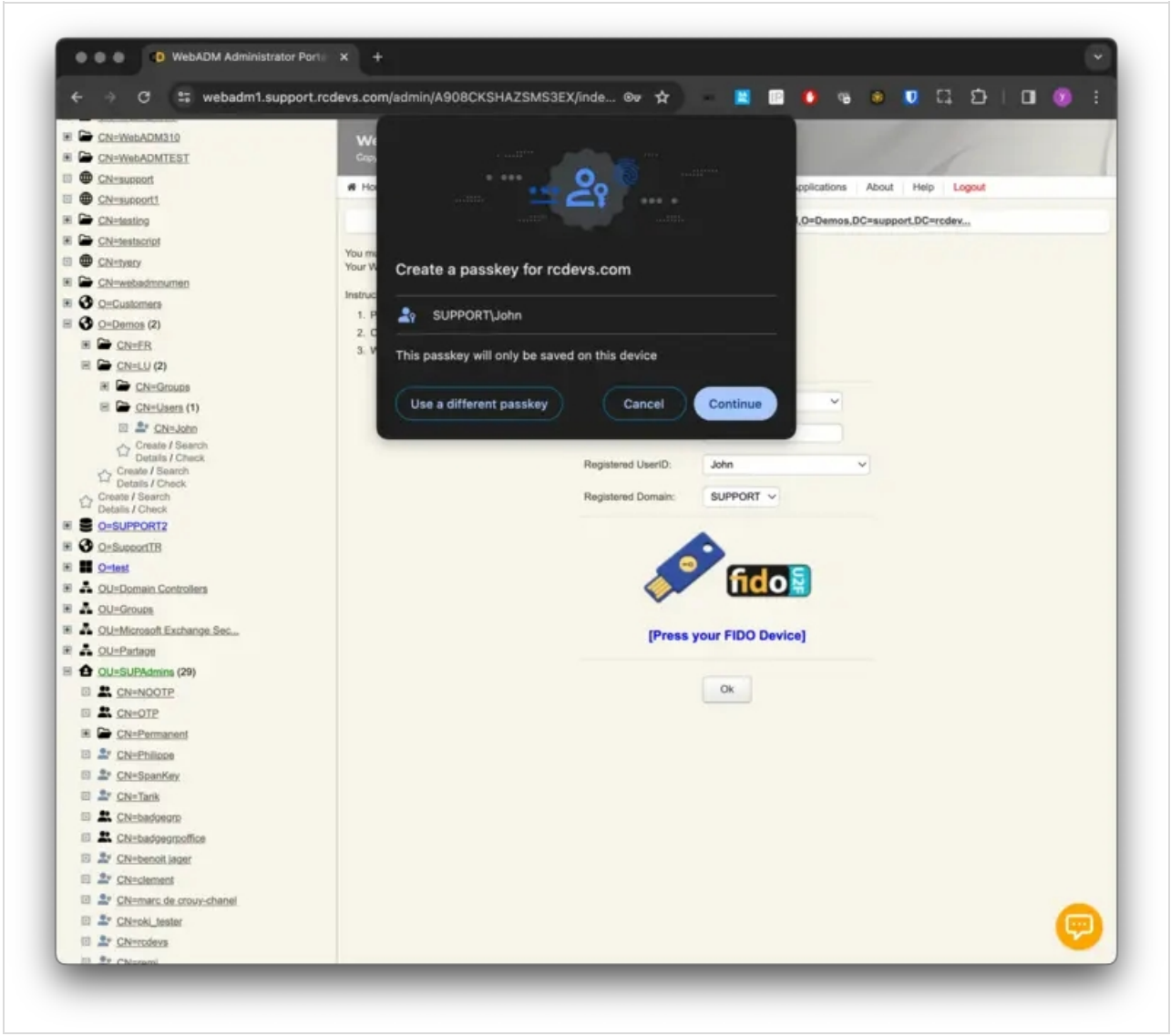
After clicking on the blinking red message, the following appears:



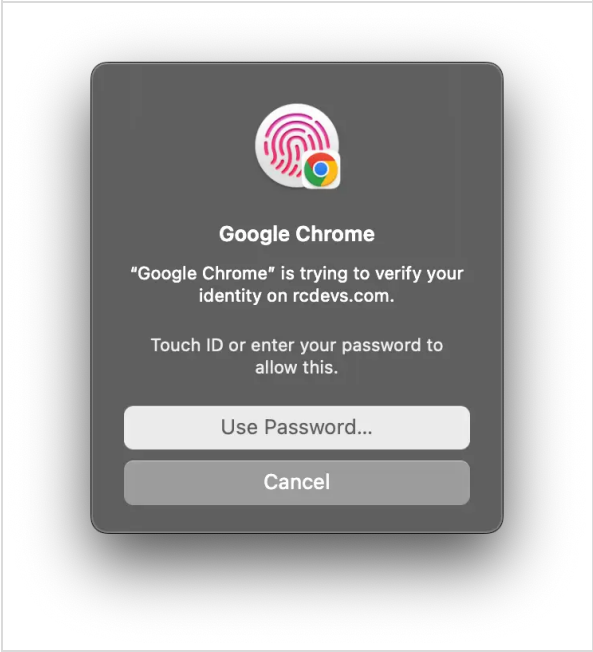

I can directly provide my fingerprint for enrollment, and the passkey will be stored in my iCloud Keychain. If I click on the “Other Options” button, I have the following possibilities that we explained before:



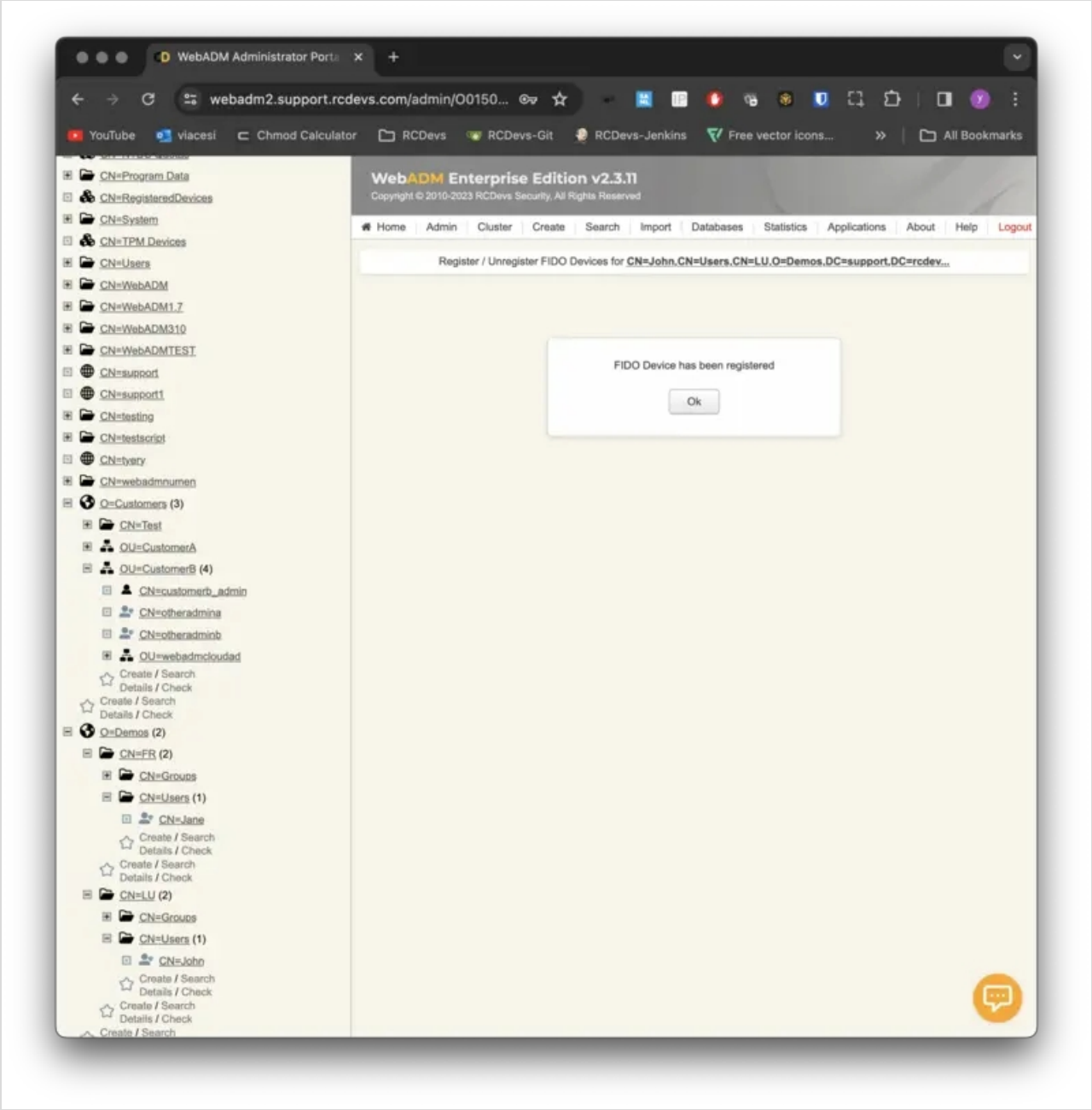

5.2 Passkey stored on local device (TPM used)




If I click `Continue` button, it is going to register my MacOS device as a Passkey:

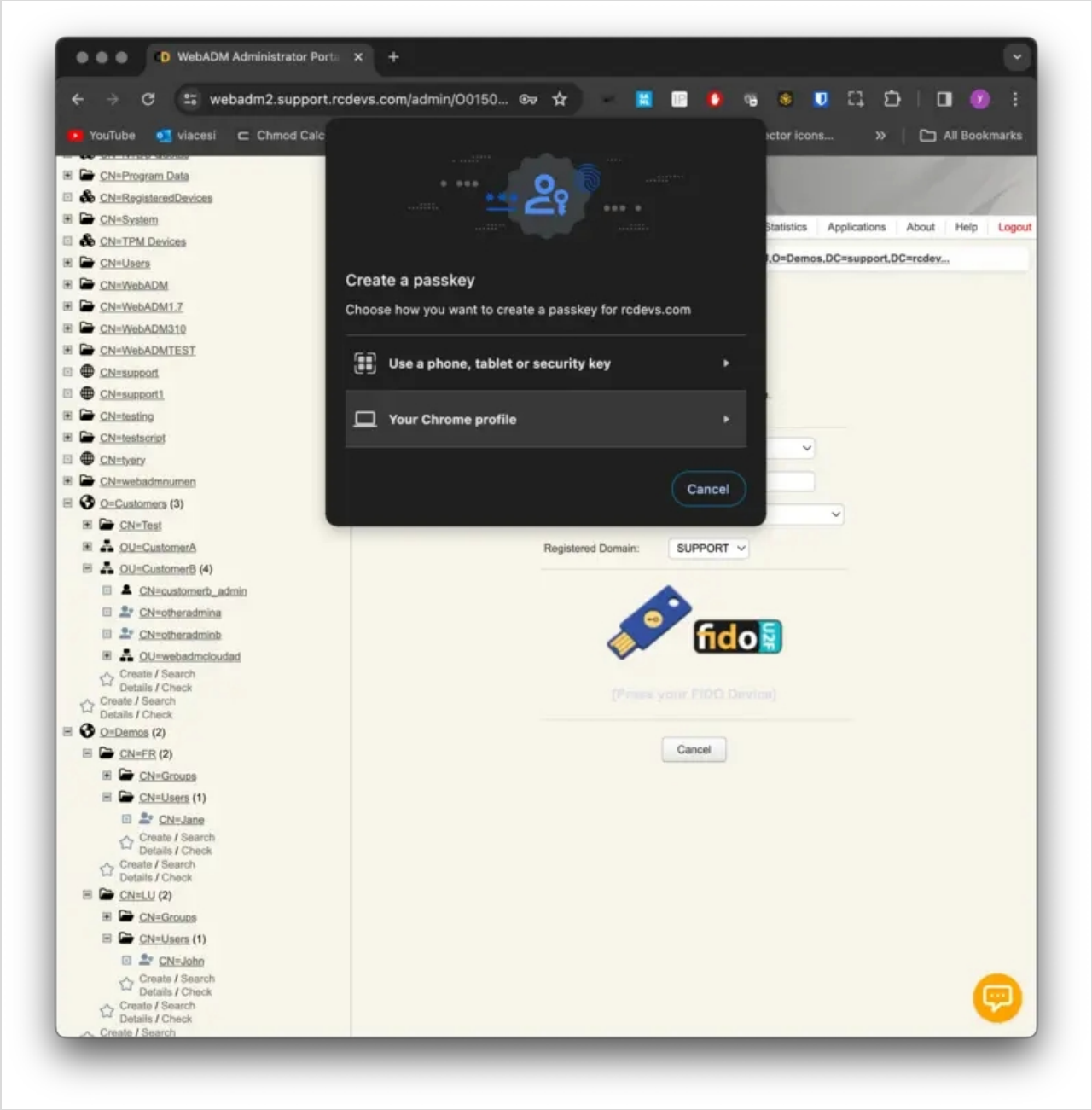



I am invited to provide my fingerprint to finish the enrollment and then my Macbook is registered.



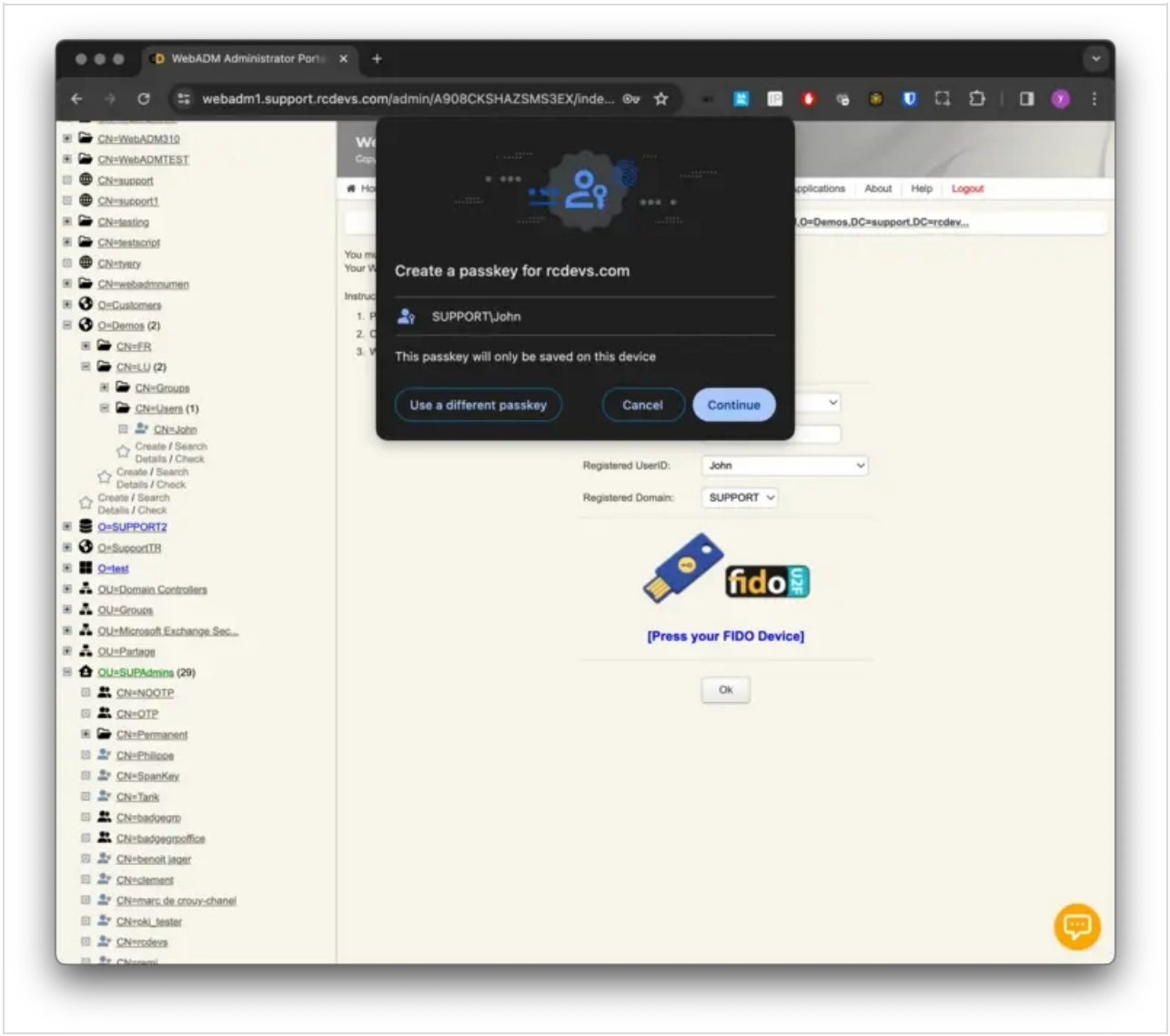

## 5.3 Passkey stored in Chrome Profile

If on the previous screen, I click `Use a different passkey`, then I would have the following behavior:




Here, I have the choice to register my Chrome profile as a Passkey or another device.

If I choose my Chrome profile I would have the following behavior:

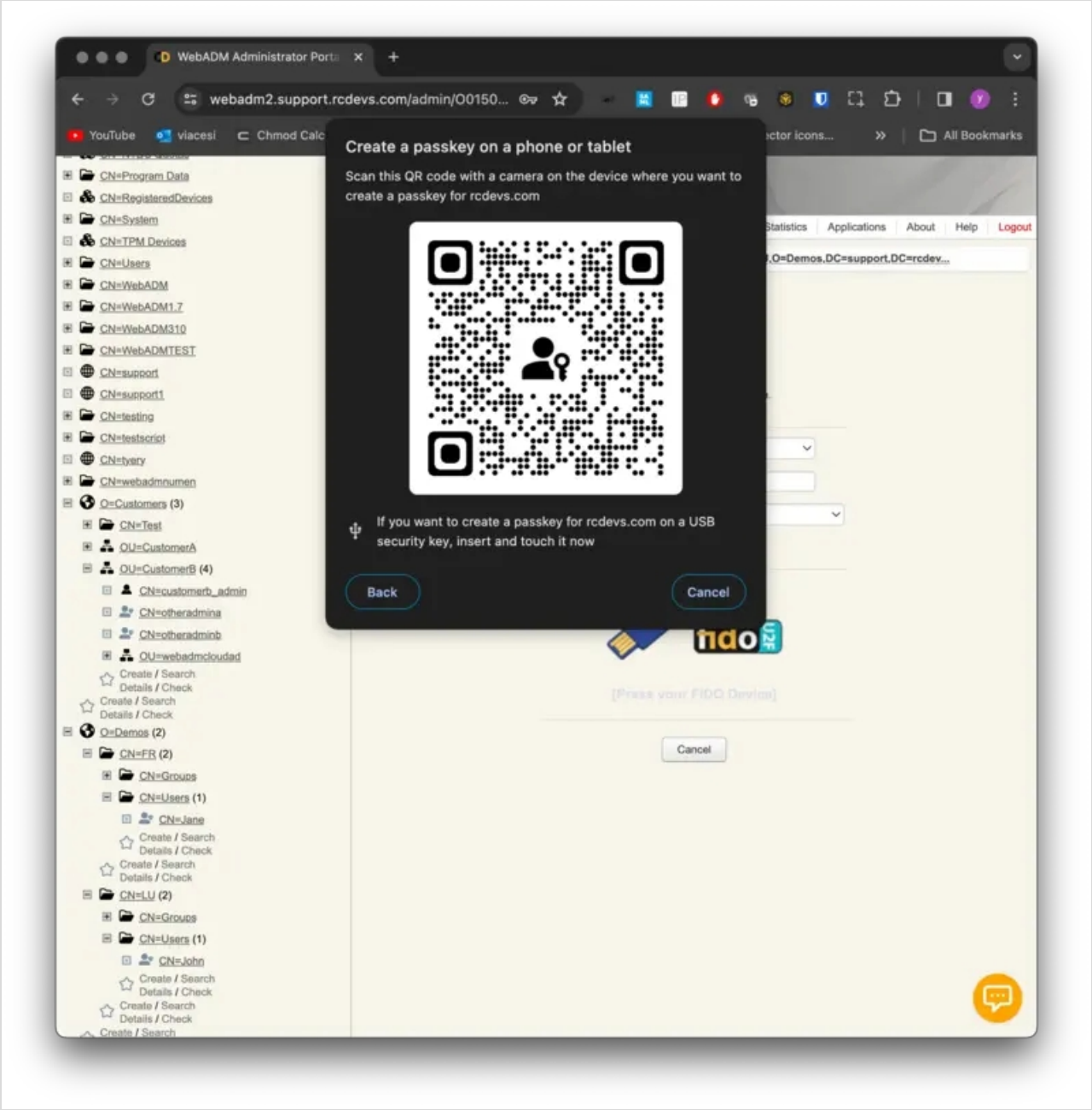



Click on `Continue` button and you are invited to provide your Fingerprint. Your passkey is registered.

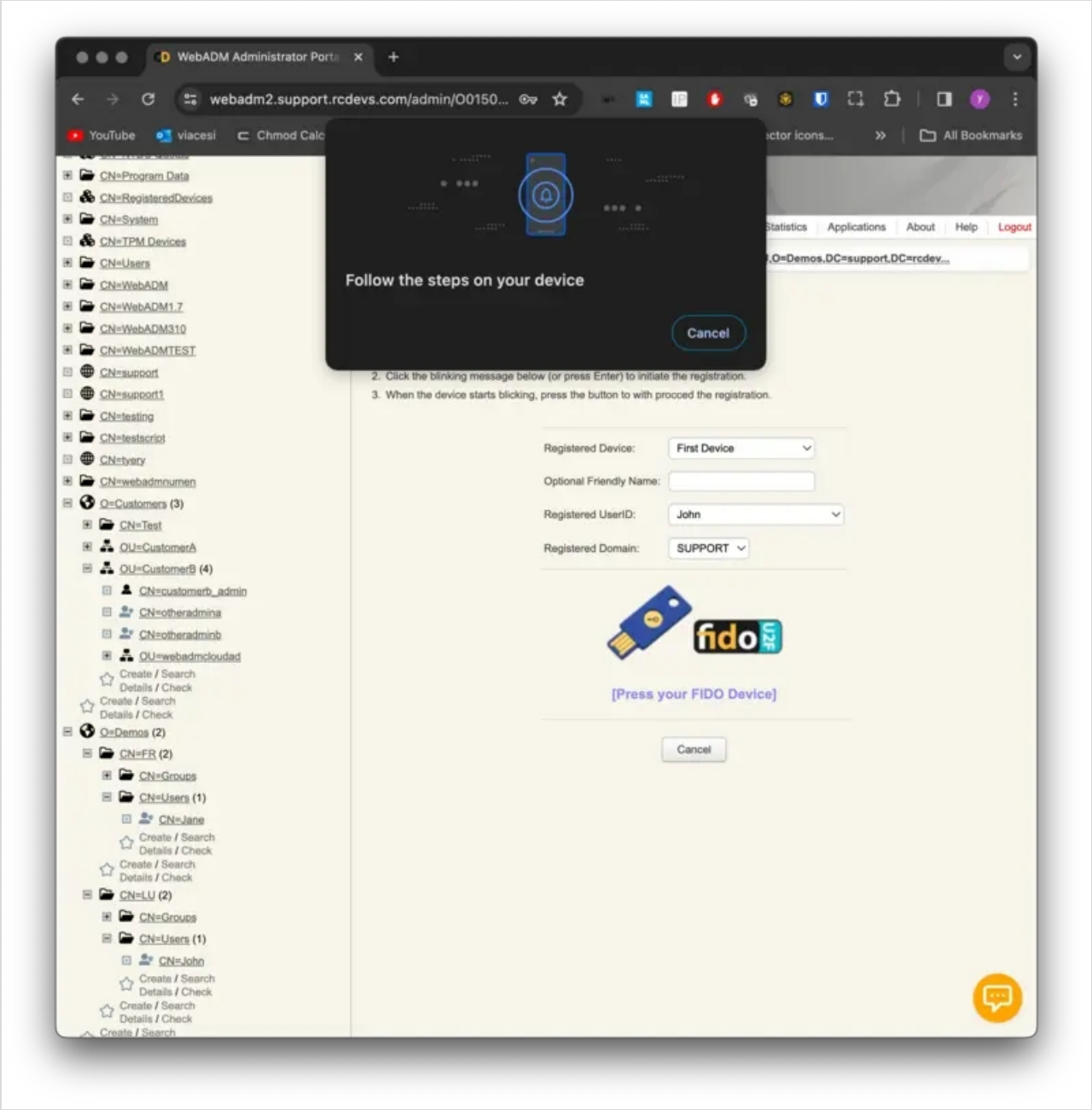
## 5.4 Passkey from a device with a camera

### 5.4.1 iOS device

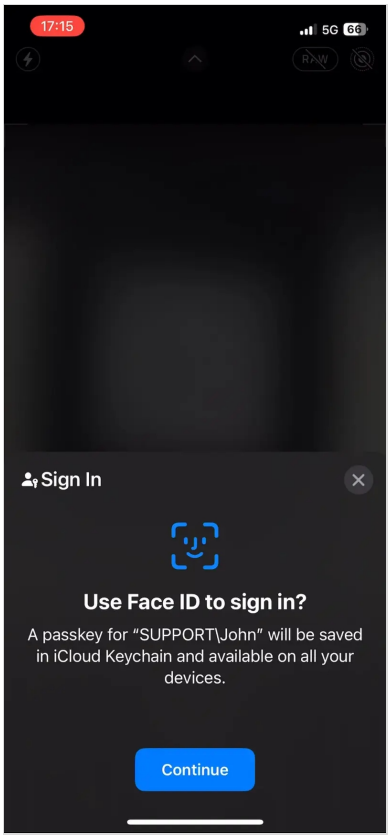
The last option is through the `Use a phone, tablet or security key` method. Click on it and then the following is prompted:



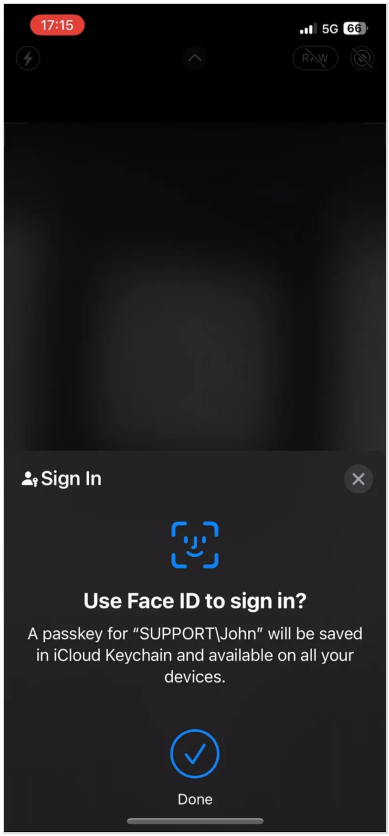

I’m going to use my iPhone to scan it. Open your camera, scan the QRCode, and click on the link once the QRCode has been parsed by your phone. Once you have scanned the QRCode, the following message will appear on your web browser page:




On the mobile side, you have the following screens after cliking the link provided through the QRCode:



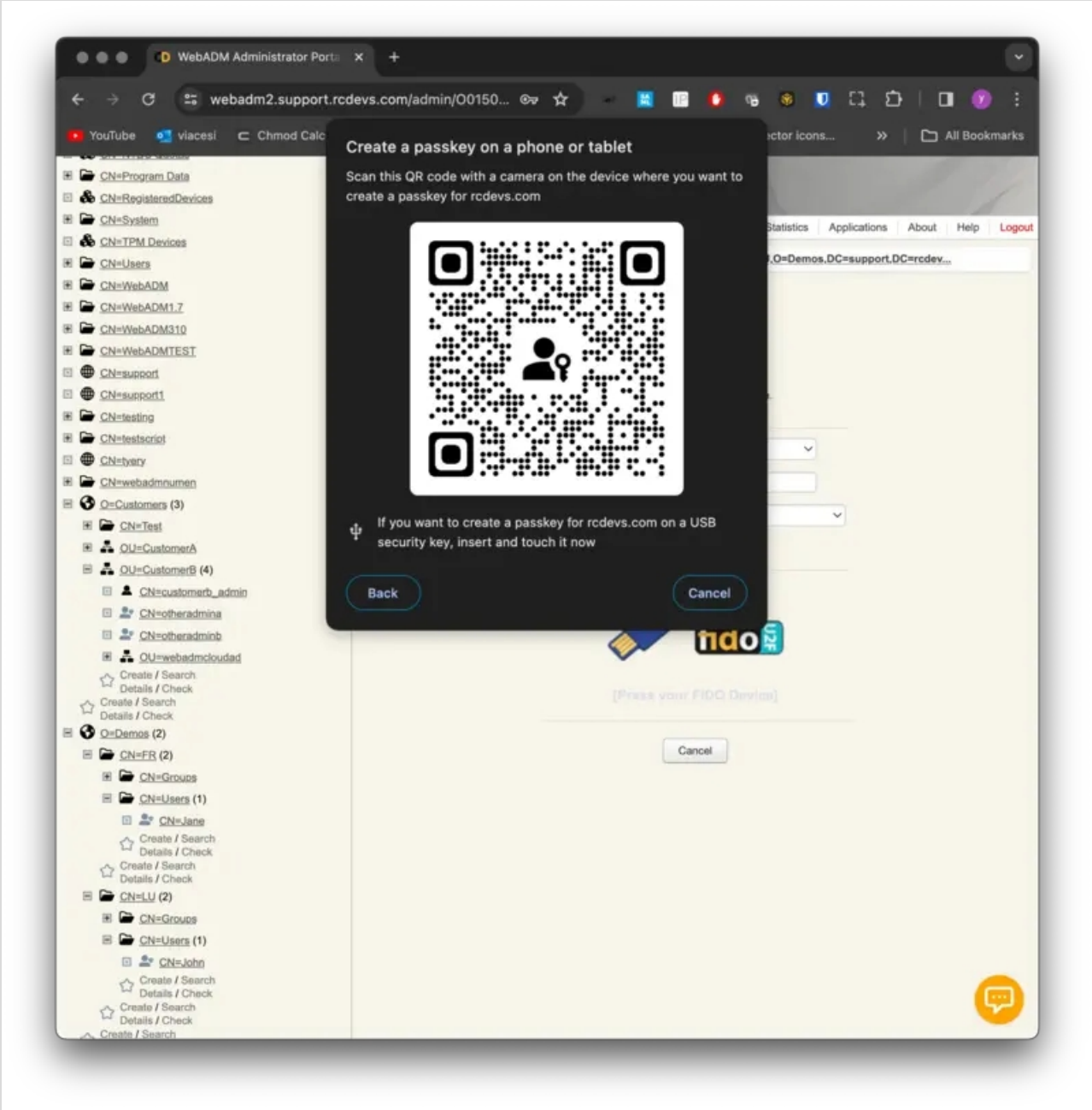

Click `Continue` button and you are invited to provide your FaceID:



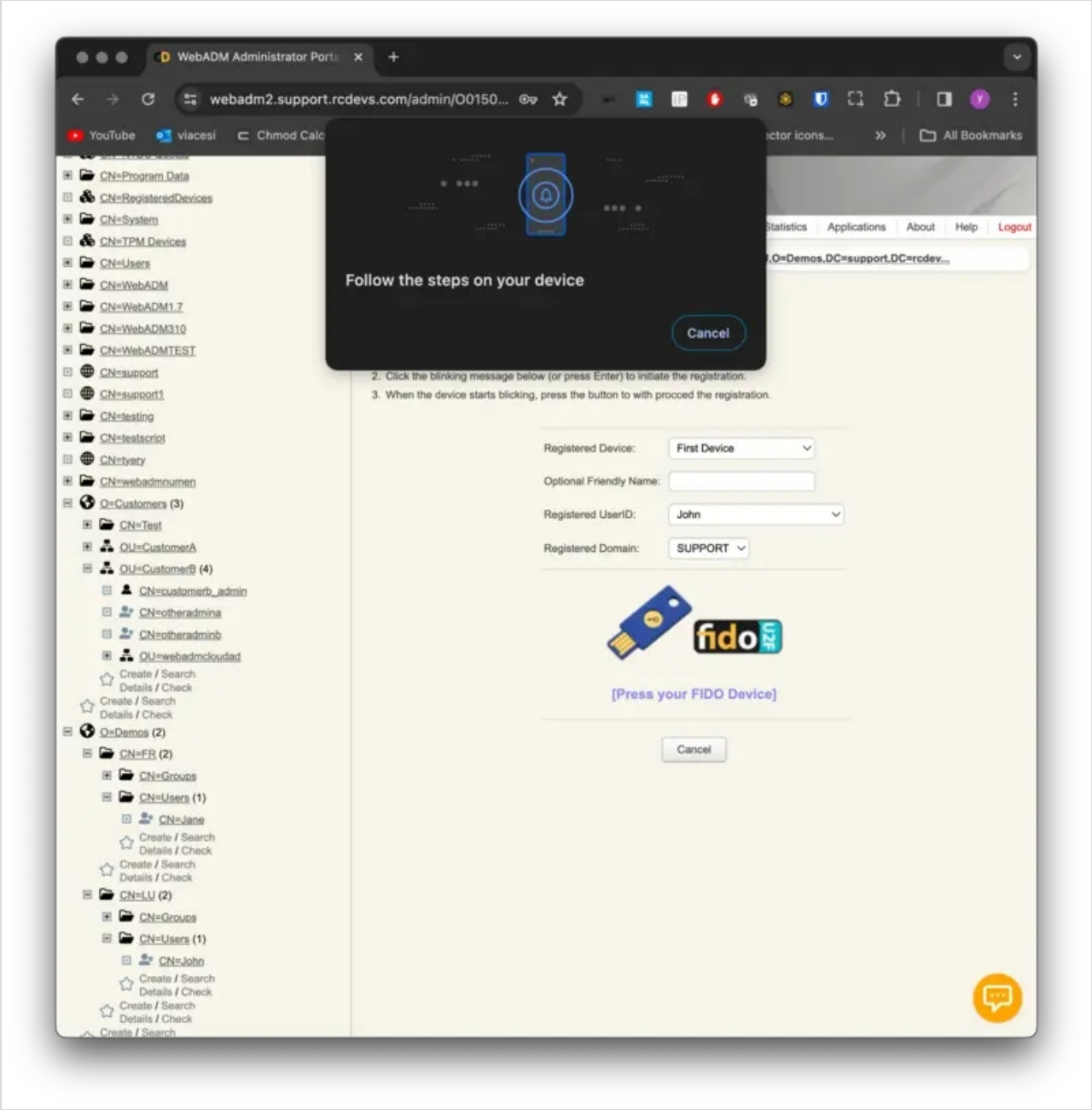

Once FaceID has been validated on your phone, then the enrollment should be done on WebADM side. You will be invited to use your enrolled Passkey during authentication with OpenOTP.

### 5.4.2 Android device

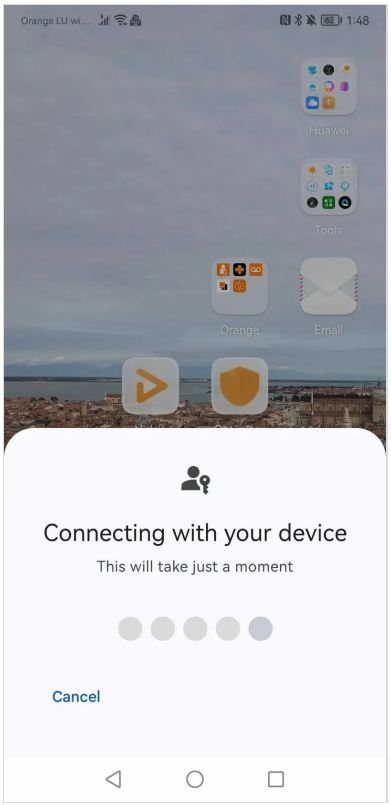
The last option is through the `Use a phone, tablet or security key` method. Click on it and then the following is prompted:



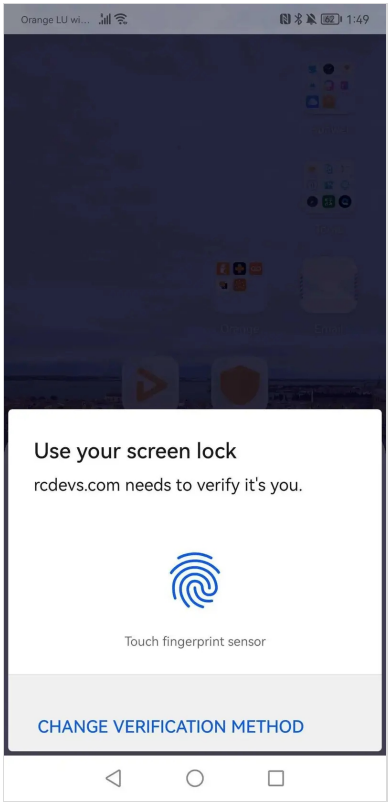

I'm going to use my Android phone to scan it. Open your camera, scan the QRCode and click on the link once the QRCode has been parsed by your phone. Once you scanned the QRCode, on your web browser page, the following message appears:



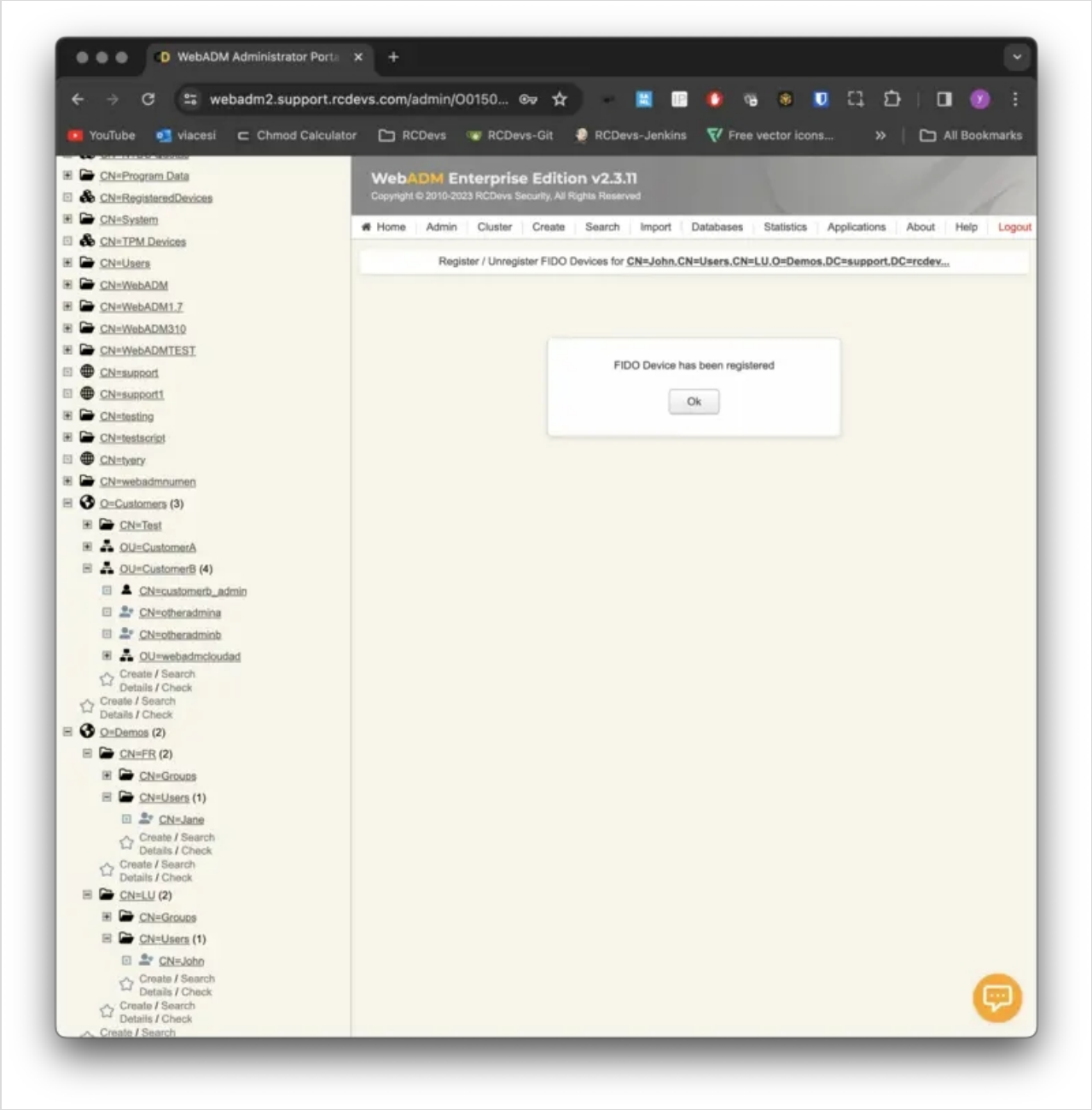

On the mobile side, you have the following screen for a second after cliking the link:




You are then invited to provide your fingerprint or passcode. Here we provided the fingerprint.

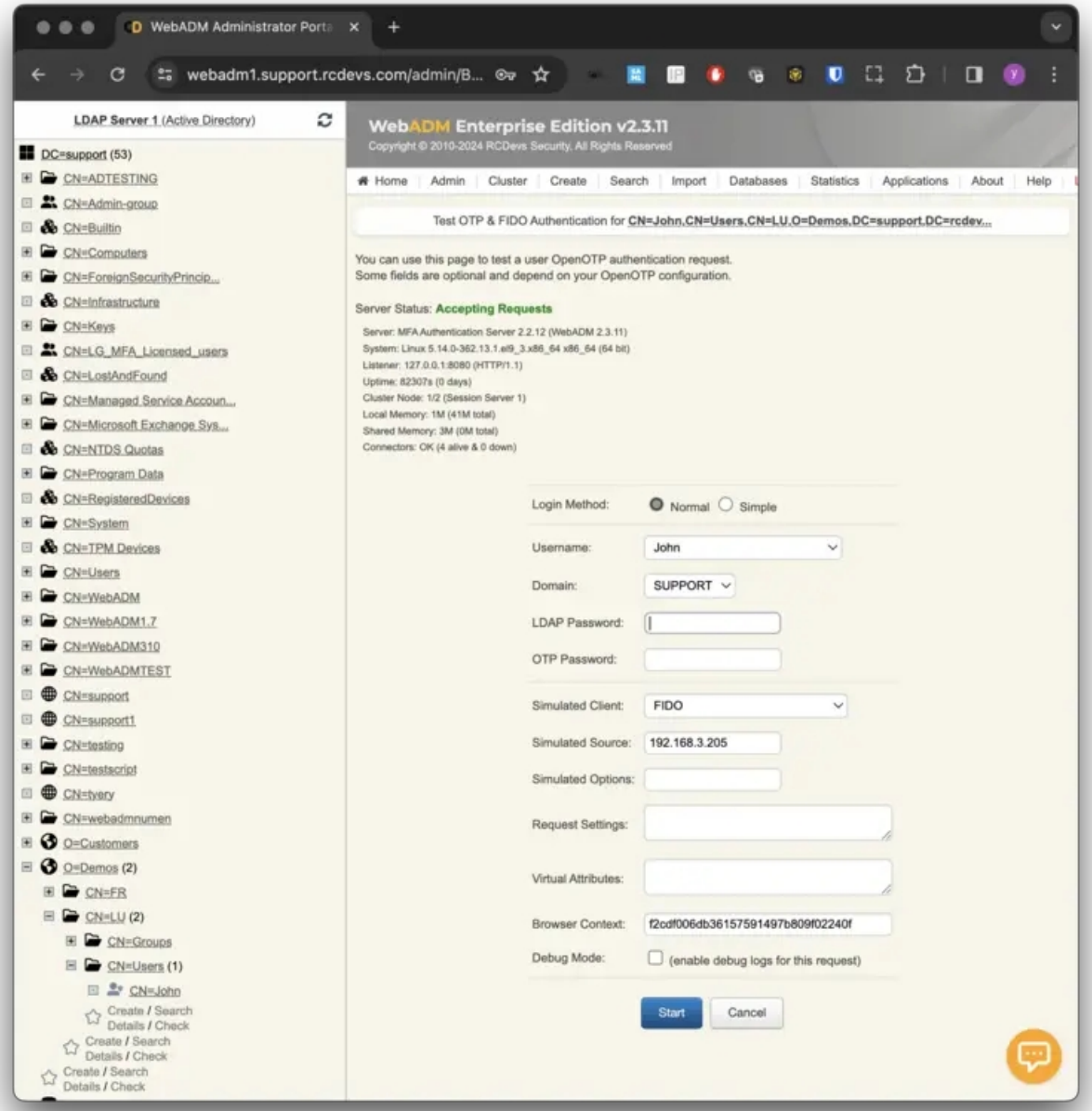


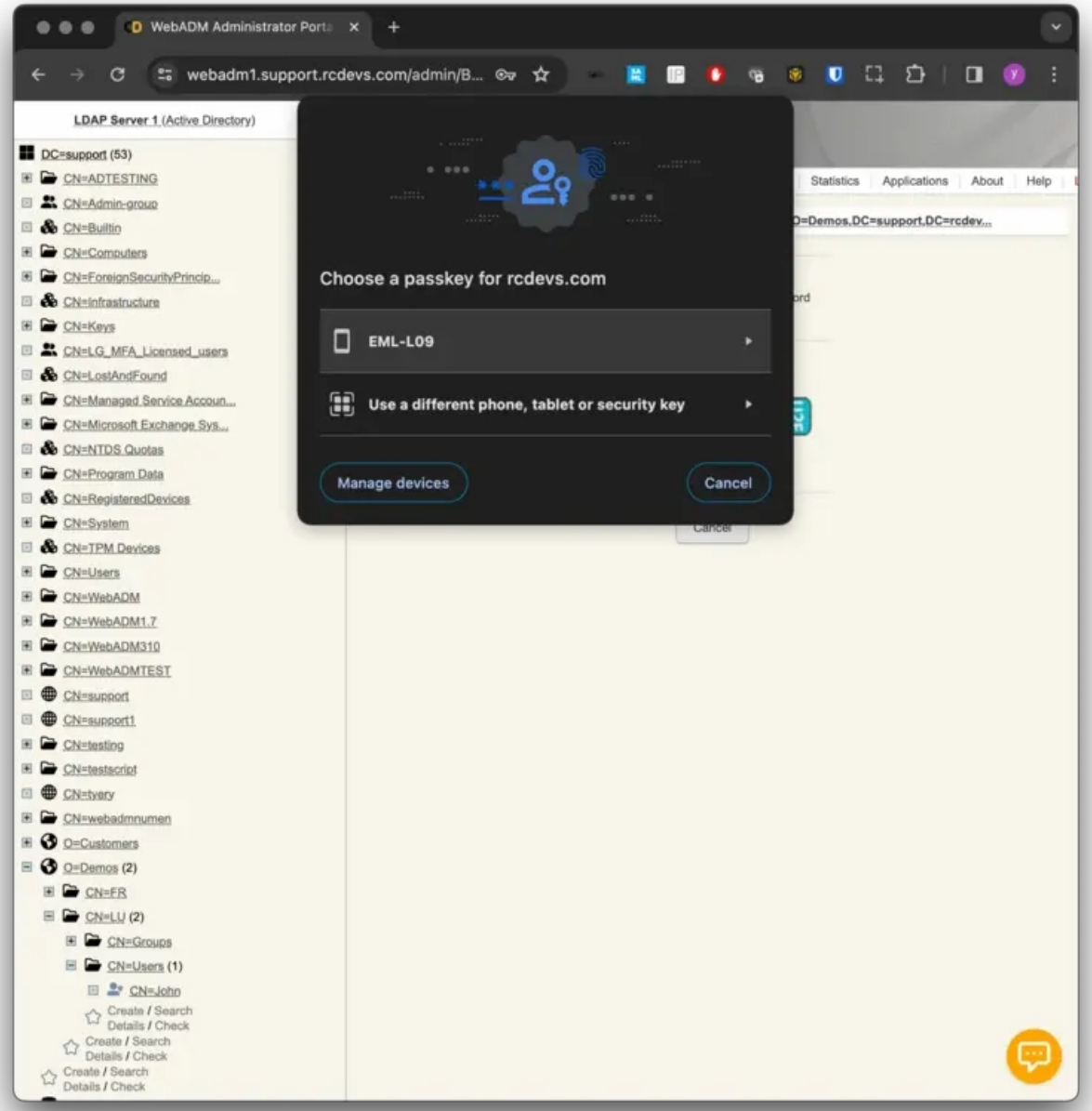

The enrollment is completed.

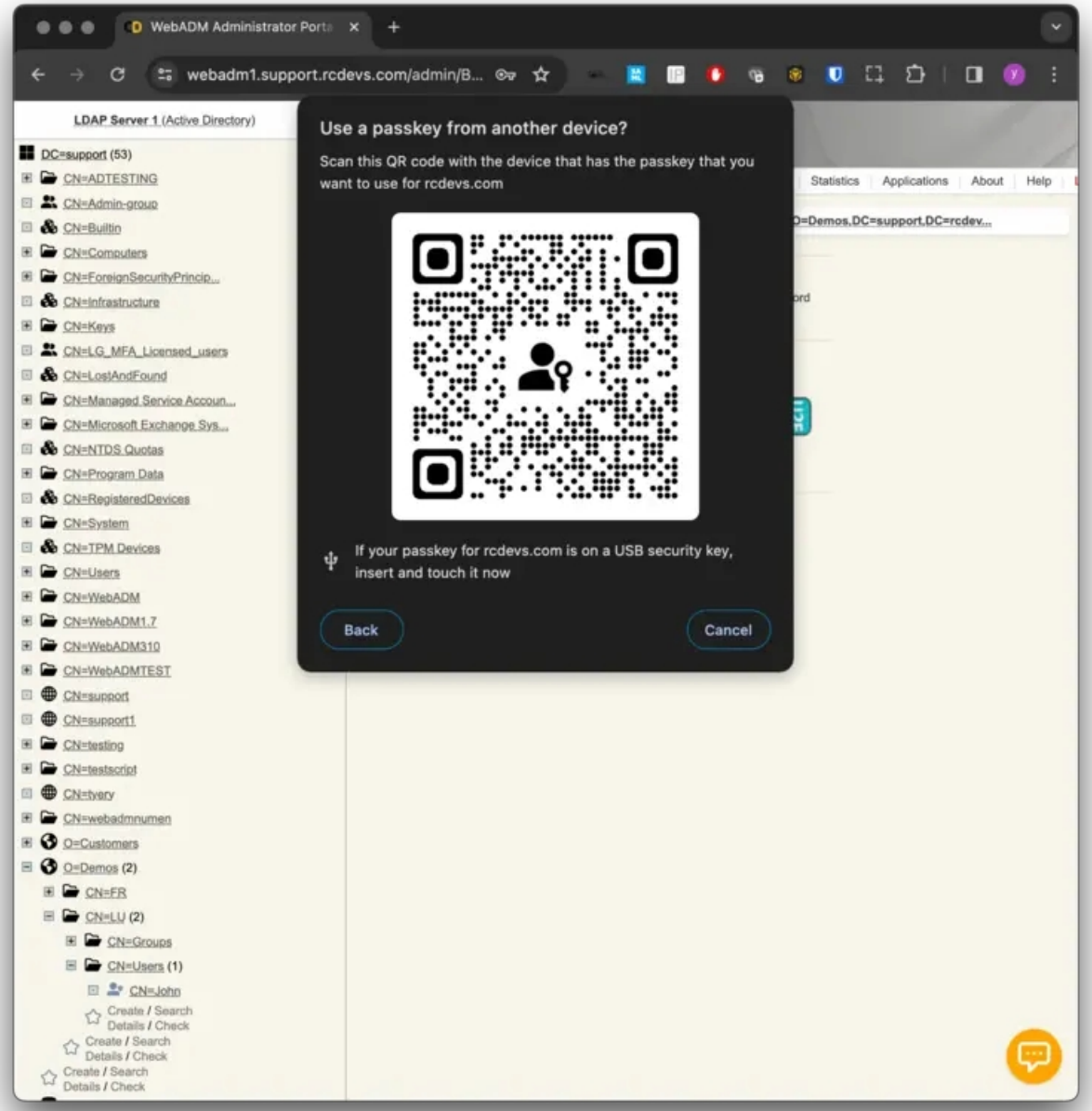


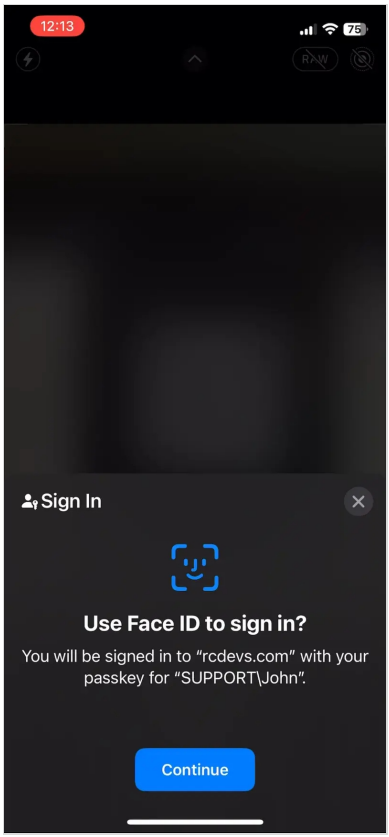

## 6 Login Test and logs

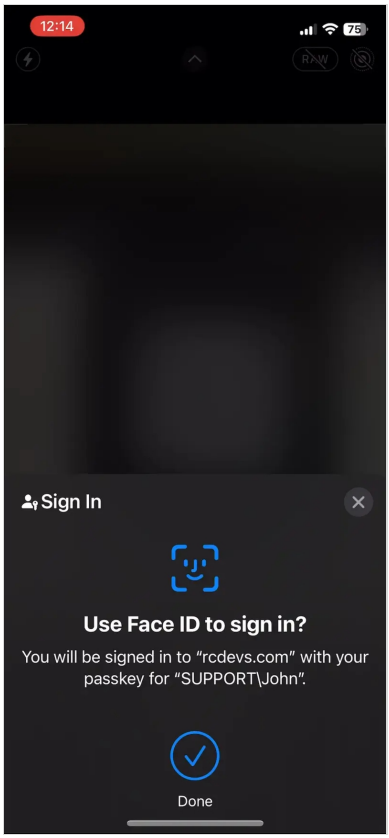
Once your security key or passkey is registered on your account, you can test it through the WebADM admin GUI or all other Web Application through the login tester functionality. Click on your User account in the LDAP tree > `Application Actions` > `MFA Authentication` > `Test OTP & FIDO authentication`. To test the FIDO logins from WebADM, the `Login Mode` setting of OpenOTP must be configured to `LDAPMFA` or `LDAPU2F` or `U2F` or `MFA`. Have a look on OpenOTP configuration or create a user group or client policy to meet that requirement.

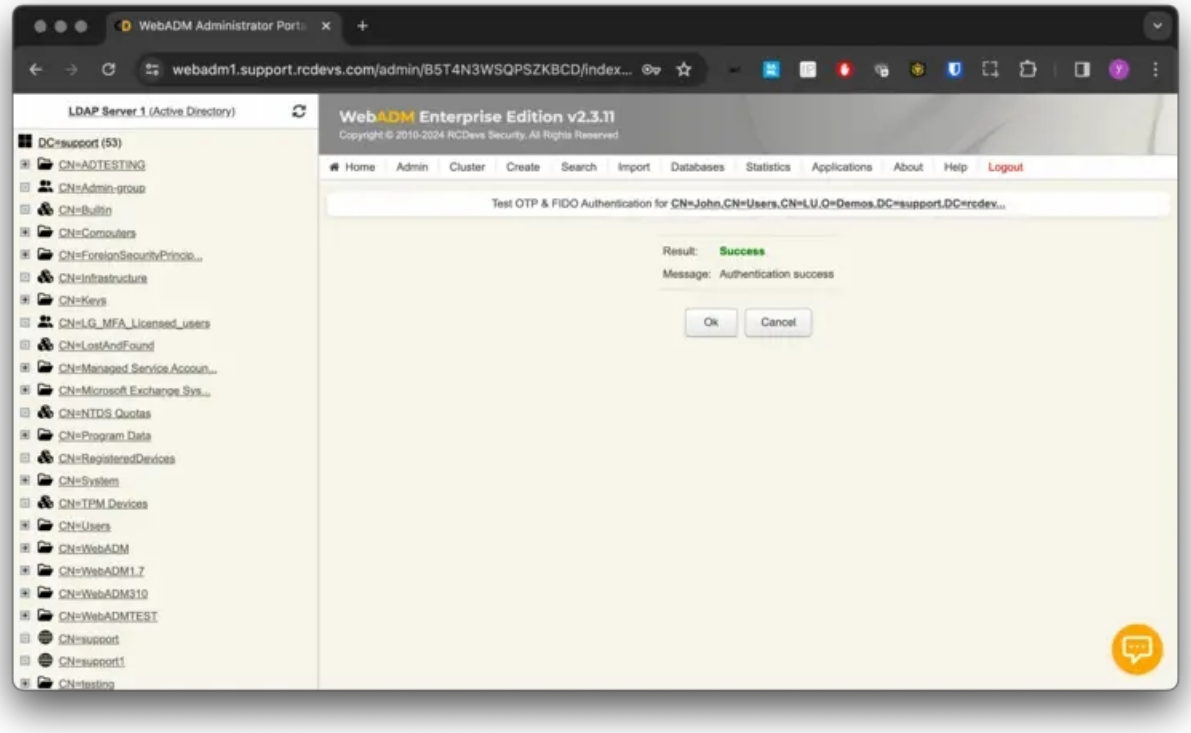

WebADM Administrator Porta
webadm1.support.rcdevs.com/admin/B...
LDAP Server 1 (Active Directory)
DC=support (53)
CN=ADTESTING
CN=Admin-group
CN=Builtin
CN=Computers
CN=ForeignSecurityPrincip...
CN=Infrastructure
CN=Keys
CN=LG_MFA_Licensed_users
CN=LostAndFound
CN=Managed Service Accoun...
CN=Microsoft Exchange Sys...
CN=NTDS Quotas
CN=Program Data
CN=RegisteredDevices
CN=System
CN=TPM Devices
CN=Users
CN=WebADM
CN=WebADM1.7
CN=WebADM310
CN=WebADMTEST
CN=support
CN=support1
CN=testing
CN=testscript
CN=tyery
CN=webadmnumen
O=Customers
O=Demos (2)
CN=FR
CN=LU (2)
CN=Groups
CN=Users (1)
CN=John
Create / Search
Details / Check
Create / Search
Details / Check
Create / Search
Details / Check
WebADM Enterprise Edition v2.3.11
Copyright © 2010-2024 RCDevs Security, All Rights Reserved
Home
Admin
Cluster
Create
Search
Import
Databases
Statistics
Applications
About
Help
Test OTP & FIDO Authentication for CN=John,CN=Users,CN=LU,O=Demos,DC=support,DC=rcdev...
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 2.2.12 (WebADM 2.3.11)
System: Linux 5.14.0-362.13.1.el9_3.x86_64 x86_64 (64 bit)
Listener: 127.0.0.1:8080 (HTTP/1.1)
Uptime: 82307s (0 days)
Cluster Node: 1/2 (Session Server 1)
Local Memory: 1M (41M total)
Shared Memory: 3M (0M total)
Connectors: OK (4 alive & 0 down)
Login Method:
Normal
Simple
Username:
John
Domain:
SUPPORT
LDAP Password:
OTP Password:
Simulated Client:
FIDO
Simulated Source:
192.168.3.205
Simulated Options:
Request Settings:
Virtual Attributes:
Browser Context:
f2cdf006db36157591497b809f02240f
Debug Mode:
(enable debug logs for this request)
Start
Cancel


WebADM Administrator Porta
webadm1.support.rcdevs.com/admin/B...
LDAP Server 1 (Active Directory)
DC=support (53)
CN=ADTESTING
CN=Admin-group
CN=Builtin
CN=Computers
CN=ForeignSecurityPrincip...
CN=Infrastructure
CN=Keys
CN=LG_MFA_Licensed_users
CN=LostAndFound
CN=Managed Service Accoun...
CN=Microsoft Exchange Sys...
CN=NTDS Quotas
CN=Program Data
CN=RegisteredDevices
CN=System
CN=TPM Devices
CN=Users
CN=WebADM
CN=WebADM1.7
CN=WebADM310
CN=WebADMTEST
CN=support
CN=support1
CN=testing
CN=testscript
CN=tvery
CN=webadmnumen
O=Customers
O=Demos (2)
CN=FR
CN=LU (2)
CN=Groups
CN=Users (1)
CN=John
Create / Search
Details / Check
Statistics
Applications
About
Help
Choose a passkey for rcdevs.com
EML-L09
Use a different phone, tablet or security key
Manage devices
Cancel


WebADM Administrator Porta
webadm1.support.rcdevs.com/admin/B...
LDAP Server 1 (Active Directory)
DC=support (53)
CN=ADTESTING
CN=Admin-group
CN=Builtin
CN=Computers
CN=ForeignSecurityPrincip...
CN=Infrastructure
CN=Keys
CN=LG_MFA_Licensed_users
CN=LostAndFound
CN=Managed Service Accoun...
CN=Microsoft Exchange Sys...
CN=NTDS Quotas
CN=Program Data
CN=RegisteredDevices
CN=System
CN=TPM Devices
CN=Users
CN=WebADM
CN=WebADM1.7
CN=WebADM310
CN=WebADMTEST
CN=support
CN=support1
CN=testing
CN=testscript
CN=tvery
CN=webadmnumen
O=Customers
O=Demos (2)
CN=FR
CN=LU (2)
CN=Groups
CN=Users (1)
CN=John
Create / Search
Details / Check
Create / Search
Details / Check
Create / Search
Details / Check
Use a passkey from another device?
Scan this QR code with the device that has the passkey that you want to use for rcdevs.com
If your passkey for rcdevs.com is on a USB security key, insert and touch it now
Back
Cancel
Statistics
Applications
About
Help
O=Demos,DC=support,DC=rcdev...


12:13
Sign In
Use Face ID to sign in?
You will be signed in to "rcdevs.com" with your passkey for "SUPPORT\John".
Continue


12:14
Sign In
Use Face ID to sign in?
You will be signed in to "rcdevs.com" with your passkey for "SUPPORT\John".
Done


WebADM Administrator Porta
webadm1.support.rcdevs.com/admin/B5T4N3WSQPSZKBCD/index...
LDAP Server 1 (Active Directory)
DC=support (53)
CN=ADTESTING
CN=Admin-group
CN=Builtin
CN=Computers
CN=ForeignSecurityPrincip...
CN=Infrastructure
CN=Keys
CN=LG_MFA_Licensed_users
CN=LostAndFound
CN=Managed Service Accoun...
CN=Microsoft Exchange Sys...
CN=NTDS Quotas
CN=Program Data
CN=RegisteredDevices
CN=System
CN=TPM Devices
CN=Users
CN=WebADM
CN=WebADM1.7
CN=WebADM310
CN=WebADMTEST
CN=support
CN=support1
CN=testing
WebADM Enterprise Edition v2.3.11
Copyright © 2010-2024 RCDevs Security. All Rights Reserved
Home
Admin
Cluster
Create
Search
Import
Databases
Statistics
Applications
About
Help
Logout
Test OTP & FIDO Authentication for CN=John,CN=Users,CN=LU,O=Demos,DC=support,DC=rcdev...
Result: Success
Message: Authentication success
Ok
Cancel

```
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] New openotpNormalLogin SOAP request
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] > Username: John
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] > Domain: SUPPORT
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] > Client ID: FIDO
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] > Source IP: 192.168.3.205
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] > Context ID:
2a90ff648866f895d11503b02567a598
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Enforcing client policy: FIDO (matched
client ID)
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Registered openotpNormalLogin request
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Resolved LDAP user:
CN=John,CN=Users,CN=LU,O=Demos,DC=support,DC=rcdevs,DC=com (cached with route #00)
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] New openotpNormalLogin request
(SUPPORT\John)
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Started transaction lock for user
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Found 1 user emails: yoann@rcdevs.com
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Found 50 user settings:
LoginMode=U2F,OTPType=TOKEN,PushLogin=Yes,PushVoice=No,MaxTries=3,MaxPwned=0,BlockNotify=MA
1:HOTP-SHA1-6:QN06-
T1M,U2FPINMode=Discouraged,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,PrefetchExp

[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Found 4 user data:
Device1Type,Device1Name,Device1Data,Device1State
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Found 1 registered FIDO device
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Requested login factors: U2F
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Authentication challenge required
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] U2F authentication challenge (valid 90
seconds)
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Started U2F authentication session of ID
GWKc6Uom0FO8u7e5 valid for 90 seconds
[2024-01-10 12:13:50] [127.0.0.1:48316] [OpenOTP:Q2UIUHZS] Sent login challenge response
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] New openotpChallenge SOAP request
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] > Username: John
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] > Domain: SUPPORT
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] > Session: GWKc6Uom0FO8u7e5
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] > U2F Response: 585 Bytes
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] Found authentication session started
2024-01-10 12:13:50
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] New openotpChallenge request
(SUPPORT\John)
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] Started transaction lock for user
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] FIDO response Ok (device #1)
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] Updated user data
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] Authentication success (FIDO #1)
[2024-01-10 12:14:03] [127.0.0.1:44528] [OpenOTP:Q2UIUHZS] Sent login success response
[2024-01-10 12:15:45] [127.0.0.1:37308] [OpenOTP:5KLR71UI] New openotpStatus SOAP request
[2024-01-10 12:15:45] [127.0.0.1:37308] [OpenOTP:5KLR71UI] Sent status response (Ok)
```