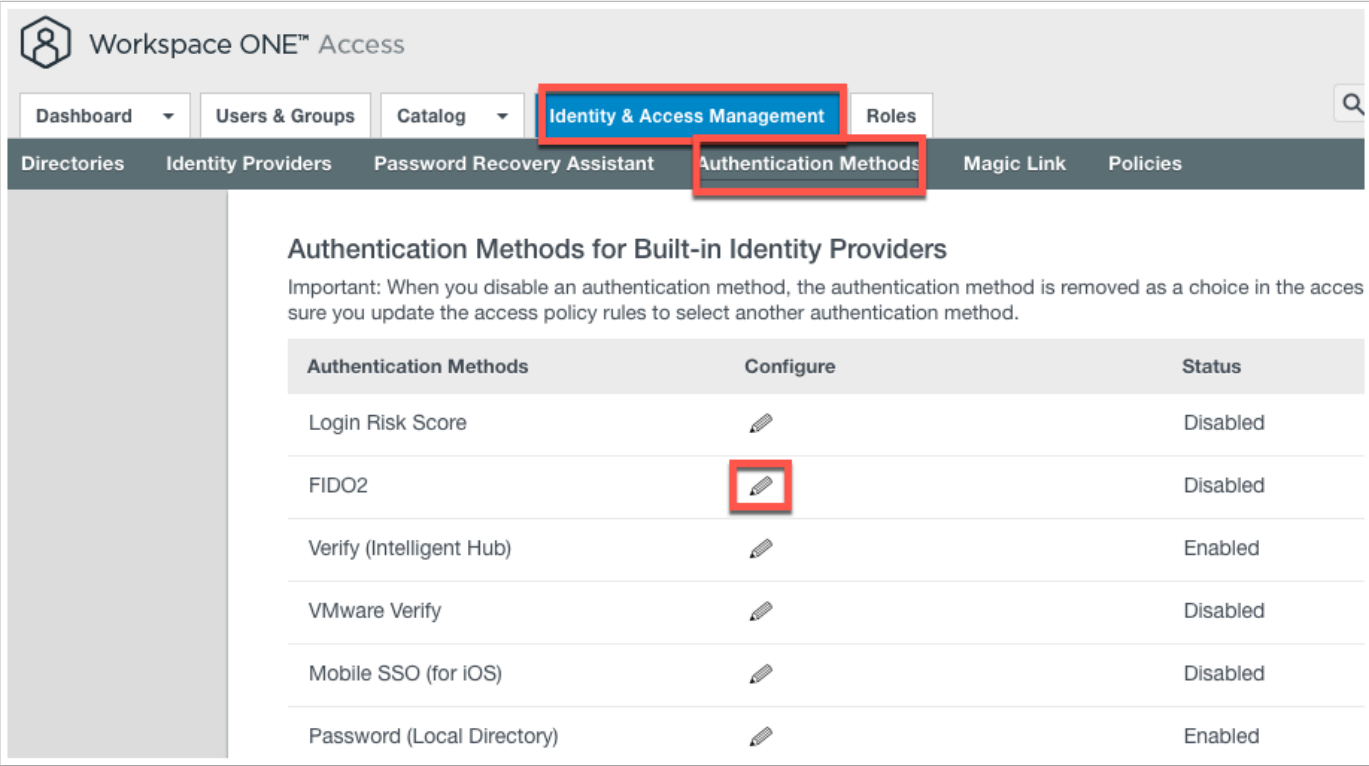


# (BETA)FIDO2 Configuration in Access (MacOS)

This lab is designed to help you understand how to setup and authenticate using FIDO2 (Fast Identity Online). You will discover the requirements and implement the solution into your existing Workspace ONE Access environment.

- Part 1: Setup FIDO2
- Part 2: Register Authenticator
- Part 3: Administer FIDO2 Keys

## Part 1: Setup FIDO2



- Log into your WorkspaceONE Access tenant as the system administrator.
  - Navigate to **Identity & Access Management** > **Authentication Methods** click the **pencil** icon next to **FIDO2**.

**FIDO2**

**Enable FIDO2 Adapter** ☒   
 Enable user login using FIDO2 Adapter

**Enable Registration During Login** ☒   
 Enable user registration during login using FIDO2 Adapter

**Authentication Timeout in Seconds\***    
 Time in seconds the user has to authenticate before the session times out

**Registration Timeout in Seconds\***    
 Time in seconds the user has to register before the session times out

**Max Authentication Attempts\***    
 Max Authentication Attempts

**User Verification Preference\***    
 User verification requirement for credential creation

**Authenticator Type Preference\***    
 Authenticators' attachment modalities

**Attestation Conveyance Preference\***    
 Specify preference regarding attestation conveyance during credential generation. Attestation "none" is not recommended from a security standpoint.

[Cancel](#) [Save](#)

## 2. Click **Enable FIDO2 Adapter**

- Set the User Verification Preference to **required**
- Set the Attestation Conveyance Preference to **none**
- click **Save** at the bottom of the page.

Workspace ONE™ Access Tenant Admin ▾ AW-HI

Dashboard ▾ Users & Groups Catalog ▾ **Identity & Access Management** Roles

Directories **Identity Providers** Password Recovery Assistant Authentication Methods Magic Link Policies

Identity Providers (4) [Add Identity Provider](#)

Identity Provi...	Auth Methods	Directory	Network Ran...	Connector(s)	Type	Status
<a href="#">System Identity Provider</a>	Password (Local Directory)	System Directory	ALL RANGES		Built-in	Enabled
<b><a href="#">Built-in</a></b>	Verify (Intelligent Hub) Certificate (cloud deployment) Password (cloud deployment)	LivefireSync	ALL RANGES	ws1-connector.euc-livfire.com	Built-in	Enabled
<a href="#">Workspacel..._3666</a>	Password	LivefireSync	ALL RANGES	ws1-connector.euc-livfire.com	Workspace ONE Access	Enabled
<a href="#">Auth0</a>	Auth0	Auth0-Directory	ALL RANGES		OpenID Connect	Enabled

## 3. Navigate to **Identity Provider** and click **Built-in**

Authentication Methods	Associate Authentication Method
FIDO2	<input checked="" type="checkbox"/>
Verify (Intelligent Hub)	<input checked="" type="checkbox"/>
Password (Local Directory)	<input type="checkbox"/>
Device Compliance (with Workspace ONE UEM)	<input type="checkbox"/>
Certificate (cloud deployment)	<input checked="" type="checkbox"/>

Connector(s) ☒ ws1-connector (ws1-connector.euc-livefire.com) ✖

**Add a Connector**

You can select additional connectors for high availability (HA). Create the connector activation code from the Add a Connector page and set up the connector, and then select the connector for this IdP.

Important: For high availability, each connector must have the same authentication method configuration.

**Connector Authentication Methods**

Authentication Methods	Associate Authentication Method
Password (cloud deployment)	<input checked="" type="checkbox"/>

**KDC Certificate Export** [Download Certificate](#)

Export the KDC server root certificate for use in a Mobile Device Management profile.

**Save** Cancel

- After the **Authentication Methods** loads on the Built-in IDP screen click to enable the **FIDO2** authentication method.
  - Click **Save** at the bottom of the screen

Dashboard
Users & Groups
Catalog
Identity & Access Management
Roles

Directories
Identity Providers
Password Recovery Assistant
Authentication Methods
Magic Link
Policies

ADD POLICY
EDIT
DELETE
EDIT DEFAULT POLICY
NETWORK RANGES

	Policy Name	Applies to	Rule
<input type="radio"/>	Application Policy	0 Application(s)	1 Rule(s)
<input type="radio"/>	default_access_policy_set	5 Application(s)	3 Rule(s)

- Navigate to **Policies** then click **Edit Default Policy**

Edit Policy

×

1 Definition

2 Configuration

3 Summary

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate
:: ALL RANGES	Web Browser	Certificate (cloud depl...	8 Hour(s) ×
:: ALL RANGES	Workspace ONE App ...	Password (cloud deplo...	2160 Hour(s) ×
:: ALL RANGES	Windows 10	Certificate (cloud depl...	8 Hour(s) ×

+ ADD POLICY RULE

6. Click **Configuration** and click **+ ADD POLICY RULE**

FIGURATION

Add Policy Rule

If a user's network range is \*

ALL RANGES

ⓘ

and the user accessing content from \*

All Device Types

ⓘ

and user belongs to group(s)

🔍 Select Groups...

ⓘ

Rule applies to all users if no group(s) selected.

and user is registering FIDO2 authenticator \*

☒ Yes

ⓘ

Then perform this action

Authenticate using...

ⓘ

then the user may authenticate using \*

Password (cloud deployment)

ⓘ +

If the preceding method fails or is not applicable, then

Password (Local Directory)

ⓘ +

+ ADD FALLBACK METHOD

CANCEL

SAVE

7. Set the Policy to **All Device Types**
- Change the switch for **registering FIDO2 authenticator** to **YES**
  - Set the authentication method to **Password (cloud deployment)**
  - Set the fallback method to **Password (Local Directory)**



The screenshot shows a web form with two distinct sections. The top section contains a 'CANCEL' button, a 'BACK' button, and a 'NEXT' button. The 'NEXT' button is highlighted with a red rectangular box. The bottom section contains a 'CANCEL' button, a 'BACK' button, and a 'SAVE' button. The 'SAVE' button is also highlighted with a red rectangular box. There is a horizontal line separating the two sections. The text 'yment)' is visible at the bottom of the form.

10. Click **NEXT** and **SAVE**

## Part 2: Register Authenticator

The screenshot shows a web browser window with the address bar displaying 'https://aw-herbertvogal.vidmpreview.com/authcontrol/auth/request'. The main content area features a white card with a blue hexagonal logo at the top. Below the logo is a blue button labeled 'Sign in with FIDO2 Authenticator'. Underneath this button, the text 'First time signing in?' is displayed, followed by a red rectangular box highlighting the text 'Register your FIDO2 Authenticator'. Below this box is a link that says 'Sign in another way'. At the bottom of the card, there is a note: 'In case of questions, contact your IT administrator.' followed by a link 'Learn more about FIDO2 Authentication.'


1. Close our **Chrome** and **re-open** it and browse to your **WorkspaceONE Access URL**.

Do **NOT** do this in the lab environment. As we will require a physical device with supported authentication Type (See below)

- You should now see Sign in with FIDO2 Authenticator.
- Click **Register** your **FIDO2** Authenticator

Browser	OS	Authenticator Type
Chrome 85	MacOS 10.15.7	TouchID
		External (Yubikey)
	Windows 10	Windows Hello
		External (Yubikey)
Safari 14.0.2 and higher	MacOS 10.15.7	External (Yubikey)
Edge Chromium 85	Windows 10	Windows Hello
		External (Yubikey)
Firefox 81	Windows 10	External (Yubikey)

2. Note the authentication form factors on the various different browsers and operating systems. Make sure you are using one of these and not in a virtual lab environment.

  
Workspace ONE™

Select Your Domain


✓ System Domain

euc-livewire.com

Auth0

Next

vmware

  
Workspace ONE™

username

mark

password

\*\*\*\*\*

euc-livewire.com

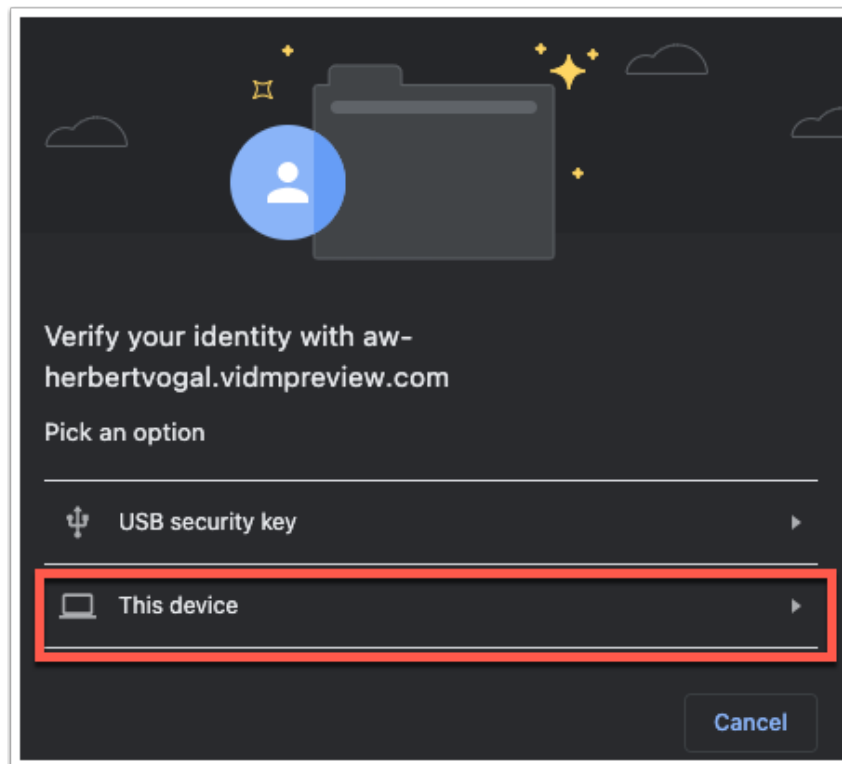
Sign in

[Forgot password?](#)

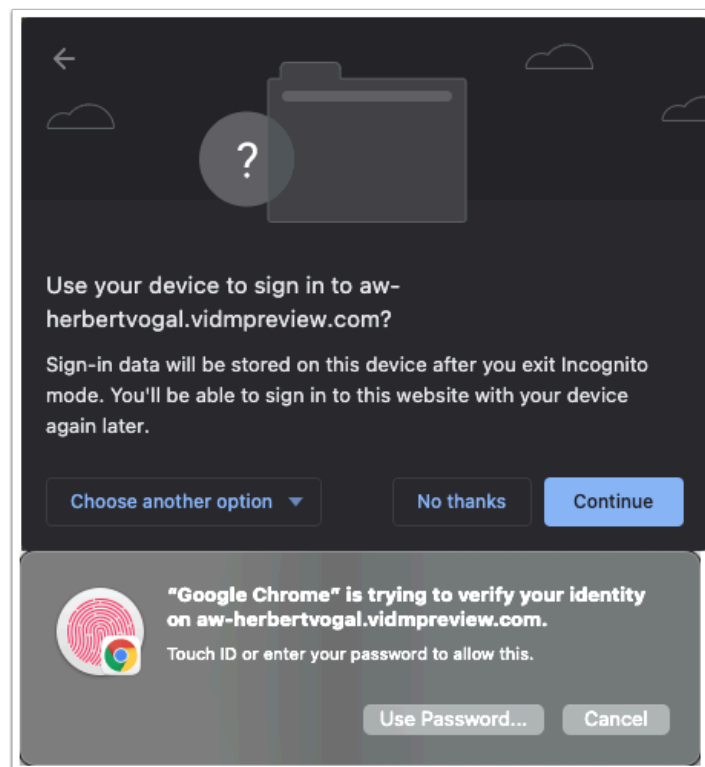
[Change to a different domain](#)

vmware

3. Select the euc-livewire.com domain and authenticate using the **Mark VMware1!** account. Click **Sign in**

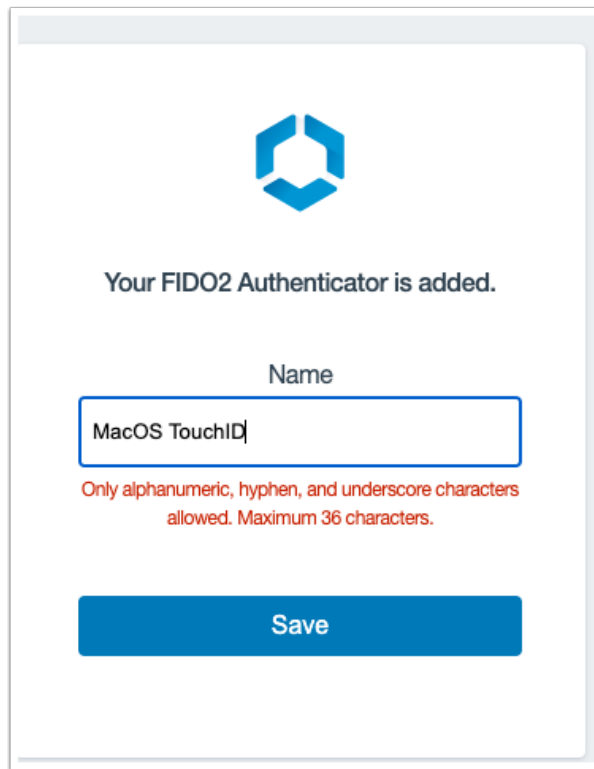


4. At this point the registration for **FIDO2** kicks in and you will be asked in by the browser to select how to verify your identity.
- click **This device**



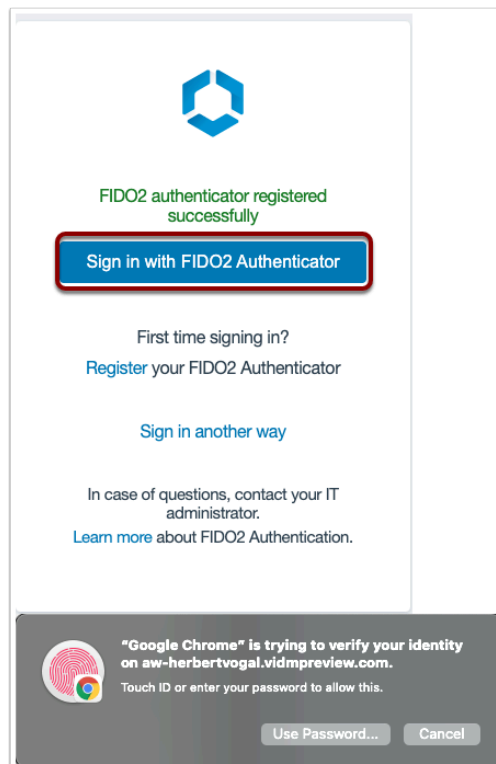
5. Click **Continue** on the next prompt
- Then use you Password & Windows Hello or Touch ID





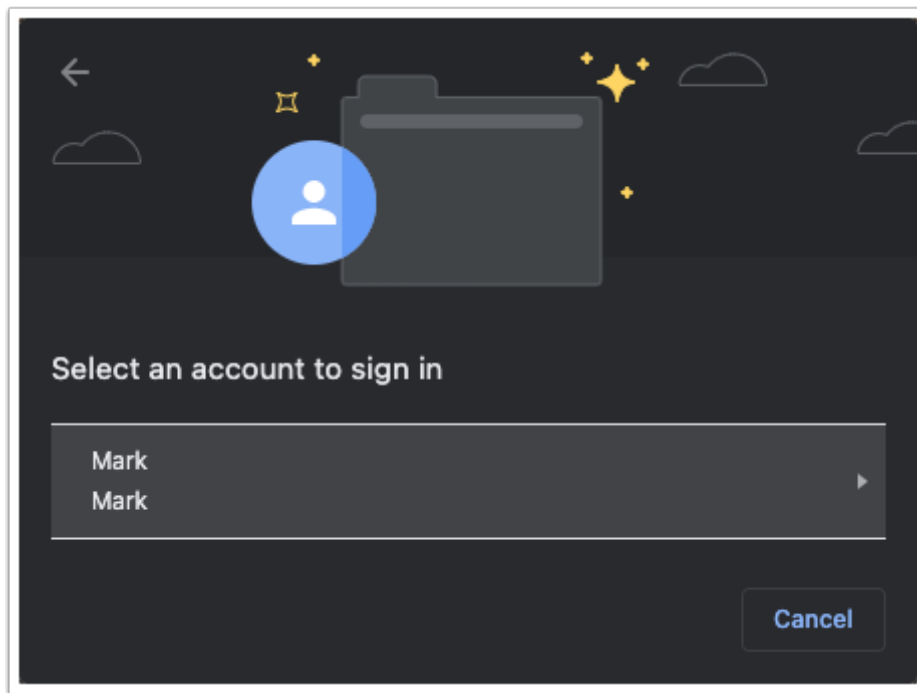
The image shows a web browser window with a white background. At the top center is a blue hexagonal logo. Below it, the text "Your FIDO2 Authenticator is added." is displayed. Underneath is a label "Name" followed by a text input field containing "MacOS TouchID". Below the input field is a red error message: "Only alphanumeric, hyphen, and underscore characters allowed. Maximum 36 characters." At the bottom is a large blue button with the word "Save" in white.

6. Give your authenticator method a name and click **Save**

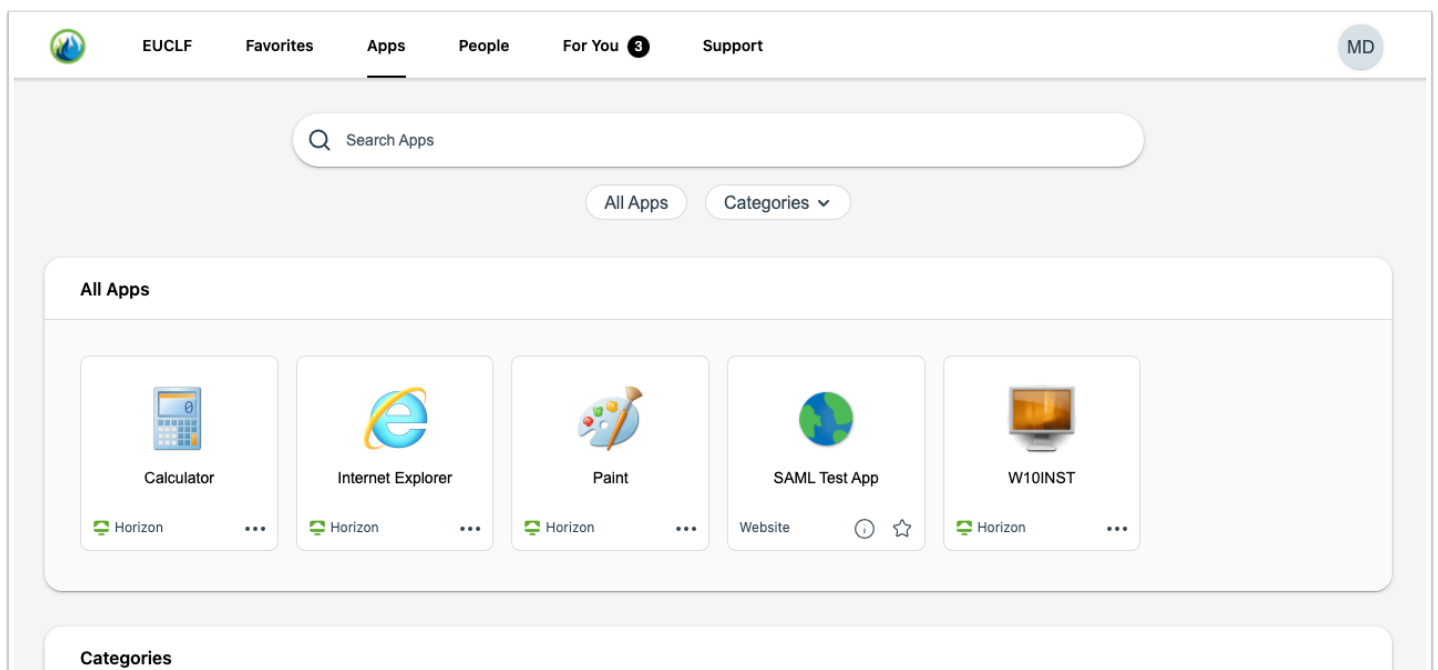


The image shows a web browser window with a white background. At the top center is a blue hexagonal logo. Below it, the text "FIDO2 authenticator registered successfully" is displayed in green. Underneath is a blue button with a red border and the text "Sign in with FIDO2 Authenticator". Below the button is the text "First time signing in?" followed by a link "Register your FIDO2 Authenticator". Below that is a link "Sign in another way". At the bottom, there is text "In case of questions, contact your IT administrator." and a link "Learn more about FIDO2 Authentication." At the very bottom, there is a dark grey overlay with a fingerprint icon, the text "Google Chrome is trying to verify your identity on aw-herbertvogal.vidmpreview.com.", and the text "Touch ID or enter your password to allow this." with two buttons: "Use Password..." and "Cancel".

7. Now click **Sign in with FIDO2 Authenticator** and use the Windows Hello or TouchID to authenticate.



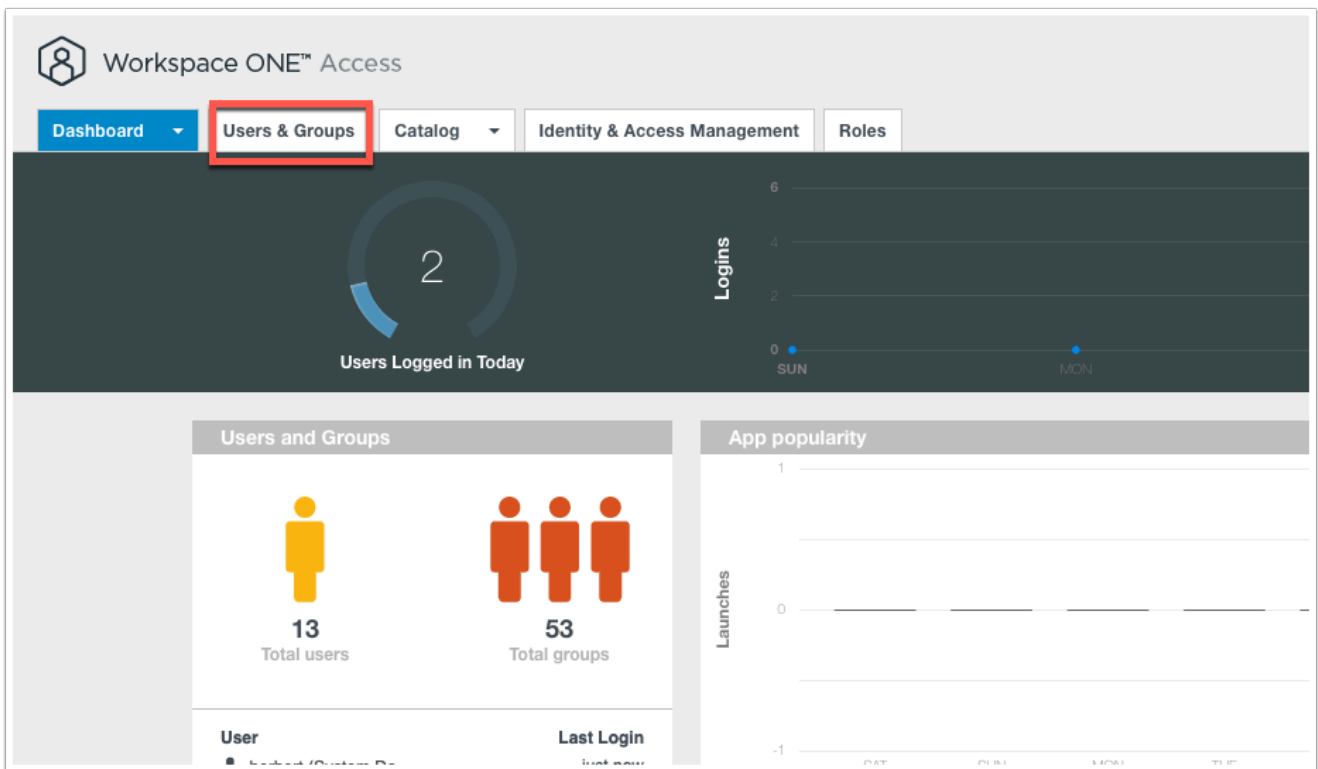
8. Select the user associated with that authenticator **Mark**



9. You should be authenticated with the user **Mark** to **Intelligent Hub**.
- Close the Chrome and re-open.
  - Experience seamless FIDO2 authentication to Intelligent Hub.

## Part 3: Administer FIDO2 Keys

The WorkspaceONE Access admin console offers the ability to manage FIDO2 keys within the user attributes.



1. Log into the **WorkspaceONE Access admin** console. This may require you to close the browser and re-open it or use a different browser.
  - Once logged in click on **Users & Groups**

The screenshot shows the VMware Workspace ONE Access console. The top navigation bar includes 'Dashboard', 'Users & Groups', 'Catalog', 'Identity & Access Management', and 'Roles'. The 'Users & Groups' section is active, showing a list of users. The user 'Mark Debio' is highlighted with a red box. Below the list, the 'Two-Factor Authentication' tab is selected, showing the user's profile details and authentication settings.

User Name	User ID	Domain	Directo
Admin,Tenant	herbert	System Domain	System
Debio,Mark	Mark	euc-livfire.com	Livfire
Dusello,Fernando	Fernando	euc-livfire.com	Livfire
Ikin,Kevin	Kevin	euc-livfire.com	Livfire
Marios,Tom	Tom	euc-livfire.com	Livfire
Markez,Kim	kim	euc-livfire.com	Livfire

Mark Debio (Mark)  
Domain: euc-livfire.com  
Directory: LivfireSync  
Status: User is enabled

Principal Name: Mark@euc-livfire.com  
Distinguished Name: CN=Mark Debio,OU=Sales,OU=Corp,DC=euc-livfire,DC=com  
External ID: d710751c-b022-407c-b086-8ba634c9f22c

First Name: Mark  
Last Name: Debio  
Username: Mark  
Email: mark@euc-livfire.com  
Role: User

Enable  
Delete User

2. **Select** the user that you have been doing the tests with. (My case this is **Mark Debio**)
  - Click **Two-Factor Authentication** on the user record

The screenshot shows the 'Two-Factor Authentication' settings for the user 'Mark Debio'. The 'Intelligent Hub Verify' section is active, showing a 'Reset' button and device information. The 'FIDO2' section is highlighted with a red box, showing a table of configured security keys.

Intelligent Hub Verify  
Preferred device receives Intelligent Hub verify requests. Reset will reset the user's selection of preferred device.

Reset

Device Friendly Name: Herbertvogal@gmail.com Android X1X0Android\_Android SDK built for x86\_64\_358240051111110  
UDID: ac57448021ca066eb28a46f30e47f724a95fb48a9  
Make/Model: google Android SDK built for x86\_64

VMware Verify  
No VMware Verify devices found. Looks like the user hasn't enabled VMware Verify yet.

FIDO2  
Add up to ten FIDO2 security keys. Only USB security keys are allowed.

Add Delete Rename Block Unblock ⓘ

Name	Make/Model	Registration Time	Status ⓘ
Mac2	Not Detectable	Jul 15, 2021 5:47:22 PM	Activated
MacOSTouchID	Not Detectable	Jul 15, 2021 1:31:27 PM	Activated

3. We are interested in the FIDO2 section on this page where you will find the current security authenticators that have been configured for this user.

## FIDO2

Add up to ten FIDO2 security keys. Only USB security keys are allowed.

[Add](#) [Delete](#) [Rename](#) [Block](#) [Unblock](#) ⓘ

	Name	Make/Model	Registration Time	Status ⓘ
<input type="radio"/>	Mac2	Not Detectable	Jul 15, 2021 5:47:22 PM	Activated
<input checked="" type="radio"/>	MacOSTouchID	Not Detectable	Jul 15, 2021 1:31:27 PM	Activated

4. Select a authenticator and note the options you have to delete, rename and block this authenticator.

This concludes the lab on configuring FIDO2 authentication on WorkspaceONE Access.

Author: Simeon Frank